MATH 145 - Introduction to Number Theory

1 Greatest Common Divisor

Lecture 1 Wed 09/04
Introduction, definition of gcd

Number theory is in some sense about the interplay between addition and multiplication. The theorems can be very innocent looking but the proofs tend to involve every branch of pure mathematics. For example, Fermat's Last Theorem states that the equation $x^n + y^n = z^n$ has no nonzero integer solutions when $n \geq 3$. The proof by Wiles and Taylor almost 30 years ago uses techniques from geometry, topology, analysis and algebraic number theory. Some examples of innocent looking but unsolved conjectures include Landau's four problems about primes:

- (Goldbach) Every even integer at least 4 is a sum of two primes.
- (Twin prime) There are infinitely many primes p such that $p + 2$ is prime.
- (Legendre) For any positive integer n, there is a prime between n^2 and $(n + 1)^2$.
- (Bunyakovsky) There are infinitely many integers n such that $n^2 + 1$ is prime.

What do we need to do to **prove** these? Let's pretend we have a truly marvelous proof of Goldbach but it doesn't fit in the margin.

- (Direct proof) Let n be an arbitrary even integer at least 4. Explain why n can be written as $p + q$ where p and q are primes. One possible way to do this is by writing down a formula for p and q and check that $n = p + q$ and that p and q are both prime.

  Why doesn't the following work? Let n be an arbitrary even integer at least 4. Let $p = n - 3$ and $q = 3$. Then $n = p + q$.

- (Proof by contradiction) Suppose for a contradiction that n is an even integer at least 4 that is not a sum of two primes. Use this to derive something that possibly can't be true. Two types of contradictions:

  – A false statement. E.g. $1 = 0$.
  – Two statements that can't be true at the same time. E.g. $x < y$ and $y < x$.

  A better set up: Suppose for a contradiction that n is the smallest even integer at least 4 that is not a sum of two primes. Now imagine that we somehow prove that $n - 2$ is not a sum of two primes and that $n - 2 \geq 4$. Are we done?

What allows us to pick the smallest counterexample above, is the following well-ordering principle.

Proposition 1.1 *The set $\mathbb{N}$ is well-ordered. In other words, every non-empty collection of positive integers has a smallest element.*

Proof: Texts in this kind of blue color are generally skipped in class.

- (We are proving a statement about **every** non-empty subset of $\mathbb{N}$): Let S be a non-empty subset of $\mathbb{N}$.

- (Give a formula for a candidate for the smallest element): Let $n \in S$ be an element. Let $T = \{x \in S : x \leq n\}$. Then T is a non-empty finite set and thus has a smallest element n_0.
- (Prove that n_0 is the smallest element of S): For any $x \in S$, if $x > n$, then $x > n \geq n_0$; if $x \leq n$, then $x \in T$ and so $x \geq n_0$.

Therefore, n_0 is the smallest element of S. □

Corollary 1.2 *The set $\mathbb{N} \cup \{0\}$ is well-ordered. In other words, every non-empty collection of non-negative integers has a smallest element.*

Proposition 1.3 *(Division algorithm) Let a, b be integers such that $a > 0$. Then there exists integers q, r such that*

$$b = aq + r, \qquad 0 \leq r < a.$$

"Proof" by example: Let's try to divide $b = 420$ by $a = 69$. Which of the following works?

$$\begin{aligned} 420 &= 69 \cdot 0 + 420 \\ 420 &= 69 \cdot 1 + 351 \\ 420 &= 69 \cdot 2 + 282 \\ 420 &= 69 \cdot 3 + 213 \\ 420 &= 69 \cdot 4 + 144 \\ 420 &= 69 \cdot 5 + 75 \\ 420 &= 69 \cdot 6 + 6 \\ 420 &= 69 \cdot 7 - 63 \end{aligned}$$

So we may take $q = 6$ and $r = 6$. How can we turn this into a proper proof? Main idea: We kept subtracting 69 from 420 until we can't anymore without going negative. How do we know this process will always end? Consider the set

$$\begin{aligned} S &= \{420 - 69k : k \in \mathbb{Z}, 420 - 69k \geq 0\} \\ &= \{6, 75, 144, 213, 282, 351, 420, 489, \ldots\}. \end{aligned}$$

Then r can be constructed as the smallest element of S.

Proof:

- (Define the set S): Consider the set $S = \{b - ak : k \in \mathbb{Z}, b - ak \geq 0\}$. The set S is a subset of $\mathbb{N} \cup \{0\}$.
- (To use Corollary 1.2, we need to make sure S is non-empty): Since $a > 0$, we see that $\lim_{k \to -\infty} b - ak = \infty$. Hence for k sufficiently negative, $b - ak \geq 0$. Hence $S \subseteq \mathbb{N} \cup \{0\}$ is non-empty.
- (Give the definition of r): Let $r \in S$ be its smallest element.
- (Give the definition of q): Then $r = b - ak$ for some $k \in \mathbb{Z}$. Let $q = k$ so that $b = aq + r$.
- (Prove that r satisfies the desired inequality): By definition, $r \geq 0$. It remains to prove that $r < a$. (It is usually a good idea to tell your reader what you are going to prove next.)
- (When in doubt, proof by contradiction): Suppose for a contradiction that $r \geq a$.
- (Find something smaller than r in S): Then $r - a \geq 0$ and $r - a = b - ak - a = b - a(k + 1) \in S$. However, $r - a < r$ contradicting the minimality of r.

Therefore, $b = aq + r$ and $0 \leq r < a$. □

Remark: The integers q, r are unique and are called the quotient and remainder when b is divided by a. We also have the division algorithm for negative a. In general, we have

$$\exists q, r \in \mathbb{Z}, \quad b = aq + r \text{ and } 0 \leq r < |a|.$$

Question: What is the smallest positive integer d that can be written as

$$69x + 420y \qquad \text{where} \qquad x, y \in \mathbb{Z}?$$

Can d be 1? Can d be 2? Note that $3 \mid 69$ and $3 \mid 420$. So for any integers x, y, we have $3 \mid 69x + 420y$. This implies that d has to be divisible by 3. Can d be 3? Note from the above division algorithm, we have

$$6 = 69 \times (-6) + 420 \times 1.$$

Is $d = 3$ or $d = 6$? What if we apply the division algorithm to divide 69 by 6? We get

$$69 = 6 \times 11 + 3.$$

So we have

$$\begin{aligned} 3 &= 69 - 6 \times 11 \\ &= 69 - (69 \times (-6) + 420 \times 1) \times 11 \\ &= 69 \times (1 - (-6) \times 11) + 420 \times (-11) \\ &= 69 \times 67 + 420 \times (-11). \end{aligned}$$

What allows us to find something positive and smaller than 6 that can be written as $69x + 420y$? Why can't we keep going to possibly find something smaller than 3? The key point is that $6 \nmid 69$. So when we divide 69 by 6, we get a nonzero remainder 3. However, $3 \mid 69$ and $3 \mid 420$, so we will have a remainder of 0 if we were to divide 69 or 420 by 3.

Proposition 1.4 *Let a, b be integers that are not both 0. Let d be the smallest positive integer of the form $ax + by$ for some integers x, y.*

(a) If e is an integer such that $e \mid a$ and $e \mid b$, then $e \mid d$.

(b) We have $d \mid a$ and $d \mid b$.

We write $d = \gcd(a, b)$ and say d is the **greatest common divisor** of a and b.

Proof:

- (Give some names to the x, y that make up d): Let x_0 and y_0 be integers such that $d = ax_0 + by_0$.
- (Proof of (a)): If $e \mid a$ and $e \mid b$, then $e \mid ax_0 + by_0$. So $e \mid d$.
- (a and b are symmetric): We now prove the $d \mid a$ part of (b).
- (Perform the same operation as in the example to find something smaller): Suppose for a contradiction that $d \nmid a$. We apply the division algorithm to find integers q, r such that $a = dq + r$ with $0 \leq r < d$. The assumption $d \nmid a$ implies that $r \neq 0$. So r is positive and smaller than d.
- (Prove as in the example that r is of the form $ax + by$): Then

  $$r = a - dq = a - (ax_0 + by_0)q = a(1 - x_0 q) + b(-y_0 q).$$

  Note that $1 - x_0 q$ and $-y_0 q$ are integers.

This contradicts the minimality of d. So we have $d \mid a$. The argument for $d \mid b$ is the same. □

We define $\gcd(0,0) = 0$.

Corollary 1.5 *(Bezout's Lemma) Let a, b be integers. Then there exist integers x, y such that*

$$\gcd(a,b) = ax + by.$$

In fact, $\gcd(a,b)$ is the smallest positive integer of the form $ax + by$, when a and b are not both 0.

Lecture 2 Fri 09/06

Properties of gcd

Proposition 1.6 *Let a, b be integers. Let d be a non-negative integer. Then the following are equivalent:*

(a) $d \mid a$ and $d \mid b$ and $d = ax + by$ for some integers x, y;

(b) $d = \gcd(a,b)$.

Proof: (Proving a statement like this requires proving that (a) implies (b) and (b) implies (a). You are free to pick which one to do first.) $(b) \Rightarrow (a)$ follows from the definition of gcd. We now prove $(a) \Rightarrow (b)$. (One way to prove that two non-negative integers n and m are equal is to prove that $n \mid m$ and $m \mid n$.) Since $d \mid a$ and $d \mid b$ and $\gcd(a,b)$ is of the form $ax + by$ for some integers x, y, we have $d \mid \gcd(a,b)$. Since $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$ and d is of the form $ax + by$ for some integers x, y, we have $\gcd(a,b) \mid d$. Hence $d = \pm \gcd(a,b)$. Since both are non-negative, we have $d = \gcd(a,b)$. □

Corollary 1.7 *Let a, b be integers. Then the following are equivalent:*

(a) $a \mid b$;

(b) $\gcd(a,b) = |a|$.

In particular, we have $\gcd(a,0) = |a|$.

Proof: $(b) \Rightarrow (a)$: Suppose $\gcd(a,b) = |a|$. Then from $a \mid |a|$ and $|a| \mid b$, we have $a \mid b$. (It is also true that $|a| \mid a$, but we don't need it here.)

$(a) \Rightarrow (b)$: Suppose $a \mid b$. We use Proposition 1.6 with $d = |a|$ to prove $d = \gcd(a,b)$. From $|a| \mid a$ and $a \mid b$, we have $|a| \mid b$. Moreover, we know that $|a| = a \cdot (\pm 1)$ is of the form $ax + by$. So $|a| = \gcd(a,b)$. □

Proposition 1.8 *Let a, b, q be integers. Then $\gcd(a,b) = \gcd(a, b - aq)$.*

Proof: We use Proposition 1.6 with $d = \gcd(a, b - aq) \geq 0$ to prove $d = \gcd(a,b)$. It suffices to prove that $d \mid a$, $d \mid b$ and $d = ax + by$ for some integers x, y. From $d = \gcd(a, b - aq)$, we have $d \mid a$ and $d \mid b - aq$. Since $b = (b - aq) + aq$, we have $d \mid b$. From Bezout's lemma, we know there are integers x_0, y_0 such that $d = ax_0 + (b - aq)y_0$, which we can rearrange into

$$d = a(x_0 - qy_0) + by_0$$

with $x_0 - qy_0$ and y_0 both integers. □

Proposition 1.8 makes calculation very easy. Let's compute $\gcd(69, 2024)$. We know for any integer q, we have

$$\gcd(69, 2024) = \gcd(69, 2024 - 69q).$$

Note we don't have to take q to be the quotient when dividing 2024 by 69. A convenient choice could be $q = 30$ so that $69q = 2070$. Then

$$\gcd(69, 2024) = \gcd(69, -46) = \gcd(46, 69) = \gcd(46, 69 - 46) = \gcd(46, 23) = 23.$$

Here, we also used

$$\gcd(a,b) = \gcd(b,a) \qquad \text{and} \qquad \gcd(a,b) = \gcd(a,-b)$$

which you will prove in HW 1 P1.

In the formula $\gcd(a,b) = \gcd(a, b-aq)$, there is a fairly natural choice for q when $a \neq 0$. Namely, we can apply the division algorithm to write $b = aq + r$ where $0 \leq r < |a|$. Then

$$\gcd(a,b) = \gcd(a, b-aq) = \gcd(a,r) = \gcd(r,a).$$

The upshot now is that the absolute value of the first coordinate becomes smaller when we replace (a,b) by (r,a). This process can be repeated until the first coordinate becomes 0, in which case the gcd is easy to compute. This is the Euclidean algorithm.

Euclidean algorithm: Input a pair of integers (a,b). Output $\gcd(a,b)$.

- Step 1: If $a = 0$, return $|b|$.
- Step 2: If $a \neq 0$, replace (a,b) by (r,a) where r is the remainder when b is divided by a. Go back to Step 1.

As an example, we can compute

$$\gcd(1239, 735) = \gcd(735, 1239) = \gcd(504, 735) = \gcd(231, 504) = \gcd(42, 231) = \gcd(21, 42) = \gcd(0, 21) = 21.$$

Question: (IMO 1959P1) Let n be an integer. What values can $\gcd(14n+3, 21n+4)$ take?

$$\gcd(14n+3, 21n+4) = \gcd(14n+3, 21n+4-(14n+3)) = \gcd(14n+3, 7n+1)$$

and

$$\gcd(14n+3, 7n+1) = \gcd(14n+3-(7n+1)2, 7n+1) = \gcd(1, 7n+1) = 1.$$

Challenge Question: Let n be an integer. What values can $\gcd(506-n^2, 506-(n+1)^2)$ take?

We say two integers a and b are **coprime** if $\gcd(a,b) = 1$.

Corollary 1.9 *Let a, b be integers. Then there exist integers x, y such that $ax + by = 1$ if and only if $\gcd(a,b) = 1$.*

Proof: Apply Proposition 1.6 with $d = 1$. □

Revisiting $\gcd(14n+3, 21n+4)$, we observe that

$$3(14n+3) + (-2)(21n+4) = 1.$$

So $\gcd(14n+3, 21n+4) = 1$ for all integers n.

Proposition 1.10 *Let a, b, c be integers such that $\gcd(a,c) = 1$. Then $\gcd(c, ab) = \gcd(c,b)$.*

Proof: We apply Proposition 1.6 with $d = \gcd(c,b) \geq 0$ to prove that $d = \gcd(c, ab)$. In other words, we prove $d \mid c$, $d \mid ab$, and $d = cx + aby$ for some integers x, y. From $d = \gcd(c,b)$, we have $d \mid c$ and $d \mid b$, which with $b \mid ab$ gives $d \mid ab$. By Bezout's lemma, we have

$$\begin{aligned} d &= cx_1 + by_1 \\ 1 &= cx_2 + ay_2 \end{aligned}$$

for some integers x_1, y_1, x_2, y_2. Multiply them to get

$$d = c(cx_1x_2 + ax_1y_2 + bx_2y_1) + ab(y_1y_2).$$

We take $x = cx_1x_2 + ax_1y_2 + bx_2y_1$ and $y = y_1y_2$. Then $d = cx + aby$ with integers x, y. □

Corollary 1.11 *Let a, b, c be integers. Suppose $c \mid ab$ and $\gcd(a, c) = 1$. Then $c \mid b$.*

Proof: Since $c \mid ab$, we have by Corollary 1.7 that $\gcd(c, ab) = |c|$. Since $\gcd(a, c) = 1$, we have by Proposition 1.10 that $\gcd(c, ab) = \gcd(c, b)$. Hence $|c| = \gcd(c, b)$. By Corollary 1.7 again, we have $c \mid b$. □

Proof: We give another (but equivalent) proof without invoking the earlier results. From $\gcd(a, c) = 1$, we have $1 = ax + cy$ for some integers x, y. Multiplying by b gives $b = abx + cby$. Since $c \mid ab$ and $c \mid c$, we have $c \mid abx + cby$ and so $c \mid b$. □

Exercises

1.1 (Uniqueness of division algorithm) Given integers a, b such that $a \neq 0$, prove that the integers q, r such that $b = aq + r$ and $0 \leq r < |a|$ are unique.

1.2 Given $a, b, c \in \mathbb{Z}$ that not all 0, let $\gcd(a, b, c)$ be the smallest positive integer of the form $ax + by + cz$. Prove that $\gcd(a, b, c) = \gcd(a, \gcd(b, c))$.

1.3 Let a, b, c, d be nonzero integers such that $ad - bc = \pm \gcd(a, c)$. Prove that $\gcd(an + b, cn + d) = 1$ for every integer n.

1.4 Let n be any integer. What values can $\gcd(506 - n^2, 506 - (n + 1)^2)$ take?

Lecture 2.5 (Tutorial) Fri 09/06

Congruences

Given integers m, a, b, we say a and b are congruent mod m if and only if $m \mid a - b$ and write

$$a \equiv b \pmod{m}.$$

For example, we have

$$15 \equiv 9 \pmod{3}, \qquad 420 \equiv 6 \pmod{69}.$$

When $m = 0$, we have

$$a \equiv b \pmod{0} \iff 0 \mid a - b \iff \exists k \in \mathbb{Z}, a - b = 0 \cdot k \iff a = b.$$

Note also that $a \equiv 0 \pmod{m}$ if and only if $m \mid a$. Congruences is an equivalence relation:

- (Reflexive) $a \equiv a \pmod{m}$: since $m \mid a - a$;
- (Symmetric) if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$: since $m \mid a - b$ implies $m \mid b - a$;
- (Transitive) if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$: since $m \mid a - b$ and $m \mid b - c$ imply $m \mid (a - b) + (b - c)$.

When you have an equivalence relation, things generally work out as you expected!

Lemma 1.12 *Suppose $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$. Then*

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m} \qquad \text{and} \qquad a_1 b_1 \equiv a_2 b_2 \pmod{m}.$$

Proof: We are given that $m \mid a_1 - a_2$ and $m \mid b_1 - b_2$. I will leave the additive one as an exercise. For the multiplicative one, we need to prove that

$$m \mid a_1 b_1 - a_2 b_2.$$

We use the following trick

$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_2 b_1 + a_2 b_1 - a_2 b_2 = (a_1 - a_2) b_1 + a_2 (b_1 - b_2).$$

Since $m \mid a_1 - a_2$ and $m \mid b_1 - b_2$, we are done. $\square$

For example, we have

$$10 \equiv 1 \pmod 3 \qquad \text{so} \qquad 10^n \equiv 1^n \equiv 1 \pmod 3$$

for any positive integer n. As a result,

$$\begin{aligned} 69145 &= 6 \cdot 10^4 + 9 \cdot 10^3 + 1 \cdot 10^2 + 4 \cdot 10 + 5 \\ &\equiv 6 + 9 + 1 + 4 + 5 \pmod 3 \\ &\equiv 1 \pmod 3. \end{aligned}$$

We thus have the familiar divisibility by 3 rule: a positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

You have probably heard of the following:

$$\begin{aligned} 1/7 &= 0.142857142857\cdots \\ 2/7 &= 0.285714285714\cdots \\ 3/7 &= 0.428571428571\cdots \\ 4/7 &= 0.571428571428\cdots \\ 5/7 &= 0.714285714285\cdots \\ 6/7 &= 0.857142857142\cdots \end{aligned}$$

Thus, the fractions $m/7$ for $m = 1, \ldots, 6$ are all formed from repeating 142857 but starting from different spots. Why does this happen? The shifting of the digits is a consequence of

$$\begin{aligned} 10/7 &= 1 + 3/7 \\ 100/7 &= 14 + 2/7 \\ 1000/7 &= 142 + 6/7 \\ 10000/7 &= 1428 + 4/7 \\ 100000/7 &= 14285 + 5/7 \\ 1000000/7 &= 142857 + 1/7 \end{aligned}$$

In terms of congruences, this reads

$$\begin{aligned} 10 &\equiv 3 \pmod 7 \\ 10^2 &\equiv 2 \pmod 7 \\ 10^3 &\equiv 6 \pmod 7 \\ 10^4 &\equiv 4 \pmod 7 \\ 10^5 &\equiv 5 \pmod 7 \\ 10^6 &\equiv 1 \pmod 7 \end{aligned}$$

Therefore, the reason why 1/7, 2/7, ..., 6/7 have the above pattern is because the remainder of 10, 10^2, ..., 10^6 when divided by 7 recover $1, 2, \ldots, 6$ (in a possibly different order). If we were to try this mod 11, we just get $10^2 \equiv 1 \pmod{11}$ and then it will just repeat 10 and 1. If we try this mod 13, we get

$$\begin{aligned} 10 &\equiv 10 \pmod{13} \\ 10^2 &\equiv 100 \equiv 9 \pmod{13} \\ 10^3 &\equiv 90 \equiv -1 \pmod{13} \\ 10^6 &\equiv 1 \pmod{13} \end{aligned}$$

This means that it will cycle with a period of 6.

Exercise: Check that this works for 17. It is unknown whether this happens for infinitely many primes p.

Note above that $10^{12} \equiv 1 \pmod{13}$, and $10^{10} \equiv 1 \pmod{11}$.

Theorem 1.13 *(Fermat's little Theorem) Let p be a prime and let $a \in \mathbb{Z}$ such that $p \nmid a$. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

"Proof" by example: We have

$$\begin{aligned} 10 \cdot 1 &\equiv 3 \pmod{7} \\ 10 \cdot 2 &\equiv 6 \pmod{7} \\ 10 \cdot 3 &\equiv 2 \pmod{7} \\ 10 \cdot 4 &\equiv 5 \pmod{7} \\ 10 \cdot 5 &\equiv 1 \pmod{7} \\ 10 \cdot 6 &\equiv 4 \pmod{7} \end{aligned}$$

Multiplying them together gives

$$10^6 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7}.$$

Canceling the $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$ from both sides gives $10^6 \equiv 1 \pmod{7}$.

Lemma 1.14 *Let m, a, b, c be integers such that $\gcd(c, m) \neq 0$. Suppose $ac \equiv bc \pmod{m}$. Then*

$$a \equiv b \pmod{\frac{m}{\gcd(c,m)}}.$$

Proof: We have $m \mid ac - bc$. So

$$\frac{m}{\gcd(c,m)} \mid \frac{c}{\gcd(c,m)}(a-b).$$

(We prove next that $\gcd(\frac{m}{\gcd(c,m)}, \frac{c}{\gcd(c,m)}) = 1$): By Bezout's lemma, we have $\gcd(c,m) = mx + cy$ for some integers x, y. Divide it by $\gcd(c,m)$ to get

$$1 = \frac{m}{\gcd(c,m)}x + \frac{c}{\gcd(c,m)}y.$$

By Corollary 1.9, we have $\gcd(\frac{m}{\gcd(c,m)}, \frac{c}{\gcd(c,m)}) = 1$. Then by Corollary 1.11, we have

$$\frac{m}{\gcd(c,m)} \mid a - b$$

which is equivalent to the desired congruence. □

Lecture 3 Mon 09/09
Unique factorization via p-adic valuation

2 Prime factorization

A **prime** is an integer $p > 1$ such that its only positive divisors are 1 and p. For any integer a, $\gcd(p, a)$ can only be 1 and p and more precisely,

$$\gcd(p,a) = \begin{cases} 1 & \text{if } p \nmid a, \\ p & \text{if } p \mid a. \end{cases}$$

Note that if p and q are two primes, then

$$p \mid q \iff p = q.$$

In other words, distinct primes are coprime. This is the origin of the name "coprime".

Proposition 2.1 *(Euclid's Lemma) Let p be a prime. Then for any integers a, b, if $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof: If $p \mid a$, then we are done. Suppose $p \nmid a$. Then $\gcd(p, a) = 1$. Then from $p \mid ab$, we get $p \mid b$ by Corollary 1.11. □

Corollary 2.2 *(Contrapositive of Euclid's Lemma) Let p be a prime. Then for any integers a, b, if $p \nmid a$ and $p \nmid b$, then $p \nmid ab$.*

The converse of Euclid's Lemma is also true:

Proposition 2.3 *Let $n > 1$ be an integer such that whenever n divides a product of integers, n must divide one of the factors. Then n is a prime.*

Proof: Let $d \mid n$ be a positive divisor of n. (We prove that either $d = 1$ or $d = n$) Then $n = de$ for some $e \in \mathbb{Z}$. Since $d, n > 0$, we have $e > 0$ and $e \mid n$. Since $n = de$, we have $n \mid de$ and so we get $n \mid d$ or $n \mid e$. If $n \mid d$, then along with $d \mid n$, we get $d = n$. If $n \mid e$, then along with $e \mid n$, we get $e = n$ and so $d = 1$. □

Remark: The proof of Euclid's Lemma ⇒ prime uses only division, whereas the proof of prime ⇒ Euclid's Lemma requires the theory of gcd. There are number systems in general where the notion of gcd doesn't exist, or worse where unique factorization doesn't hold.

Our next major result is the famous fundamental theorem of arithmetic, which you are probably taking for granted.

Theorem 2.4 *(Fundamental Theorem of Arithmetic) Every positive integer can be written as a product of primes, unique up to reordering.*

For example, we have

$$\begin{aligned} 69 &= 3 \cdot 23 \\ 145 &= 5 \cdot 29 \\ 420 &= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \\ 2023 &= 7 \cdot 17 \cdot 17 \\ 2024 &= 2 \cdot 2 \cdot 2 \cdot 11 \cdot 23 \\ 2025 &= 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \end{aligned}$$

For any prime p and any integer $n \neq 0$, we define the p-adic valuation $\nu_p(n)$ to be the largest integer k such that $p^k \mid n$. A commonly used notation is

$$p^{\nu_p(n)} \mid\mid n.$$

Alternatively, $\nu_p(n)$ is the unique non-negative integer k such that

$$p^k \mid n \qquad \text{and} \qquad p \nmid \frac{n}{p^k}.$$

We use the convention $\nu_p(0) = \infty$. For example,

$$\nu_3(2025) = 4, \qquad \nu_2(2024) = 3, \qquad \nu_2(420) = 2.$$

It follows immediately from the definitions that if p and q are two primes, then

$$\nu_p(q) = \begin{cases} 1 & \text{if } q = p, \\ 0 & \text{if } q \neq p. \end{cases}$$

Proposition 2.5 *Let p be any prime and let n, m nonzero integers. Then*

$$\nu_p(nm) = \nu_p(n) + \nu_p(m), \qquad \nu_p(n+m) \geq \min\{\nu_p(n), \nu_p(m)\}.$$

If $\nu_p(n) \neq \nu_p(m)$, then

$$\nu_p(n+m) = \min\{\nu_p(n), \nu_p(m)\}.$$

Proof: Let $k = \nu_p(n)$ and $\ell = \nu_p(m)$. From $p^k \mid n$ and $p^\ell \mid m$, we have $p^{k+\ell} \mid nm$. From $p \nmid n/p^k$ and $p \nmid m/p^\ell$, we have $p \nmid nm/p^{k+\ell}$ by Corollary 2.2. Therefore, $\nu_p(nm) = k + \ell$.

Suppose without loss of generality that $k \leq \ell$. Then $p^k \mid p^\ell$ and so $p^k \mid m$. Since $p^k \mid n$, we have $p^k \mid n + m$. Thus $\nu_p(n+m) \geq k$. Suppose $k < \ell$. Then $p \mid m/p^k$ but $p \nmid n/p^k$. Hence $p \nmid (n+m)/p^k$. So $\nu_p(n+m) = k$. □

Corollary 2.6 *For any positive integer $\ell \in \mathbb{N}$ and nonzero integers $n_1, \ldots, n_\ell$, we have*

$$\nu_p\Big(\prod_{i=1}^{\ell} n_i\Big) = \nu_p(n_1 \cdots n_\ell) = \nu_p(n_1) + \cdots + \nu_p(n_\ell) = \sum_{i=1}^{\ell} \nu_p(n_i).$$

Proof: We prove by induction on ℓ.

- (Prove the base case when $\ell = 1$): Suppose first $\ell = 1$. Then we need to prove that $\nu_p(n_1) = \nu_p(n_1)$, which is clearly true.
- (Suppose $\ell \geq 2$ and that the statement is true for all the previous cases): Suppose now $\ell \geq 2$. Suppose that for any $k = 1, 2, \ldots, \ell - 1$ and any nonzero integers $m_1, \ldots, m_k$, we have

  $$\nu_p(m_1 \cdots m_k) = \nu_p(m_1) + \cdots + \nu_p(m_k).$$

- (Under the above inductive hypothesis, prove the case for ℓ): Let $n_1, \ldots, n_\ell$ be arbitrary nonzero integers. Since $\ell \geq 2$, we have $\ell - 1 \geq 1$. So by the inductive hypothesis with $k = \ell - 1$, we have

  $$\nu_p(n_1 \cdots n_{\ell-1}) = \nu_p(n_1) + \cdots + \nu_p(n_{\ell-1}).$$

  Now by Proposition 2.5, we have

  $$\begin{aligned} \nu_p(n_1 \cdots n_\ell) &= \nu_p((n_1 \cdots n_{\ell-1})n_\ell) \\ &= \nu_p(n_1 \cdots n_{\ell-1}) + \nu_p(n_\ell) \\ &= \nu_p(n_1) + \cdots + \nu_p(n_{\ell-1}) + \nu_p(n_\ell). \end{aligned}$$

Therefore, we are done. □

Whenever you notice that your proof involves "repeatedly" or "$\cdots$", induction is typically the way to make things precise.

Corollary 2.7 *Let n_q be non-negative integers for primes q such that all but finitely many of them are 0. Then for any prime p,*

$$\nu_p\left(\prod_q q^{n_q}\right) = \sum_q \nu_p(q^{n_q}) = n_p.$$

In particular, prime factorizations are unique, because the exponent of a prime p can be recovered as the p-adic valuation. (Unless otherwise specified, a sum or product over an index p or q is running only over primes p.)

We prove next the existence of prime factorization.

Theorem 2.8 *Let $n \in \mathbb{N}$. Then $\nu_p(n) = 0$ for all but finitely many primes p and*

$$n = \prod_p p^{\nu_p(n)}.$$

In particular, prime factorizations exist.

Proof: If $p > n$, then clearly $p \nmid n$ and so $\nu_p(n) = 0$. We prove the second statement by induction on n. Suppose first that $n = 1$. Then $\nu_p(1) = 0$ for all primes p and $\prod_p p^0 = 1$. Hence the statement is true for the base case $n = 1$.

Suppose now $n \geq 2$ and that for every integer $m = 1, 2, \ldots, n-1$, we have $m = \prod_p p^{\nu_p(m)}$. We now prove $n = \prod_p p^{\nu_p(n)}$. Suppose first that $n = q$ is a prime. In this case,

$$\prod_p p^{\nu_p(q)} = q^1 \prod_{p \neq q} p^0 = q.$$

Suppose now n is not a prime. Let d be a positive divisor of n with $1 < d < n$. Let $e = n/d$. Then e is an integer with $1 < e < n$. By the induction hypothesis, we have

$$d = \prod_p p^{\nu_p(d)}, \qquad e = \prod_p p^{\nu_p(e)}.$$

Multiplying them gives

$$n = de = \prod_p p^{\nu_p(d)+\nu_p(e)} = \prod_p p^{\nu_p(n)}$$

since $\nu_p(d) + \nu_p(e) = \nu_p(de) = \nu_p(n)$. □

Lecture 4 Wed 09/11

Some applications of unique factorization

We can extend ν_p to all rational numbers by defining $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$. The multiplicative property of ν_p implies that if $a/b = c/d$, then $ad = bc$ and so $\nu_p(a) + \nu_p(d) = \nu_p(b) + \nu_p(c)$. In other words,

$$\nu_p(a) - \nu_p(b) = \nu_p(c) - \nu_p(d).$$

Hence $\nu_p(a/b)$ is independent on the choices of a and b.

Corollary 2.9 *(Unique prime factorization for rational numbers.) Let $r \in \mathbb{Q}$ be nonzero. Then*

$$r = \pm \prod_p p^{\nu_p(r)}.$$

As a consequence,

(a) $r \in \mathbb{Z}$ if and only if $\nu_p(r) \geq 0$ for all primes p;

(b) $r = \pm 1$ if and only if $\nu_p(r) = 0$ for all primes p.

Corollary 2.10 *Let d, n be nonzero integers. Then $d \mid n$ if and only if $\nu_p(d) \leq \nu_p(n)$ for all primes p.*

Proof: We have $d \mid n$ if and only if $n/d \in \mathbb{Z}$ if and only if $\nu_p(n/d) = \nu_p(n) - \nu_p(d) \geq 0$ for all primes p. □

Corollary 2.11 *Let n be a nonzero integer. Then the number of positive divisors of n is*

$$\prod_p (1 + \nu_p(n)).$$

Proof: Any positive divisor d is uniquely determined by $\nu_p(d)$ for all primes p. There are $1+\nu_p(n)$ possible values for $\nu_p(d)$ in order for $0 \leq \nu_p(d) \leq \nu_p(n)$. □

Question: Suppose $n \in \mathbb{N}$. When is the number of positive divisor of n odd?

We need $\nu_p(n)$ to be even for all prime p. In other words, n is a perfect square. Alternatively, we can pair up the positive divisors of n by $(m, n/m)$. In order for there to be an odd number of them, there is some m such that $m = n/m$, implying that $n = m^2$.

Corollary 2.12 *Let n, m be nonzero integers. Then for any prime p,*

$$\nu_p(\gcd(n,m)) = \min\{\nu_p(n), \nu_p(m)\}.$$

Proof: Since $\gcd(n,m)$ divides n and m, we see that for any prime p, $\nu_p(\gcd(n,m)) \leq \nu_p(n)$ and also $\leq \nu_p(m)$. Hence $\nu_p(\gcd(n,m)) \leq \min\{\nu_p(n), \nu_p(m)\}$. For the other inequality, let $d_p = \min\{\nu_p(n), \nu_p(m)\}$. Note that $d_p = 0$ for $p > \max\{n, m\}$. We let $d = \prod_p p^{d_p}$. From $d_p \leq \nu_p(n)$ for all p, we get $d \mid n$ and similarly $d \mid m$. Hence $d \mid \gcd(n,m)$ and so $d_p \leq \nu_p(\gcd(n,m))$ for all primes p. □

This formula allows us to compute gcd very quickly from the prime factorization. For example,

$$\gcd(2^4 3^5 5^2 7^3, 2^2 3^2 7^4) = 2^2 3^2 7^3.$$

However, in practice (to a computer), Euclidean's algorithm is much faster for computing gcd, since factorization is very hard. Using this formula, we can give another proof for Proposition 1.10: Let a, b, c be integers such that $\gcd(a,c) = 1$. Then $\gcd(c, ab) = \gcd(c, b)$.

Second proof of Proposition 1.10: Let p be any prime. It suffices to prove that

$$\min\{\nu_p(c), \nu_p(a) + \nu_p(b)\} = \min\{\nu_p(c), \nu_p(b)\}.$$

The assumption $\gcd(a,c) = 1$ gives that $\min\{\nu_p(a), \nu_p(c)\} = 0$. That is, either $\nu_p(a) = 0$ or $\nu_p(c) = 0$. If $\nu_p(a) = 0$, then we have

$$\min\{\nu_p(c), \nu_p(a) + \nu_p(b)\} = \min\{\nu_p(c), 0 + \nu_p(b)\} = \min\{\nu_p(c), \nu_p(b)\}.$$

If $\nu_p(c) = 0$, then we have

$$\min\{\nu_p(c), \nu_p(a) + \nu_p(b)\} = 0 = \min\{\nu_p(c), \nu_p(b)\}.$$

This concludes the proof. □

Similarly for nonzero integers x, y, z, we have

$$\nu_p(\gcd(x,y,z)) = \min\{\nu_p(x), \nu_p(y), \nu_p(z)\}.$$

A related concept is the least common multiple $\mathrm{lcm}(m,n)$ of two integers m, n, or of multiple integers. One easily checks that

$$\nu_p(\mathrm{lcm}(n,m)) = \max\{\nu_p(n), \nu_p(m)\}.$$

Since

$$\min\{a,b\} + \max\{a,b\} = a + b,$$

we get

$$\gcd(n,m)\mathrm{lcm}(n,m) = |nm|.$$

The extra absolute value is only to deal with the case where m or n is negative, as the p-adic valuations don't see the sign of an integer.

We end this section with an application to the irrationality of $\sqrt{2}$.

Proposition 2.13 *The equation $x^2 = 2y^2$ has no nonzero integer solutions. As a consequence, $\sqrt{2}$ is irrational.*

Proof: Suppose for a contradiction that a, b are nonzero integers such $a^2 = 2b^2$. We take ν_2 of both sides to get

$$2\nu_2(a) = 1 + 2\nu_2(b).$$

This is a contradiction because the LHS is an even integer while the RHS is an odd integer. □

Exercises

2.1 Prove that the equation $2^x = 3^y$ has no positive integer solutions. This implies that $\log_2 3$ is irrational.

2.2 Let p be a prime. Define $|r|_p$ for any nonzero $r \in \mathbb{Q}$ by $|r|_p = p^{-\nu_p(r)}$ and define $|0|_p = 0$. Then for any $r, s \in \mathbb{Q}$, prove that

(a) $|rs|_p = |r|_p|s|_p$,

(b) $|r + s|_p \leq \max\{|r|_p, |s|_p\} \leq |r|_p + |s|_p$.

In other words, $|.|_p$ behaves similar to the usual absolute value, and is called the p-adic absolute value.

2.3 Prove that the equation $x^3 = 2y^3 + 4z^3$ has no non-zero integer solutions.

Lecture 5 Fri 09/13
p-adic valuation of the binomial coefficients

3 Binomial coefficients

The number

$$L_n = \text{lcm}(1, 2, \ldots, n)$$

is closely related to the prime counting function.

We consider a seemingly unrelated question. What is the prime factorization of L_{69}?

$$L_{69} = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67.$$

Let p be any prime. Let k be a non-negative integer such that $p^k \leq n < p^{k+1}$. Then no integer from 1 to n is divisible by p^{k+1} and $p^k \leq n$ with $\nu_p(p^k) = k$. In other words

$$\nu_p(L_n) = \max\{\nu_p(1), \ldots, \nu_p(n)\} = k.$$

Now from $p^k \leq n < p^{k+1}$, we have

$$k \leq \log_p n < k + 1 \qquad \text{so} \qquad \nu_p(L_n) = k = \left\lfloor \frac{\log n}{\log p} \right\rfloor.$$

In this class, unless otherwise specified, log will be the natural log. We will prove that

$$2^n \leq L_n \leq 4^{n-1}$$

for $n \geq 7$. The actual growth rate of L_n is e^n. We can observe from the above formula for L_{69} that it is very close to just the product of all the primes less than 69.

Theorem 3.1 *(Prime number theorem) We have*

$$\lim_{n\to\infty} \frac{\log L_n}{n} = 1.$$

You might be more familiar with the Prime number theorem stated in terms of the prime counting function $\pi(x)$ which counts the number of primes less than or equal to x.

Theorem 3.2 *The Prime number theorem is equivalent to*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

Note that

$$\log L_n = \sum_{p\le n} \left\lfloor \frac{\log n}{\log p} \right\rfloor \log p.$$

Roughly speaking, most of the contribution will come from the primes p that are close to n, in which case $\log p \sim \log n$ and $\left\lfloor \frac{\log n}{\log p} \right\rfloor = 1$. So $\log L_n \sim \pi(n) \log n$. Making this precise requires some very careful estimates, which is too technical to fit the margins here.

To prove the bounds $2^n \le L_n \le 4^{n-1}$, we need to prove some results about binomial coefficients. We start with Legendre's formula.

Proposition 3.3 *For any prime p and any positive integer n,*

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Proof: For any $k \in \mathbb{N}$, let $u(k)$ denote the number of integers from 1 to n that are multiplies of p^k. Then $u(k) - u(k+1)$ is the number of integers from 1 to n with $\nu_p = k$. Then

$$\nu_p(n!) = (u(1) - u(2)) + 2(u(2) - u(3)) + 3(u(3) - u(4)) + \cdots = u(1) + u(2) + u(3) + \cdots .$$

We are done because $u(k) = \lfloor n/p^k \rfloor$. □

We recall the definition of the binomial coefficients

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n(n-1)\cdots(n-r+1)}{r!}$$

for $0 \le r \le n$. We define it to be 0 if $r < 0$ or if $r > n$. They have combinatoric interpretations as the number of ways to pick r objects from a collection of n objects.

Theorem 3.4 *(Binomial Theorem) We have the algebraic identity:*

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}.$$

Proof: When expanding a product of n terms of the form $x + y$, the coefficient of $x^r y^{n-r}$ is the number of ways to pick x a total of r times. □

Proof: Alternatively, prove by induction and Pascal's identity $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$. □

We care more about the p-adic valuation of the binomial coefficients:

Lemma 3.5 *Let $a, n \in \mathbb{N}$ and $m = 0, 1, \ldots, n$. Let n_a, m_a be the remainders when n, m are divided by a. Then*

$$\left\lfloor \frac{n}{a} \right\rfloor - \left\lfloor \frac{m}{a} \right\rfloor - \left\lfloor \frac{n-m}{a} \right\rfloor = \begin{cases} 1 & \text{if } n_a < m_a, \\ 0 & \text{if } n_a \ge m_a. \end{cases}$$

"Proof" by example: We note that

$$\frac{2024}{69} = 29 + \frac{23}{69}, \qquad \frac{420}{69} = 6 + \frac{6}{69}, \qquad \frac{145}{69} = 2 + \frac{7}{69}.$$

Then

$$\begin{aligned} \frac{2024-420}{69} &= 29 - 6 + \frac{23-6}{69} = 29 - 6 + \frac{17}{69} \\ \frac{420-145}{69} &= 6 - 2 + \frac{6-7}{69} = 6 - 2 - 1 + \frac{68}{69}. \end{aligned}$$

Proof: We have

$$\left\lfloor \frac{n}{a} \right\rfloor = \frac{n-n_a}{a}, \qquad \left\lfloor \frac{m}{a} \right\rfloor = \frac{m-m_a}{a}$$

and

$$\frac{n-m}{a} = \frac{n-n_a}{a} - \frac{m-m_a}{a} + \frac{n_a-m_a}{a} = \left\lfloor \frac{n}{a} \right\rfloor - \left\lfloor \frac{m}{a} \right\rfloor + \frac{n_a-m_a}{a}.$$

Since n_a, m_a are remainders, we know that $-1 < (n_a - m_a)/a < 1$. If $n_a \geq m_a$, then $(n_a - m_a)/a \in [0, 1)$ and so

$$\left\lfloor \frac{n-m}{a} \right\rfloor = \left\lfloor \frac{n}{a} \right\rfloor - \left\lfloor \frac{m}{a} \right\rfloor.$$

If $n_a < m_a$, then $(n_a - m_a)/a \in (-1, 0)$ and so

$$\left\lfloor \frac{n-m}{a} \right\rfloor = \left\lfloor \frac{n}{a} \right\rfloor - \left\lfloor \frac{m}{a} \right\rfloor - 1.$$

Hence we are done. □

Corollary 3.6 *Let $n \in \mathbb{N}$ and $r = 0, 1, \ldots, n$. Let p be a prime. Then*

$$0 \leq \nu_p\left(\binom{n}{r}\right) \leq \left\lfloor \frac{\log n}{\log p} \right\rfloor.$$

Proof: By Legendre's formula (Proposition 3.3), we have

$$\nu_p\left(\binom{n}{r}\right) = \sum_{k=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{r}{p^k} \right\rfloor - \left\lfloor \frac{n-r}{p^k} \right\rfloor.$$

By Lemma 3.5, each summand is either 0 or 1 and the number of terms in the sum is $\left\lfloor \frac{\log n}{\log p} \right\rfloor$. □

Lecture 5.5 (Tutorial) Fri 09/13
Lifting the Exponent

Our motivating example is: find

$$\nu_{11}(10^{11^{12}} + 12^{11^{10}}).$$

This question originated from the IMO 1991 shortlist, which asked for the largest integer k such that

$$1991^k \mid 1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

The method is essentially the same, with the extra twist that $1991 = 11 \times 181$. Note first that

$$\begin{aligned} 10^{11^{12}} &\equiv (-1)^{odd} \equiv -1 \pmod{11} \\ 12^{11^{10}} &\equiv 1 \pmod{11}. \end{aligned}$$

So the answer is at least 1. The first trick we use is

$$10^{11^{12}} = 10^{11^2 \cdot 11^{10}} = \left(10^{11^2}\right)^{11^{10}}.$$

Hence, we have

$$10^{11^{12}} + 12^{11^{10}} = \left(10^{11^2}\right)^{11^{10}} - \Big(-12\Big)^{11^{10}}.$$

Now we hit it with the hammer known as LTE.

Proposition 3.7 *(LTE, p odd) Let p be an odd prime and let a, b be integers such that $p \nmid a$, $p \nmid b$ and $p \mid a - b$. Let $n \in \mathbb{N}$. Then*

$$\nu_p(a^n - b^n) = \nu_p(a - b) + \nu_p(n).$$

Note that

$$10^{11^2} \equiv (-1)^{odd} \equiv -1 \equiv -12 \pmod{11}.$$

Hence we can apply LTE with $p = 11$, $a = 10^{11^2}$ and $b = -12$ to find that

$$\nu_{11}(a^{11^{10}} - b^{11^{10}}) = \nu_{11}(a - b) + \nu_{11}(11^{10}) = \nu_{11}(a - b) + 10.$$

What about $\nu_{11}(a - b)$? We use LTE again!

$$\nu_{11}(10^{11^2} - (-1)^{11^2}) = \nu_{11}(10 - (-1)) + 2 = 3.$$

Note that $(-1)^{11^2} = -1$. So

$$\nu_{11}(10^{11^2} - (-12)) = \nu_{11}(10^{11^2} - (-1)^{11^2} + 11) = 1.$$

Therefore, the answer is

$$\nu_{11}(10^{11^{12}} + 12^{11^{10}}) = 11.$$

Now let's prove LTE. First we note that it follows from the following two lemmas by induction.

Lemma 3.8 *Let p be a prime and let a, b be integers such that $p \nmid a$, $p \nmid b$. Let $n \in \mathbb{N}$ such that $p \nmid n$. Then*

$$\nu_p(a^n - b^n) = \nu_p(a - b).$$

Lemma 3.9 *Let p be an odd prime and let a, b be integers such that $p \nmid a$, $p \nmid b$ and $p \mid a - b$. Then*

$$\nu_p(a^p - b^p) = \nu_p(a - b) + 1.$$

Proof of Proposition 3.7 from Lemmas 3.8 and 3.9: We prove by induction on n. When $n = 1$, both sides equal $\nu_p(a - b)$, so it is true. Suppose now $n \geq 2$ and that $\nu_p(a^m - b^m) = \nu_p(a - b) + \nu_p(m)$ for all $m = 1, \ldots, n - 1$. Suppose first that $p \nmid n$. Then $\nu_p(n) = 0$ and we are done by Lemma 3.8:

$$\nu_p(a^n - b^n) = \nu_p(a - b) = \nu_p(a - b) + \nu_p(n).$$

Suppose now $p \mid n$. Let $m = n/p$. Then $1 \leq m \leq n - 1$. Then we know from the inductive hypothesis that $\nu_p(a^m - b^m) = \nu_p(a - b) + \nu_p(m) \geq \nu_p(a - b) \geq 1$. We can now apply Lemma 3.9 to a^m and b^m to get

$$\nu_p(a^{pm} - b^{pm}) = \nu_p(a^m - b^m) + 1.$$

Hence

$$\nu_p(a^n - b^n) = \nu_p(a^m - b^m) + 1 = \nu_p(a - b) + \nu_p(m) + 1 = \nu_p(a - b) + \nu_p(n).$$

Proof of Lemma 3.8: It suffices to prove that

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2}b + \cdots + b^{n-1}$$

is not divisible by p. Since $a \equiv b \pmod{p}$, we have

$$a^{n-1} + a^{n-2}b + \cdots + b^{n-1} \equiv b^{n-1} + b^{n-1} + \cdots + b^{n-1} \equiv nb^{n-1} \not\equiv 0 \pmod{p}$$

since $p \nmid b$ and $p \nmid n$. □

The following lemma is very important on its own!

Lemma 3.10 *Let p be a prime and let $r = 1, \ldots, p-1$. Then $p \mid \binom{p}{r}$ and $p^2 \nmid \binom{p}{r}$.*

Proof: In fact, we have

$$\nu_p\left(\binom{p}{r}\right) = \left\lfloor \frac{p}{p} \right\rfloor - \left\lfloor \frac{r}{p} \right\rfloor - \left\lfloor \frac{p-r}{p} \right\rfloor = 1 - 0 - 0 = 1.$$

Alternatively,

$$\binom{p}{r} = \frac{p(p-1)\cdots(p-r+1)}{r(r-1)\cdots 1}.$$

We see that there is a p in the numerator but no p in the denominator. So it will survive the division. □

Proof of Lemma 3.9: We write $a = b + p^k c$ where $k = \nu_p(a-b) \geq 1$ and $p \nmid c$. Then we expand

$$a^p = (b + p^k c)^p = b^p + pb^{p-1}p^k c + \sum_{r=2}^{p-1} \binom{p}{r} b^{p-r}(p^k c)^r + p^{kp}c^p.$$

Let's look at the p-adic valuation of each term. The b^p term gets cancelled when we take $a^p - b^p$. Since $p \nmid b$ and $p \nmid c$, we see that $\nu_p(pb^{p-1}p^k c) = k+1$. We now prove that the remaining terms all have p-adic valuation at least $k+2$. For $r = 2, \ldots, p-1$, we have

$$\nu_p\left(\binom{p}{r} b^{p-r}(p^k c)^r\right) = 1 + rk \geq 1 + 2k = 1 + k + k \geq 1 + k + 1 = k + 2$$

and since $p \geq 3$, we have

$$\nu_p(p^{kp}c^p) = kp \geq 3k = k + k + k \geq k + 1 + 1 = k + 2.$$

Therefore, we have $\nu_p(a^b - p^b) = k + 1 = \nu_p(a-b) + 1$ as desired. □

Where does this fail for $p = 2$? In this case, $\nu_p(p^{kp}c^p) = 2k$ could be $k+1$ when $k = 1$. In fact,

$$\nu_2(3^2 - 1^2) = \nu_2(8) = 3 = \nu_2(3-1) + 2.$$

Proposition 3.11 *(LTE, $p = 2$). Suppose a, b are odd and n is even. Then*

$$\nu_2(a^n - b^n) = \nu_2(a-b) + \nu_2(n) + \begin{cases} 0 & \text{if} \quad 4 \mid a-b, \\ 1 & \text{if} \quad 4 \nmid a-b. \end{cases}$$

Lecture 6 Mon 09/16

Lower bound for L_n

We now work towards the lower bound:

Theorem 3.12 *For any integer $n \geq 7$, we have*

$$L_n = \operatorname{lcm}(1, 2, \ldots, n) > 2^n.$$

Note that

$$\begin{aligned} L_6 &= 2^2 \cdot 3 \cdot 5 = 60 < 2^6 \\ L_7 &= 420 > 2^7 \\ L_8 &= 840 > 2^8. \end{aligned}$$

Lemma 3.13 *Let m, n be positive integers such that $1 \le m \le n$. Then $m\binom{n}{m} \mid L_n$*

Proof: Let p be any prime and let k be the unique non-negative integer such that $p^k \le n < p^{k+1}$. In other words, $k = \nu_p(L_n)$. It is enough to prove that

$$\nu_p\left(m\binom{n}{m}\right) \le k.$$

Let $\nu_p(m) = \ell \ge 0$. Then the remainders when m is divided by $p, p^2, \ldots, p^\ell$ are all 0. Hence, we have

$$\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{m}{p^j} \right\rfloor - \left\lfloor \frac{n-m}{p^j} \right\rfloor = 0 \qquad \text{if } j \le \ell.$$

Since it is also at most 1 for any $j = \ell + 1, \ldots, k$, we have

$$\nu_p\left(\binom{n}{m}\right) \le k - \ell.$$

Combining with $\nu_p(m) = \ell$ completes the proof. □

Exercise: Prove that

$$L_n = \operatorname{lcm}\left(1\binom{n}{1}, 2\binom{n}{2}, \ldots, n\binom{n}{n}\right).$$

Lemma 3.14 *Let m be a positive integer. Then $m(m+1)\binom{2m+1}{m} \mid L_{2m+1}$.*

Proof: Apply Lemma 3.13 to $n = 2m+1$ gives

$$m\binom{2m+1}{m} \mid L_{2m+1} \qquad \text{and} \qquad (m+1)\binom{2m+1}{m+1} \mid L_{2m+1}.$$

Since $\binom{2m+1}{m+1} = \binom{2m+1}{m}$ and $\gcd(m, m+1) = 1$, we have

$$\gcd\left(m\binom{2m+1}{m}, (m+1)\binom{2m+1}{m+1}\right) = \binom{2m+1}{m}\gcd(m, m+1) = \binom{2m+1}{m}.$$

So their lcm is $m(m+1)\binom{2m+1}{m}$ and it divides L_{2m+1}. □

Lemma 3.15 *Let m be a positive integer. Then*

$$\frac{4^m}{m+1} < \binom{2m+1}{m} < 4^m \qquad \textit{and} \qquad \frac{4^m}{2m+1} < \binom{2m}{m} < 4^m.$$

Proof: Note the formula

$$2^{2m+1} = \sum_{r=0}^{2m+1} \binom{2m+1}{r} \qquad \text{and} \qquad 2^{2m} = \sum_{r=0}^{2m} \binom{2m}{r}.$$

Note also that $\binom{2m+1}{m} = \binom{2m+1}{m+1}$ is the largest binomial coefficient of the form $\binom{2m+1}{r}$, and $\binom{2m}{m}$ is the largest binomial coefficient of the form $\binom{2m}{r}$. Hence we have

$$2\binom{2m+1}{m} < \sum_{r=0}^{2m+1} \binom{2m+1}{r} = 2 \cdot 4^m < (2m+2)\binom{2m+1}{m}$$

and

$$\binom{2m}{m} < \sum_{r=0}^{2m} \binom{2m}{r} = 4^m < (2m+1)\binom{2m}{m}.$$

Dividing by $\binom{2m+1}{m}$ and $\binom{2m}{m}$ respectively gives the desired inequalities. □

Remark: From the Stirling's approximation

$$m! \sim \sqrt{2\pi m}\left(\frac{m}{e}\right)^m,$$

we can get the more precise estimate

$$\binom{2m}{m} \sim \frac{4^m}{\sqrt{\pi m}}.$$

Proof of Theorem 3.12: Suppose first $n = 2m+1$ is odd, with $m \geq 3$. By Lemma 3.14 and Lemma 3.15, we have

$$L_{2m+1} \geq m(m+1)\binom{2m+1}{m} > m4^m > 2 \cdot 4^m = 2^{2m+1}.$$

Suppose now $n = 2m+2$ is even. We have already checked $L_8 > 2^8$ explicitly. So we may assume $n \geq 10$ and so $m \geq 4$. Then once again,

$$L_{2m+2} \geq L_{2m+1} > m4^m \geq 4 \cdot 4^m = 2^{2m+2}.$$

Lecture 7 Wed 09/18

Upper bound of L_n, Bertrand postulate

We now prove the upper bound:

Theorem 3.16 *For any $n \in \mathbb{N}$, we have*

$$L_n = \operatorname{lcm}(1, 2, \ldots, n) \leq 4^{n-1}.$$

This implies Erdös' bound

$$\prod_{p \leq n} p \leq L_n \leq 4^{n-1}.$$

Proof: We will prove by induction on n. The base case $n = 1$ is clear since $L_1 = 1 = 4^{1-1}$. Suppose now $n \geq 2$ and that $L_k \leq 4^{k-1}$ for every $k = 1, \ldots, n-1$. Suppose first that $n = 2m$ is even. Note that L_n can only be different from L_{n-1} when n is a power of a prime p in which case $L_n/L_{n-1} = p$. Since n is even, we see that either $L_n = L_{n-1}$ when n is not a power of 2 or $L_n = 2L_{n-1}$ when n is a power of 2. In both cases,

$$L_n \leq 2L_{n-1} \leq 2 \cdot 4^{n-2} \leq 4^{n-1}$$

by induction. Suppose now $n = 2m+1$ is odd. We note that the desired result follows from

$$L_{2m+1} \mid L_{m+1}\binom{2m+1}{m}$$

because then

$$L_{2m+1} \leq L_{m+1}\binom{2m+1}{m} < 4^m \cdot 4^m = 4^{2m}$$

by induction.

Let p be any prime. It suffices to prove that

$$\nu_p(L_{2m+1}) - \nu_p(L_{m+1}) \le \nu_p\left(\binom{2m+1}{m}\right).$$

"Proof" by example: Let's prove

$$\nu_2(L_{139}) - \nu_2(L_{70}) \le \nu_2\left(\binom{139}{69}\right).$$

From

$$64 \le 70 < 128 \le 139 < 256,$$

we have

$$\nu_2(L_{139}) - \nu_2(L_{70}) = 7 - 6 = 1.$$

On the other hand,

$$\nu_2\left(\binom{139}{69}\right) \ge \left\lfloor \frac{139}{128} \right\rfloor - \left\lfloor \frac{69}{128} \right\rfloor - \left\lfloor \frac{70}{128} \right\rfloor = 1 = \nu_2(L_{139}) - \nu_2(L_{70}).$$

As another example, let's prove

$$\nu_7(L_{139}) - \nu_7(L_{70}) \le \nu_7\left(\binom{139}{69}\right).$$

In this case, we have

$$49 \le 70 < 139 < 343,$$

so we have

$$\nu_7(L_{139}) - \nu_7(L_{70}) = 2 - 2 = 0 \le \nu_7\left(\binom{139}{69}\right).$$

These two examples illustrate the only 2 possibilities:

$$p^k \le m+1 < p^{k+1} \le 2m+1 < p^{k+2}, \qquad \text{or} \qquad p^k \le m+1 < 2m+1 < p^{k+1}.$$

In the first case,

$$\nu_p(L_{m+1}) = k \qquad \text{and} \qquad \nu_p(L_{2m+1}) = k+1$$

while

$$\nu_p\left(\binom{2m+1}{m}\right) \ge \left\lfloor \frac{2m+1}{p^{k+1}} \right\rfloor - \left\lfloor \frac{m+1}{p^{k+1}} \right\rfloor - \left\lfloor \frac{m}{p^{k+1}} \right\rfloor \ge 1 - 0 - 0 = 1.$$

In the second case,

$$\nu_p(L_{m+1}) = \nu_p(L_{2m+1}) = k, \qquad \text{so} \qquad \nu_p(L_{2m+1}) - \nu_p(L_{m+1}) = 0 \le \nu_p\left(\binom{2m+1}{m}\right).$$

Finally we note that

$$2m+1 < 2(m+1) < 2p^{k+1} \le p^{k+2}.$$

Hence, it is not possible for $2m+1 \ge p^{k+2}$. □

We now work towards proving Bertrand's postulate, that there is always a prime between n and $2n$. I will prove that there is a prime between 1012 and 2024 and leave it to you (HW 3) to translate this into a proper proof.

From Lemma 3.15 with $m = 1012$, we have

$$\frac{4^{1012}}{2025} \le \binom{2024}{1012}.$$

We consider the prime factorization of $\binom{2024}{1012}$. For any prime p, recall we have the bound (Corollary 3.6):

$$\nu_p\left(\binom{2024}{1012}\right) \leq \left\lfloor \log_p(2024) \right\rfloor.$$

In particular, no prime $p > 2024$ can divide it; and if $p > \sqrt{2024} \simeq 45$, then $\log_p(2024) < 2$ and so

$$\nu_p\left(\binom{2024}{1012}\right) \leq 1.$$

We want to be more precise on when it is 0 or 1. Suppose now $p > \sqrt{2024}$. Then

$$\nu_p\left(\binom{2024}{1012}\right) = \left\lfloor \frac{2024}{p} \right\rfloor - 2\left\lfloor \frac{1012}{p} \right\rfloor.$$

Note that if $1012 < p \leq 2024$ (which is the range we really care about), then

$$1 \leq \frac{2024}{p} < 2, \qquad \frac{1012}{p} < 1 \qquad \Longrightarrow \qquad \nu_p\left(\binom{2024}{1012}\right) = \left\lfloor \frac{2024}{p} \right\rfloor - 2\left\lfloor \frac{1012}{p} \right\rfloor = 1 - 2 \cdot 0 = 1.$$

On the other hand, if $2024/3 < p \leq 1012$, then

$$2 \leq \frac{2024}{p} < 3, \qquad 1 \leq \frac{1012}{p} < \frac{3}{2} \qquad \Longrightarrow \qquad \nu_p\left(\binom{2024}{1012}\right) = \left\lfloor \frac{2024}{p} \right\rfloor - 2\left\lfloor \frac{1012}{p} \right\rfloor = 2 - 2 \cdot 1 = 0.$$

Putting these together, we have

$$\begin{aligned}
\frac{4^{1012}}{2025} \leq \binom{2024}{1012} &= \prod_{p \leq 2024} p^{\nu_p\left(\binom{2024}{1012}\right)} \\
&\leq \prod_{p \leq \sqrt{2024}} p^{\log_p(2024)} \prod_{\sqrt{2024} < p \leq 2024/3} p^1 \prod_{1012 < p \leq 2024} p \\
&= \prod_{p \leq \sqrt{2024}} 2024 \cdot \prod_{p \leq 2024/3} p \cdot \prod_{1012 < p \leq 2024} 2024 \\
&\leq 2024^{\sqrt{2024} + \pi(2024) - \pi(1012)} \cdot 4^{2024/3 - 1}.
\end{aligned}$$

Rearranging gives

$$\pi(2024) - \pi(1012) \geq \log_{2024}(4^{1012 - 2024/3 + 1}/2025) - \sqrt{2024} \simeq 15.62.$$

In HW 3, you will prove that

$$\pi(2n) - \pi(n) \geq \frac{(n/3+1)\log 4 - \log(2n+1)}{\log 2n} - \sqrt{2n}.$$

Using a bit of calculus and computer aids, one finds that this lower bound is positive for $n \geq 459$. For $n < 459$, we can verify that $\pi(2n) - \pi(n) > 0$ directly using the primes $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$. This concludes the proof of Bertrand's postulate.

Theorem 3.17 *(Bertrand's postulate) For any positive integer n, there is a prime $p \in (n, 2n]$.*

Exercises

3.1 Prove that for every prime $p \neq 3$, there exists a positive integer n, an integer $a = 0, 1$ and an integer $b = 0, 1, \ldots, n-1$ such that $p = n^2 + an + b$.

3.2 How many 0's does the number 40! ends in?

Challenge Question: Can you figure out what the last nonzero digit of 40! is?

3.3 Prove that for any $n \in \mathbb{N}$ and any prime p, we have $\nu_p(n!) < n/(p-1)$.

3.4 Prove that for any $n \in \mathbb{N}$, if $n \mid \binom{n}{m}$ for all $m = 1, \ldots, n-1$, then n is a prime.

3.5 According to the Prime number theorem, we know that $L_n \sim e^n$. Prove (without using the PNT) that for any $\alpha > 0$, we have $L_n \geq 4^{n-\alpha}$ for n sufficiently large (depending on α). You may use the better asympototic for the binomial coefficient from Sterling's formula.

3.6 Use Exercise 3.3 to conclude that

$$\sum_p \frac{\log p}{p-1} \to \infty.$$

With a little bit more effort, one can prove that

$$\sum_{p \leq n} \frac{\log p}{p} = \log n + O(1).$$

In other words, there exists an absolute constant $C > 0$ such that for any $n \in \mathbb{N}$,

$$\left| \sum_{p \leq n} \frac{\log p}{p} - \log n \right| \leq C.$$

Lecture 8 Fri 09/20

Infinitude of primes of the form $4k+1$, $4k+3$

4 Euclid's proof of the infinitude of primes

Before all of these fancy results on the prime counting function, the very first proof of the infinitude of primes was due to Euclid. Here is another way to think about the proof. The key ideas are as follows:

(a) Every integer $n \geq 2$ has a prime divisor.

(b) Construct an infinite sequence of pairwise coprime integers at least 2.

The sequence constructed from Euclid's proof is $a_1 = 2$ and

$$a_{n+1} = a_1 a_2 \cdots a_n + 1, \qquad \text{for } n \geq 1.$$

Then for $i < j$, we have $a_i \mid a_1 a_2 \cdots a_{j-1}$ and so $\gcd(a_i, a_j) = \gcd(a_i, 1) = 1$.

Alternatively, if we take a_1 odd and use $a_{n+1} = a_1 \cdots a_n + 2$, we also have $\gcd(a_i, a_j) = \gcd(a_i, 2) = 1$ since each a_i is odd. This sequence is actually a very famous one!

Proposition 4.1 *The sequence defined by $F_0 = 3$ and*

$$F_{n+1} = F_0 F_1 \cdots F_n + 2, \qquad \textit{for } n \geq 0$$

is the sequence of Fermat numbers $F_n = 2^{2^n} + 1$.

Proof: It suffices to prove that $F_n = 2^{2^n} + 1$ satisfies the recursion formula. This follows from an induction exercise. □

There is a more general result on the infinitude of primes satisfying congruence conditions. Recall that $a \equiv b \pmod{m}$ means that $m \mid a - b$, or equivalently that a and b have the same remainder when divided by m. Since numbers congruent to a mod m form an arithmetic progression, this result is also referred to as the infinitude of primes in arithmetic progressions. It marks the beginning of modern analytic number theory.

Theorem 4.2 *(Dirichlet) Let a, m be coprime positive integers. Then there are infinitely many primes $p \equiv a \pmod{m}$.*

We now know (Siegel-Walfisz) that there are an equal number of them, asymptotically, over all possible congruence classes. More precisely, if $p \equiv a \pmod{m}$, then $\gcd(p, m) = \gcd(a, m)$. If p is prime large enough to not divide m, then $\gcd(p, m) = 1$. The number of integers $a = 1, \ldots, m$ such that $\gcd(a, m) = 1$ is $\phi(m)$, the Euler-ϕ (or the Euler-Totient) function of m. Then

$$\lim_{x \to \infty} \frac{\#\text{ primes } p \leq x, p \equiv a \pmod{m}}{x/\log x} = \frac{1}{\phi(m)}.$$

We can give an Euclid's type proof for this result in some special cases.

Primes $\equiv 3 \pmod{4}$

We modify the key idea of Euclid's proof to:

(a) Every integer $n \geq 2$ of the form $4k + 3$ has a prime divisor that is congruent to 3 mod 4..

(b) Construct an infinite sequence of pairwise coprime integers at least 2 that are of the form $4k + 3$.

Property (a) follows because products of numbers of the form $4k + 1$ are still of the form $4k + 1$. In terms of congruences, we can say that if $a \equiv 1 \pmod{4}$ and $b \equiv 1 \pmod{4}$, then $ab \equiv 1 \pmod{4}$. Hence a number of the form $4k + 3$ has a prime divisor that is not of the form $4k + 1$. Since it can't be divisible by 2, primes of the form $4k + 3$ are the only possibilities left. For the sequence in (b), we take $a_1 = 7$ and

$$a_{n+1} = 4(a_1 \cdots a_n) + 3.$$

Then first one proves by induction that $\gcd(a_i, 3) = 1$ for all $i \geq 1$. Then similar to before, for $i < j$,

$$\gcd(a_i, a_j) = \gcd(a_i, 3) = 1.$$

The same idea also works for primes of the form $3k + 2$ and primes of the form $6k + 5$ because $\phi(3) = \phi(6) = 2$ so that if not all the prime divisors are of the form $3k + 1$ (resp. $6k + 1$), and it is not divisible by 3 (resp. 2 or 3), then it has a prime divisor of the form $3k + 2$ (resp. $6k + 5$).

Primes $\equiv 1 \pmod{4}$

This is a bit trickier. Let p be an odd prime. We consider the congruence equation

$$x^2 \equiv -1 \pmod{p}.$$

Suppose it has a solution $x = a$. Then clearly $p \nmid a$ for if otherwise, we would have $a^2 \equiv 0$. So by Fermat's little Theorem,

$$a^{p-1} \equiv 1 \pmod{p}.$$

On the other hand,

$$a^{p-1} = (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}.$$

Since p is an odd prime, we see that

$$1 \equiv (-1)^{(p-1)/2} \pmod{p} \quad \Rightarrow \quad 1 = (-1)^{(p-1)/2} \quad \Rightarrow \quad p \equiv 1 \pmod{4}.$$

In other words, if p is an odd prime divisor of an integer of the form $n^2 + 1$, then $p \equiv 1 \pmod{4}$. By taking $4n^2 + 1$ instead, we remove the possibility of $p = 2$. So we have:

(a) Every integer $n \geq 2$ of the form $4k^2 + 1$ has a prime divisor that is congruent to 1 mod 4.

(b) Construct an infinite sequence of pairwise coprime integers at least 2 that are of the form $4k^2+1$.

To construct our sequence, we take $a_1 = 5$ and

$$a_{n+1} = 4(a_1 \cdots a_n)^2 + 1.$$

Lecture 8.5 (Tutorial) Fri 09/20

Order of a mod m

The crucial idea here is that if $a^2 \equiv -1 \pmod{p}$, then

$$a^4 \equiv 1 \pmod{p}$$

but

$$a^3 \equiv -a \not\equiv 1 \pmod{p}, \qquad a^2 \equiv -1 \not\equiv 1 \pmod{p}, \qquad a \not\equiv 1 \pmod{p}.$$

We define the order of an integer a mod m, where $\gcd(a,m) = 1$, denoted $o_m(a)$, to be the smallest positive integer d such that $n^d \equiv 1 \pmod{m}$. In this case, we have $o_p(a) = 4$.

As another example, recall from the first tutorial:

$$\begin{aligned} 10 &\equiv 3 \pmod{7} \\ 10^2 &\equiv 2 \pmod{7} \\ 10^3 &\equiv 6 \pmod{7} \\ 10^4 &\equiv 4 \pmod{7} \\ 10^5 &\equiv 5 \pmod{7} \\ 10^6 &\equiv 1 \pmod{7} \end{aligned}$$

This means that 6 is the smallest positive integer such that $10^d \equiv 1 \pmod{7}$. Hence $o_7(10) = 6$. Simiarly, recall that $10^3 \equiv -1 \pmod{13}$ and $10^6 \equiv 1 \pmod{13}$. This implies that $o_{13}(10) = 6$.

What about $o_{49}(2)$? First, we note that $o_7(2) = 3$ since 2 and 4 are not 1 mod 7 but 8 is. Write $d = o_{49}(2)$. Then

$$2^d \equiv 1 \pmod{49}.$$

We have $2^d \equiv 1 \pmod{7}$ as well. We divide d by 3 to write $d = 3q + r$ for some integers q, r with $r = 0, 1, 2$. Then

$$2^d = 2^{3q+r} = (2^3)^q 2^r \equiv 1^q 2^r \equiv 2^r \pmod{7}.$$

So $2^r \equiv 1 \pmod{7}$. However, $r = 0, 1, 2$ so this is only possible if $r = 0$. So at least we know $3 \mid d$. We have just given a "proof" by example for the following very important result.

Proposition 4.3 *Let a, m be coprime integers. Suppose $n \in \mathbb{N}$ with $a^n \equiv 1 \pmod{m}$. Then $o_m(a) \mid n$.*

Proof: Note that $o_m(a) \leq n$. Apply the division algorithm to get integers s, t such that $n = o_m(a)s + t$ where $0 \leq t < o_m(a)$ and $s \geq 0$. Then

$$a^t \equiv a^t (a^{o_m(a)})^s = a^{t + o_m(a)s} = a^n \equiv 1 \pmod{m}.$$

Hence it follows from the minimality of $o_m(a)$ that $t = 0$. Therefore, $o_m(a) \mid n$. □

Returning to our task of finding $d = o_{49}(2)$, we know $d = 3q$ and need

$$\nu_7(2^d - 1) \geq 2.$$

We know that $\nu_7(2^3 - 1) = 1$. Is there a way to increase the valuation by "lifting the exponent"? Using LTE (Proposition 3.7) with $a = 2^3$, $b = 1$ and $p = 7$, we have

$$\nu_7(2^{3q} - 1) = \nu_7(2^3 - 1) + \nu_7(q) = 1 + \nu_7(q).$$

The smallest q to make this at least 2 is $q = 7$. Hence $o_{49}(2) = 21$.

Exercise: Prove that for any $k \geq 1$, we have $o_{7^k}(2) = 3 \cdot 7^{k-1}$.

Corollary 4.4 *Let p be a prime and let $a \in \mathbb{Z}$ such that $p \nmid a$. Then $o_p(a) \mid p-1$. In other words,*

$$p \equiv 1 \pmod{o_p(a)}.$$

Proof: Follows immediately from Proposition 4.3 and Fermat's little theorem $a^{p-1} \equiv 1 \pmod{p}$. □

Lemma 4.5 *Let p be a prime and let $a \in \mathbb{Z}$ such that $p \nmid a$. Then $o_p(a) = p-1$ if and only if $a, a^2, \ldots, a^{p-1}$ are all distinct mod p. In this case, we say a is primitive mod p.*

Proof: Since $p \nmid a$, we have $\gcd(p, a^i) = 1$ for any positive integer i. Let $1 \leq i < j \leq p-1$ be positive integers. Then

$$a^i \equiv a^j \pmod{p} \iff a^{j-i} \equiv 1 \pmod{p}.$$

Hence $a, a^2, \ldots, a^{p-1}$ are all distinct mod p if and only if $a^n \not\equiv 1 \pmod{p}$ for all $n = 1, \ldots, p-2$ if and only if $o_p(a) = p-1$. □

Calling back to Tutorial 1, we now know that for a prime p, the numbers $1/p, 2/p, \ldots, (p-1)/p$ have the cyclic structure if and only if 10 is primitive mod p. We will be able to prove later (after quadratic reciprocity):

Proposition 4.6 *Let $p = 2^{2^n} + 1$ be a Fermat prime at least 17 (i.e., $n \geq 2$). Then 10 is primitive mod p.*

We can generalize the notion of primitive to composite modulus m. Now there are $\phi(m)$ possible coprime values mod m. We say a is primitive mod m if $o_m(a) = \phi(m)$. We will be able to classify for which m does a primitive element mod m exist later. For example, they always exist if $m = p$ is a prime. On the other hand,

$$o_8(1) = 1 \qquad \text{and} \qquad o_8(3) = o_8(5) = o_8(7) = 2, \qquad \text{but} \qquad \phi(8) = 4.$$

Our next goal is to prove the infinitude of primes $\equiv 1 \pmod{m}$ for some fixed $m \geq 2$. In light of Corollary 4.4, we need to find some criterion that p has to satisfy in order for there to exist some $a \in \mathbb{Z}$ with $o_p(a) = m$. In the case $m = 4$, we saw that if $a^2 \equiv -1 \pmod{p}$, then $o_p(a) = 4$. So by using the polynomial $f(x) = x^2 + 1$, we see that if p is an odd prime divisor of $f(a)$, then $o_p(a) = 4$ and so $p \equiv 1 \pmod{4}$.

Our next task is: For any $m \geq 2$, find a polynomial $f(x)$ with coefficients in $\mathbb{Z}$ such that if $p \mid f(a)$, then $o_p(a) = m$ and so $p \equiv 1 \pmod{m}$.

Lecture 9 Mon 09/23
$\Phi_m(x)$

Primes $\equiv 1 \pmod{q}$ where q is a prime

Suppose now a is an integer such that $a^q \equiv 1 \pmod{p}$ and $a \not\equiv 1 \pmod{p}$. Then $o_p(a) \mid q$ and $o_p(a) \neq 1$. So $o_p(a) = q$ and $q \mid p-1$. In terms of division, we have

$$p \mid a^q - 1, \qquad p \nmid a - 1.$$

So p divides the quotient $a^{q-1} + a^{q-2} + \cdots + 1$. We define the q-th **cyclotomic polynomial** to be

$$\Phi_q(x) = \frac{x^q - 1}{x - 1} = x^{q-1} + x^{q-2} + \cdots + 1.$$

Proposition 4.7 *Let q be an odd prime. If p is a prime divisor of $\Phi_q(a)$ for some integer a, then $p \equiv 1 \pmod{q}$ or $p = q$.*

Proof: Since $\Phi_q(a) \mid a^q - 1$, we have $p \mid a^q - 1$. So $o_p(a) \mid q$ by Proposition 4.3. If $o_p(a) = 1$, then $a \equiv 1 \pmod{p}$ and

$$\Phi_q(a) \equiv 1^{q-1} + \cdots + 1 \equiv q \pmod{p},$$

which implies that $p \mid q$ and so $p = q$. If $o_p(a) = q$, then we have $p \equiv 1 \pmod{q}$ by Corollary 4.4. □

We can remove the possibility of $p = q$ by taking $\Phi_q(qa) = 1 + qa(\cdots)$. Note that

$$\gcd(a, \Phi_q(qa)) = \gcd(a, 1 + qa(\cdots)) = \gcd(a, 1) = 1.$$

Then we take the sequence $a_1 = \Phi_q(q)$ and

$$a_{n+1} = \Phi_q(qa_1a_2 \cdots a_n).$$

Then:

(a) Each $a_n \geq 2$ and any prime divisor of a_n is $\equiv 1 \pmod{q}$;

(b) The a_n's are pairwise coprime.

Therefore, we get infinitely many primes $\equiv 1 \pmod{q}$.

Exercises

4.1 Use the polynomial $n^2 + 4$, and a small modification, to prove that there are infinitely many primes of the form $8k + 5$.

4.2 Let $h(x)$ is a polynomial with integer coefficients with $h(0) = 1$. Prove that the sequence defined by $a_1 = 1$ and $a_{i+1} = h(a_1a_2 \cdots a_i)$ for $i \geq 1$, consists of pairwise coprime integers.

4.3 Let $h(x) = ax + b$ where a, b are coprime integers. Prove that the sequence defined by $a_1 = 1$ and $a_{i+1} = h(a_1a_2 \cdots a_i)$ for $i \geq 1$, consists of pairwise coprime integers.

4.4 Prove that there does not exist a non-constant polynomial $h(x)$ with integer coefficients such that $h(n)$ is a prime for all integers n.

4.5 Prove that $2^{2^n} - 1$ has at least $n + 1$ distinct prime divisors when $n \geq 6$.

4.6 Prove that $\phi(m)$ is even for any integer $m \geq 3$. (Note that $\phi(1) = \phi(2) = 1$.)

4.7 Let $q > 3$ be a prime. Prove that there does not exist integers x, y such that $x^{q-1} + \cdots + x + 1 = y^{q-2} - 1$.

5 Cyclotomic polynomials and primes $\equiv 1 \pmod{m}$

Suppose now m is a positive integer, that is not necessarily a prime. We want to prove that there are infinitely many primes $\equiv 1 \pmod{m}$. Recall that our strategy: find a polynomial $f(x)$ with coefficients in $\mathbb{Z}$ such that if $p \mid f(a)$, then $o_p(a) = m$ and so $p \equiv 1 \pmod{m}$.

Let's try some small values to see what they should be. When $m = 6$, we should remove solutions to $x^2 - 1$, as they have order dividing 2, and $x^3 - 1$, as they have order dividing 3, but

$$\frac{x^6 - 1}{(x^2 - 1)(x^3 - 1)} = \frac{x^6 - 1}{x^5 - x^3 - x^2 + 1}$$

isn't a polynomial. The problem is that when we remove the solutions to $x^2 - 1$, we have already removed the solution to $x - 1$, so we shouldn't remove it again from $x^3 - 1$. In other words, we should take

$$\Phi_6(x) = \frac{x^6 - 1}{(x^2 - 1)\big((x^3 - 1)/(x - 1)\big)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1.$$

What about something more complicated like $\Phi_{105}(x)$? Using the same "inclusion-exclusion sieve", we should take

$$\Phi_{105}(x) = \frac{(x^{105}-1)(x^3-1)(x^5-1)(x^7-1)}{(x^{15}-1)(x^{21}-1)(x^{35}-1)(x-1)} = x^{48} + \cdots - 2x^{41} + \cdots + 1.$$

It seems quite random that it is actually a polynomial. We need a better definition that is easier to work with. One thing to note is that we seem to have forgotten about the prime p. So let's forget it completely and think in $\mathbb{C}$.

We define the order $o(z)$ of some complex number $z \in \mathbb{C}$ similarly as the smallest positive integer d such that $z^d = 1$, if it exists. For example, $o(i) = 4$. What are all the complex numbers z with $o(z) = 4$? They must be roots of $x^4 = 1$, which are ± 1 and $\pm i$. We have $o(1) = 1$, $o(-1) = 2$, $o(\pm i) = 4$. The polynomial $x^2 + 1$ that we used to prove the infinitude of primes $\equiv 1 \pmod 4$ factors as

$$x^2 + 1 = (x - i)(x - (-i)).$$

Let's try this with an arbitrary $m \geq 2$. What are all the complex numbers z with $o(z) = m$? They must be roots of $x^m = 1$, which are given by ζ_m^k for $k = 1, 2, \ldots, m$ where $\zeta_m = e^{2\pi i/m}$. In HW4, you will prove that

$$o(\zeta_m^k) = \frac{m}{\gcd(m,k)}.$$

I will give a "proof" by example. Let's find $o(\zeta_{2024}^{69})$. That is, we want the smallest positive integer d such that $\zeta_{2024}^{69d} = 1$. Note that

$$\zeta_{2024}^{69d} = 1 \iff e^{2\pi i \frac{69d}{2024}} = 1 \iff \frac{69d}{2024} \in \mathbb{Z} \iff 2024 \mid 69d \iff 88 \mid 3d.$$

Here $88 = 2024/23$ and $3 = 69/23$. Since $\gcd(88, 3) = 1$, we have $88 \mid 3d$ if and only if $88 \mid d$ by Corollary 1.11. So the smallest positive d is 88.

We see now that $o(\zeta_m^k) = m$ if and only if $\gcd(k, m) = 1$. We define the m-th cyclotomic polynomial $\Phi_m(x)$ as

$$\Phi_m(x) = \prod_{\substack{1 \leq k \leq m \\ \gcd(k,m)=1}} (x - \zeta_m^k) = \prod_{o(z)=m} (x - z).$$

For example, we can write down the first few $\Phi_m(x)$:

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= (x - \zeta_3)(x - \zeta_3^2) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1 \\
\Phi_4(x) &= (x - i)(x + i) = x^2 + 1 \\
\Phi_5(x) &= (x - \zeta_5)(x - \zeta_5^2)(x - \zeta_5^3)(x - \zeta_5^4) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= (x - \zeta_6)(x - \zeta_6^5) = x^2 - x + 1 \\
\Phi_7(x) &= \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.
\end{aligned}$$

Note that $\zeta_6^2 = \zeta_3$ and $\zeta_6^3 = \zeta_2 = -1$, we have

$$\begin{aligned}
x^6 - 1 &= (x - \zeta_6)(x - \zeta_6^2)(x - \zeta_6^3)(x - \zeta_6^4)(x - \zeta_6^5)(x - \zeta_6^6) \\
&= (x - \zeta_6)(x - \zeta_6^5)(x - \zeta_3)(x - \zeta_3^2)(x + 1)(x - 1) \\
&= \Phi_6(x)\, \Phi_3(x)\, \Phi_2(x)\, \Phi_1(x).
\end{aligned}$$

This is not a coincidence!

Proposition 5.1 *Let $m \in \mathbb{N}$. We have the factorization*

$$x^m - 1 = \prod_{d|m} \Phi_d(x).$$

Proof: By the definition of the cyclotomic polynomials, we have

$$\prod_{d|m} \Phi_d(x) = \prod_{d|m} \prod_{o(z)=d} (x - z) = \prod_{o(z)|m} (x - z).$$

On the other hand, if $z \in \mathbb{C}$ such that $o(z) \mid m$, then $z^m = 1$; and if $z^m = 1$, then $o(z) \mid m$ (by writing $z = \zeta_m^k$ and using the above, or by using an argument similar to the proof of Proposition 4.3). In other words, the complex numbers with order m are exactly the roots of $x^m - 1$, which are all distinct. Hence we have

$$x^m - 1 = \prod_{o(z)=m} (x - z) = \prod_{d|m} \Phi_d(x)$$

as desired. □

Corollary 5.2 *Let $m \in \mathbb{N}$. Then $m = \sum_{d|m} \phi(d)$.*

Proof: Take degrees, noting that $\deg(\Phi_d(x))$ is the number of $k = 1, 2, \ldots, d$ such that $\gcd(k, d) = 1$ and so $\deg(\Phi_d(x)) = \phi(d)$. □

Corollary 5.3 *Let $m \in \mathbb{N}$. Then $\Phi_m(x)$ is a polynomial with integer coefficients. Moreover, $\Phi_1(0) = -1$ and $\Phi_m(0) = 1$ for $m \geq 2$.*

Proof: We prove by induction on m. We have $\Phi_1(x) = x - 1$. Suppose now $m \geq 2$. We know that

$$x^m - 1 = \Phi_m(x) \cdot \Phi_1(x) \prod_{\substack{d|m \\ 1<d<m}} \Phi_d(x) = \Phi_m(x) \cdot (x - 1) \prod_{\substack{d|m \\ 1<d<m}} \Phi_d(x).$$

By induction, each of the $\Phi_d(x)$ for $d < m$ is a monic polynomial with integer coefficient and so is their product. Therefore, so is the quotient of $x^m - 1$ by it by long division of polynomials. Also by induction, we have $\Phi_d(0) = 1$ for $1 < d < m$. So setting $x = 0$ gives $\Phi_m(0) = 1$. □

Remark: There is a more direct proof of $\Phi_m(0) = 1$ for $m > 2$. Let S be the set of integers $1 \leq j < m/2$ that are coprime to m. Then the set of integers $m/2 < k \leq m$ coprime to m are all of the form $m - j$ for some $j \in S$. If $m/2$ is an integer, then it is at least 2 and divides m, so it is not coprime to m. Now

$$\Phi_m(0) = \prod_{j \in S} (-\zeta_m^j)(-\zeta_m^{m-j}) = 1.$$

Lecture 10 Wed 09/25

Division properties of $\Phi_m(x)$

Proposition 5.4 *Let $m \in \mathbb{N}$ and let $n > 1$ be an integer coprime to m. Let $a \in \mathbb{Z}$ with $n \mid \Phi_m(a)$. Then $o_n(a) = m$.*

Proof: We write $x^m - 1$ as $F(x)\Phi_m(x)$ where $F(x) \in \mathbb{Z}[x]$ is the product of $\Phi_d(x)$ over all positive integers $d \mid m$ with $d < m$. Then $\Phi_m(a) \mid a^m - 1$ and we have $n \mid a^m - 1$. Hence $o_n(a) \mid m$. Suppose for a contradiction

that $\ell := o_n(a) < m$. Then we have $n \mid a^\ell - 1$. Since $\ell \mid m$ and $\ell < m$, we know that any divisor of ℓ is a divisor of m and is less than m. In other words,

$$F(x) = \prod_{d \mid \ell} \Phi_d(x) \cdot \prod_{\substack{d \mid m \\ d < m \\ d \nmid \ell}} \Phi_d(x) = (x^\ell - 1)G(x)$$

for some $G(x) \in \mathbb{Z}[x]$. We thus have the factorization

$$a^m - 1 = (a^\ell - 1)\Phi_m(a)G(a).$$

Fix some prime p dividing n, which exists since $n > 1$. From $p \mid n$ and $n \mid \Phi_m(a)$, we have $p \mid \Phi_m(a)$ and so

$$\nu_p(a^m - 1) = \nu_p(a^\ell - 1) + \nu_p(\Phi_m(a)) + \nu_p(G(a)) > \nu_p(a^\ell - 1).$$

Since $\ell \mid m$, we write $m = \ell k$ for some positive integer k. Since n and m are coprime, we have $p \nmid k$. Hence by LTE (Lemma 3.8) and $p \mid a^\ell - 1$, we have $\nu_p(a^m - 1) = \nu_p(a^\ell - 1)$. Contradiction. □

Corollary 5.5 *Let $m \in \mathbb{N}$. Let $a \in \mathbb{Z}$. Let p be any prime divisor of $\Phi_m(a)$. Then either $p \mid m$ or $p \equiv 1 \pmod{m}$.*

Proof: If $p \mid m$, then we are done. If $p \nmid m$, then p is coprime to m and so by Proposition 5.4, we have $o_p(a) = m$ which implies $p \equiv 1 \pmod{m}$ by Corollary 4.4. □

Corollary 5.6 *Let $m \in \mathbb{N}$. Let $a \in \mathbb{Z}$. Let p be any prime divisor of $\Phi_m(ma)$. Then $p \equiv 1 \pmod{m}$.*

Proof: Since the constant term of $\Phi_m(x)$ is ± 1, we see that $\gcd(m, \Phi_m(ma)) = 1$ and so $p \nmid m$. □

Theorem 5.7 *Let $m \in \mathbb{N}$. There are infinitely many primes $\equiv 1 \pmod{m}$.*

Proof: Since $\Phi_m(x)$ is monic, we know that $\Phi_m(x) \to \infty$ as x goes to infinity. Let N be a large integer such that $\Phi_m(x) > 1$ for all $x \geq N$. We now construct the sequence by taking $a_1 = N$ and

$$a_{n+1} = \Phi_m(Nma_1a_2 \cdots a_n).$$

Then we have a sequence of pairwise coprime (because the constant term of $\Phi_m(x)$ is ± 1) integers at least 2, each having only prime divisors congruent to 1 mod m. □

It makes one wonder for which coprime positive integers a and m does there exist a Euclid type proof for the infinitude of primes congruent to a mod m. All of these proofs lead to the construction of an Euclidean polynomial for a mod m: a polynomial $h(x)$ with integer coefficients such that the prime divisors of $h(n)$ for integers n (either belong to a fixed finite set, or) are 1 mod m, or are a mod m; and that infinitely many primes that are a mod m arise this way.

Theorem 5.8 *A Euclidean polynomial for a mod m exists if and only if $a^2 \equiv 1 \pmod{m}$.*

Schur (1912) proved the backwards direction and Murty (1988) proved the forwards direction. For example, this implies that there are no Euclid type argument for the infinitude of primes of the form $5k + 2$.

Here are some Euclidean polynomials in small moduli:

(a) Primes dividing $5(2n)^2 - 1$ are congruent to 1 or 4 mod 5.

(b) Primes dividing $2n^2 + 1$ are congruent to 1 or 3 mod 8.

(c) Primes dividing $2n^2 - 1$ are congruent to 1 or 7 mod 8.

(d) Primes dividing $(7n)^3 + (7n)^2 - 2(7n) - 1$ are congruent to 1 or 6 mod 7.

(e) Primes dividing $(3n)^3 - 3(3n) - 1$ are congruent to 1 or 8 mod 9.

Statements (a) - (c) are results in Quadratic Reciprocity. Statement (d) and (e) use the theory of finite fields. Schur's result uses the theory of field extensions and Galois theory. Murty's result is about the splitting of primes and uses Chebotarev's density theorem, which is ironic because it is actually a generalization of Dirichlet's result on primes in arithmetic progression!

Here is a preview of what quadratic reciprocity says. Let's consider statement (a). Let p be an odd prime. Then statement (a) (ignoring the factor of 2) says that

$$\exists n \in \mathbb{Z}, p \mid 5n^2 - 1 \quad \iff \quad p \equiv 1, 4 \pmod 5.$$

Now

$$p \mid 5n^2 - 1 \quad \iff \quad 5n^2 \equiv 1 \pmod p \quad \iff \quad (5n)^2 \equiv 5 \pmod p.$$

In other words, p is a prime divisor of $5n^2 - 1$ for some integer n is equivalent to 5 being a square mod p. On the other hands, the squares mod 5 are exactly $0, 1, 4$ as $1^2 \equiv 4^2 \equiv 1$ and $2^2 \equiv 3^2 \equiv 4$. Since $5 \nmid 5n^2 - 1$, we may ignore the case $p = 5$. Hence, we can rephrase the above as: if $p \neq 5$, then

$$5 \text{ is a square mod } p \quad \iff \quad p \text{ is a square mod } 5.$$

Exercises

5.1 Compute $\Phi_9(x)$ and find a polynomial $f(x)$ such that $x^3 f(x + x^{-1}) = \Phi_9(x)$.

5.2 Prove that for any $k \in \mathbb{N}$, we have $\Phi_{2^k}(x) = x^{2^{k-1}} + 1$.

5.3 Prove that for any $k \in \mathbb{N}$, we have $\Phi_{3^k}(x) = x^{2 \cdot 3^{k-1}} + x^{3^{k-1}} + 1$.

5.4 Prove that for any $h, k \in \mathbb{N}$, we have $\Phi_{2^h 3^k}(x) = x^{2^h 3^{k-1}} - x^{2^{h-1} 3^{k-1}} + 1$.

5.5 Suppose $q \in \mathbb{N}$ such that $\Phi_q(x) = x^{2s} + cx^s + 1$ for some nonzero integer c, where $s = \phi(q)/2$. Prove that $c = \pm 1$.

5.6 Prove that if p is a prime at least 5, then there exists a polynomial $h(x)$ with integer coefficients such that $x^{2p} + x^p + 1 = (x^2 + x + 1)h(x)$.

5.7 We will see later that the cyclotomic polynomials $\Phi_q(x)$ are all irreducible in the sense that they do not admit a factorization into a product of polynomials with integer coefficients with smaller degrees. You will prove in HW 3 that $\Phi_q(x)$ is reciprocal in the sense that $\Phi_q(x^{-1}) = x^{-\phi(q)} \Phi_q(x)$. Prove that if $\Phi_q(x)$ is a trinomial, that is of the form $x^{\phi(q)} + cx^s + 1$ for some nonzero integers c, s, then $q = 2^h 3^k$ for some non-negative integer h and positive integer k.

5.8 Using the fact that primes dividing $2n^2 + 1$ are congruent to 1 or 3 mod 8, prove that there are infinitely many primes of the form $8k + 3$.

Lecture 11 Fri 09/27
Rings

6 Abstract Algebra

We have seen so many beautiful results about the integers and if you think about it, everything really just boils down to addition and multiplication, and a notion of size. The sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or the sets of polynomials with coefficients in them also have addition and multiplication and a notion of size. Can we try defining primes and gcd and do all of the above? For example, what should a prime in $\mathbb{R}$ mean, what should a prime in $\mathbb{R}[x]$ mean?

The key in defining a prime is the notion of divisibility. We say $a \mid b$ in $\mathbb{Z}$ if $b = ka$ for some $k \in \mathbb{Z}$. The natural extension to $\mathbb{R}$ would be that $a \mid b$ in $\mathbb{R}$ if $b = ka$ for some $k \in \mathbb{R}$. This is a little silly because we can divide in $\mathbb{R}$ so if $a \neq 0$, then by taking $k = b/a$, we have $b = ka$. This is more meaningful in $\mathbb{R}[x]$ where we say $a \mid b$ in $\mathbb{R}[x]$ if $b = ka$ for some $k \in \mathbb{R}[x]$. Then we have non-divisions like $x + 1 \nmid x^2 + 1$. Note that the definition of division only uses multiplication.

In abstract algebra, we step away from numbers and consider any set for which arithmetic operations like addition and multiplication can be defined.

Definition: A commutative ring R is a set equipped with two binary operations:

$$(a, b) \mapsto a + b : R \times R \to R, \qquad (a, b) \mapsto ab : R \times R \to R,$$

one unary operation:

$$a \mapsto -a : R \to R$$

and two nullary operations:

$$0 \in R, \qquad 1 \in R, \qquad \text{with} \quad 0 \neq 1$$

such that the usual laws of arithmetic hold:

(1) (Commutative) $a + b = b + a$ and $ab = ba$;

(2) (Associative) $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$;

(3) (Distributive) $a(b + c) = ab + ac$;

(4) (Additive identity) $a + 0 = a$ and $a + (-a) = 0$;

(5) (Multiplicative identity) $a \cdot 1 = a$.

Remark: More generally, we do not assume multiplication to be commutative (for example matrix multiplication is not commutative) in which case we will add $(b + c)a = ba + ca$ to (3) and $1 \cdot a = a$ to (5). All rings are assumed to be commutative in this class.

We do not assume that a multiplicative inverse a^{-1} always exist. We say $a \mid b$ in R if there exists $k \in R$ such that $b = ka$. If $a \mid 1$, that is if $ab = 1$ for some $b \in R$, then we say a is a unit and write $b = a^{-1}$. We define the group of units as

$$R^\times = \{a \in R \colon \exists b \in R, ab = 1\}.$$

The set $\mathbb{Z}$ of integers with the usual $0, 1, +, \times, -$ is a commutative ring. An integer $a \in \mathbb{Z}$ is a unit if and only if $a \mid 1$ if and only if $a = \pm 1$. So $\mathbb{Z}^\times = \{1, -1\}$.

The sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with the usual operations are all commutative rings. Every nonzero element is a unit. A commutative ring R is field if $R^\times = R \backslash \{0\}$.

A commutative ring is an integral domain if the product of two nonzero elements is nonzero. In other words, $a \neq 0$ and $b \neq 0 \Rightarrow ab \neq 0$. Equivalently, $ab = 0 \Rightarrow a = 0$ or $b = 0$. The ring $\mathbb{Z}$ of integers is an integral domain that is not a field. The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are both integral domains and fields.

Lemma 6.1 *Let R be a commutative ring.*

(a) For any $a \in R$, we have $a \cdot 0 = 0$, $a \cdot (-1) = -a$ and $-(-a) = a$. In particular, $0 \notin R^\times$.

(b) If $a, b \in R^\times$, then $ab \in R^\times$ and $a^{-1} \in R^\times$.

(c) If R is a field, then R is an integral domain.

Proof: Let $a \in R$ be arbitrary. Then $a \cdot 0 + a \cdot 1 = a \cdot (0+1) = a \cdot 1$. Then

$$\begin{aligned} a \cdot 0 &= a \cdot 0 + (a \cdot 1 + (-(a \cdot 1))) \\ &= (a \cdot 0 + a \cdot 1) + (-(a \cdot 1)) \\ &= a \cdot 1 + (-(a \cdot 1)) \\ &= 0. \end{aligned}$$

From $a \cdot (-1) + a \cdot 1 = a \cdot (-1+1) = a \cdot 0 = 0$, we get $a \cdot (-1) = -(a \cdot 1) = -a$ by adding $-(a \cdot 1)$ to both sides. Finally, from $a + (-a) = 0$, we add $-(-a)$ to both sides to get $a = -(-a)$. Note that 0 is never a unit because for any $b \in R$, $0 \cdot b = 0 \neq 1$.

Suppose now a, b are units. Then $ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$. Hence ab is a unit. From $aa^{-1} = 1$, we also see that $a^{-1} \in R^\times$ and $(a^{-1})^{-1} = a$. Suppose now R is a field. Then the product of two nonzero elements (which are automatically units) is a unit, which is never 0. Hence, R is an integral domain. □

To give an example of a ring that is not an integral domain, we consider

$$R = \mathbb{Z} \times \mathbb{Z} = \{(a, b) \colon a, b \in \mathbb{Z}\}.$$

We take $(0,0)$ to be 0_R and $(1,1)$ to be 1_R. We define addition and multiplication coordinate-wise:

$$(a, b) + (c, d) = (a + c, b + d) \qquad \text{and} \qquad (a, b) \cdot (c, d) = (ac, bd).$$

Then negation is given by $-(a, b) = (-a, -b)$. We note that R is not an integral domain because

$$(1, 0) \cdot (0, 1) = (0, 0).$$

In general, if R_1 and R_2 are two rings, we can define a ring structure on the Cartesian product

$$R_1 \times R_2 = \{(a, b) \colon a \in R_1, b \in R_2\}$$

exactly as above. It will not be an integral domain.

It is possible to define a ring structure on $\mathbb{Z} \times \mathbb{Z}$ that makes it an integral domain. We write $S = \mathbb{Z} \times \mathbb{Z}$ and define

$$\begin{aligned} 0_S &= (0, 0) \\ 1_S &= (1, 0) \\ (a, b) + (c, d) &= (a + c, b + d) \\ (a, b) \cdot (c, d) &= (ac - bd, ad + bc) \\ -(a, b) &= (-a, -b). \end{aligned}$$

One can check that all the ring axioms are satisfied. For example

$$(a, b) \cdot (1, 0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a, b).$$

In particular, we see that $(1, 0) \cdot (0, 1) = (0, 1) \neq (0, 0)$. Let's prove that S is an integral domain. Suppose $(a, b) \cdot (c, d) = 0$ and both (a, b) and (c, d) are nonzero. Then

$$\begin{aligned} ac - bd &= 0, \\ ad + bc &= 0. \end{aligned}$$

Multiply the first equation by c and the second by d and add them: $a(c^2 + d^2) = 0$. Since c and d are integers not both 0, we have $c^2 + d^2 \neq 0$. So $a = 0$. Then from $bc = bd = 0$, we get $b = 0$. This contradicts the assumption that $(a, b) \neq (0, 0)$.

Lecture 12 Mon 10/02
homomorphism, characteristic

What really is happening in this example? We write suggestively $i_S = (0,1)$. Note that

$$i_S^2 = (0,1)\cdot(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1,0) = -1_S.$$

Moreover, for any positive integer n and (more generally) any element r of a ring R, we write nr for the sum of n r's and $(-n)r$ for the sum of n $-r$'s. In this example, we have $n(a,b) = (na, nb)$ so every element $(a,b) \in S$ can be expressed as

$$(a,b) = a(1,0) + b(0,1) = a1_S + bi_S.$$

Then by distributivity, we can compute multiplication as

$$(a,b)\cdot(c,d) = (a1_S + bi_S)(c1_S + di_S) = ac1_S + bci_S + adi_S + bdi_S^2 = (ac-bd)1_S + (ad+bc)i_S.$$

This looks like the multiplication of complex numbers! In fact, we can define a map $f : S \to \mathbb{C}$ by $f(a,b) = a + bi$. Then we have

$$\begin{aligned} f(0_S) &= 0 \\ f(1_S) &= 1 \\ f(i_S) &= i \\ f((a,b)\cdot(c,d)) &= f(a,b)f(c,d) \\ f((a,b)+(c,d)) &= f(a,b) + f(c,d). \end{aligned}$$

The image of f is the set of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \colon a, b \in \mathbb{Z}\}.$$

In general, a ring homomorphism is a map $f : R_1 \to R_2$ between two rings R_1, R_2 such that for any $a, b \in R_1$,

$$f(a+b) = f(a) + f(b), \qquad f(ab) = f(a)f(b), \qquad f(1) = 1.$$

Take $a = b = 0$, we get $f(0) = f(0) + f(0)$ and so $f(0) = 0$. Then take $b = -a$ to get $f(-a) = -f(a)$. The assumption $f(1) = 1$ is required to rule-out the 0 map. In other words, a ring homomorphism respects all the ring operations on R_1 and R_2.

The natural inclusions $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$ are all ring homomorphisms. They are all injective. Is the map $f : \mathbb{C} \to \mathbb{R}$ taking a complex number $a + bi$ to its real part a a ring homomorphism? No, because it doesn't behave well with multiplication. For example, $f(i) = 0$ but $f(i\cdot i) = f(-1) = -1 \neq f(i)\cdot f(i)$. Does there exist any ring homomorphism $\mathbb{C} \to \mathbb{R}$? Suppose there is a ring homomorphism $g : \mathbb{C} \to \mathbb{R}$. Then from $g(1) = 1$, we see that $g(-1) = -1$. So $g(i)^2 = g(i^2) = g(-1) = -1$ but there isn't any real number that square to -1.

Lemma 6.2 *Let R_1, R_2, R_3 be commutative rings.*

(a) The projection map $R_1 \times R_2 \to R_1$ sending (a,b) to a is a ring homomorphism. Similarly for the projection map $R_1 \times R_2 \to R_2$ sending (a,b) to b.

(b) If $f : R_1 \to R_2$ and $g : R_2 \to R_3$ are ring homomorphisms, then $g \circ f : R_1 \to R_3$ is a ring homomorphism.

Proof: Just check definitions. Write $\pi_1(a,b) = a$. Then $\pi_1(1,1) = 1$ and

$$\pi_1((a,b)+(c,d)) = \pi_1(a+c, b+d) = a + c = \pi_1(a,b) + \pi_1(c,d)$$

and

$$\pi_1((a,b)\cdot(c,d)) = \pi_1(ac, bd) = ac = \pi_1(a,b)\pi_1(c,d).$$

Similarly for $\pi_2(a,b) = b$. For (b), we use the subscript $1, 2, 3$ to denote the operations in R_1, R_2, R_3. Then $g \circ f(1_1) = g(1_2) = 1_3$. For $a, b \in R_1$, we have

$$g \circ f(a +_1 b) = g(f(a) +_2 f(b)) = g(f(a)) +_3 g(f(b))$$

and

$$g \circ f(a \times_1 b) = g(f(a) \times_2 f(b)) = g(f(a)) \times_3 g(f(b)).$$

Hence $g \circ f$ is a ring homomorphism. □

Lemma 6.3 *Let R be a commutative ring. There is a unique ring homomorphism $f : \mathbb{Z} \to R$ (called the canonical homomorphism).*

Proof: Any ring homomorphism $f : \mathbb{Z} \to R$ must send the integer 1 to the element 1_R. Since it behaves well with addition, it will then send any integer n, viewed as a sum of 1's, to $n \cdot 1_R$. Hence this map is unique. Conversely, that map f sending n to $n \cdot 1_R$ is a ring homomorphism since

$$f(n) \cdot f(m) = \underbrace{(1_R + \cdots + 1_R)}_{n} \cdot \underbrace{(1_R + \cdots + 1_R)}_{m} = \underbrace{(1_R + \cdots + 1_R)}_{nm} = f(nm)$$

$$f(n) + f(m) = \underbrace{(1_R + \cdots + 1_R)}_{n} + \underbrace{(1_R + \cdots + 1_R)}_{m} = \underbrace{(1_R + \cdots + 1_R)}_{n+m} = f(n+m)$$

and certainly $f(1) = 1_R$. □

If this map f is injective, then we say that the characteristic of R is 0. In all the examples $(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z} \times \mathbb{Z}, \mathbb{Z}[i])$ we saw, the characteristic is 0. If f is not injective, then there is some nonzero integer a such that $f(a) = 0$. Now $f(-a) = -f(a) = 0$, so we may assume a is positive. The smallest positive integer d such that $f(d) = 0$ is the characteristic of R.

For any integer $m \geq 2$, there is a ring of characteristic m. Namely, $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}$. We define $0 = 0$ and $1 = 1$. We define addition and multiplication by the usual addition and multiplication and then applying the division algorithm to find the remainder by m. For example, in $\mathbb{Z}/69\mathbb{Z}$, we have $25 \times 4 = 100 = 31$. Note also that $23 \times 3 = 0$ in $\mathbb{Z}/69\mathbb{Z}$ but 23 and 3 are nonzero.

Lemma 6.4 *If R is an integral domain, then its characteristic is either 0 or a prime.*

Proof: Suppose the characteristic d of R is positive. Let q be a positive divisor of d so $d = qk$ for some $k \in \mathbb{N}$. Then $f(q)f(k) = f(d) = 0$ where $f : \mathbb{Z} \to R$ is the canonical homomorphism. Since R is an integral domain, either $f(q) = 0$ or $f(k) = 0$. Note that $q \leq d$ and $k \leq d$. Hence by minimality of d, we have $q = d$ in the first case, and $k = d$ so $q = 1$ in the second case. Hence we have shown that the only positive divisors of d are 1 and d. In other words, d is a prime. □

The converse is certainly not true because $\mathbb{Z} \times \mathbb{Z}$ is a ring of characteristic 0 but is not an integral domain, and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is a ring of characteristic p but is not an integral domain.

Lecture 13 Wed 10/04
$\mathbb{Z}/m\mathbb{Z}$ part 1, Chinese remainder theorem

We play more with the ring $\mathbb{Z}/m\mathbb{Z}$ and recover some of the results in congruence arithmetic.

Question 1: What are the units of $\mathbb{Z}/m\mathbb{Z}$?

Let's consider $\mathbb{Z}/69\mathbb{Z}$. Is 1 a unit? Yes, the element 1 in a ring is always a unit. Is 2 a unit? Can we find some $x \in \{0, 1, \ldots, 68\}$ such that the remainder when $2b$ is divided by 69 is 1? This is like solving the congruence equation

$$2x \equiv 1 \pmod{69}.$$

By observation, we see that $x = 35$ works. So $2^{-1} = 35$. What about 3? Can we solve $3x \equiv 1 \pmod{69}$? That is, we want $69 \mid 3x - 1$. So $3x - 1 = 69y$ for some integer y. Rearranging gives $3x - 69y = 1$. However, $\gcd(3, 69) = 3$ divides every integer of the form $3x - 69y$, so it can't ever be 1. Hence 3 is not a unit in $\mathbb{Z}/69\mathbb{Z}$. In general, in order for a to be a unit in $\mathbb{Z}/69\mathbb{Z}$, we need there to exist integers x and y such that

$$ax - 69y = 1.$$

We know this is possible if and only if $\gcd(a, 69) = 1$. Hence

$$(\mathbb{Z}/69\mathbb{Z})^\times = \{a = 0, 1, \ldots, 68 \colon \gcd(a, 69) = 1\}.$$

Replacing 69 by m gives:

Lemma 6.5 *For an integer $m \geq 2$, we have $(\mathbb{Z}/m\mathbb{Z})^\times = \{a = 0, 1, \ldots, m-1 \colon \gcd(a, m) = 1\}$. Its size is $\phi(m)$.*

Corollary 6.6 *For an integer $m \geq 2$, $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is a prime p. We also denote $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$.*

Proof: By definition, $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if every nonzero element is a unit if and only if $\gcd(a, m) = 1$ for every $a = 1, 2, \ldots, m-1$ if and only if m is a prime. □

Question 2: When does there exist a ring homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$?

Is there a ring homomorphism $f : \mathbb{Z}/69\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$? It should send 1 to 1; then $2 = 1+1$ to $1+1 = 0$ in $\mathbb{Z}/2\mathbb{Z}$; then $3 = 1+1+1$ to $1+1+1 = 1$ in $\mathbb{Z}/2\mathbb{Z}$. Continue on, we see that it should send every even number to 0 and every odd number to 1. Now $f(68) = 0$ and $f(1) = 1$. In $\mathbb{Z}/69\mathbb{Z}$, we have $68 + 1 = 0$, but

$$f(68) + f(1) = 0 + 1 = 1 \neq f(0) = f(68 + 1).$$

Hence there is no ring homomorphism $\mathbb{Z}/69\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. What about $\mathbb{Z}/69\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$? Simply taking the remainder by 3 gives a map $g : \mathbb{Z}/69\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$. To check that it is a ring homomorphism, we take $a, b \in \{0, 1, \ldots, 68\}$. We write $a + b = 69q + r$ with remainder $r \in \{0, 1, \ldots, 68\}$. Then $a + b = r$ in $\mathbb{Z}/69\mathbb{Z}$. Now

$$a \equiv g(a) \pmod 3, \qquad b \equiv g(b) \pmod 3, \qquad r \equiv g(r) \pmod 3.$$

From $a + b = 69q + r$, we have

$$a + b \equiv r \pmod 3 \qquad \text{and so} \qquad g(a) + g(b) \equiv g(r) \pmod 3.$$

The formula $g(a)g(b) \equiv g(ab) \pmod 3$ can be checked in the same way. The key here is that $3 \mid 69$.

Lemma 6.7 *Let R be a commutative ring of characteristic $d > 0$. Let $f : \mathbb{Z} \to R$ be the canonical homomorphism. Then $f(n) = 0$ if and only if $d \mid n$.*

Proof: If $d \mid n$, then $n = dk$ for some integer k and we have $f(n) = f(d)f(k) = 0$. Suppose conversely that $f(n) = 0$. Applying the division algorithm to n divided by d gives $n = dq + r$ for some integers q, r with $0 \leq r < d$. Then $f(r) = f(n) - f(d)f(q) = 0$. Since d is the smallest positive integer such that $f(d) = 0$ and $r < d$, we see that r can't be positive and so $r = 0$, implying that $d \mid n$. □

Corollary 6.8 *For integers $m, n \geq 2$, there exists a ring homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ if and only if $n \mid m$.*

Proof: Suppose a ring homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ exists. Consider the composition

$$h : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}.$$

By uniqueness, h is the canonical homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Note that $h(m) = 0$ since m goes 0 in $\mathbb{Z}/m\mathbb{Z}$. Hence by Lemma 6.7, we have $n \mid m$ since $\mathbb{Z}/n\mathbb{Z}$ has characteristic n.

The converse direction where $n \mid m$ follows exactly as the example of $3 \mid 69$ above. □

Question 3: What does the Chinese Remainder Theorem say?

Theorem 6.9 *(Chinese Remainder Theorem) Let m and n be coprime integers. Let a and b be integers. Then there exist a unique integer $x = 0, 1, \ldots, mn-1$ such that*

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Proof: Exercise/Look it up! A more general version of this will be discussed later. □

Since $m \mid mn$ and $n \mid mn$, we have a ring homomorphism

$$\begin{aligned} \mathbb{Z}/mn\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x &\mapsto (x \bmod m, x \bmod n). \end{aligned}$$

Then the Chinese Remainder Theorem is really saying that this ring homomorphism is bijective: injective (different elements map to different things) and surjective (the image is everything). An isomorphism is a ring homomorphism that is bijective. We say two rings R_1 and R_2 are isomorphic if there is an isomorphism between them and we write $R_1 \cong R_2$. In this case, we have

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

We can continue breaking off coprime factors. More generally, let

$$m = p_1^{k_1} \cdots p_r^{k_r}$$

be the prime factorization of m, then we have

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{k_r}\mathbb{Z} \\ \left(\mathbb{Z}/m\mathbb{Z}\right)^\times &\cong \left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_r^{k_r}\mathbb{Z}\right)^\times \end{aligned}$$

Corollary 6.10 *Let $m \in \mathbb{N}$ with prime factorization $p_1^{k_1} \cdots p_r^{k_r}$. Then*

$$\phi(m) = \prod_{i=1}^{r} \left(p_i^{k_i} - p_i^{k_i - 1}\right) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right).$$

Proof: We have $\phi(m) = \prod_{i=1}^{r} \phi(p_i^{k_i})$. It is easy to see that for any prime p and positive integer k, $\phi(p^k) = p^k - p^{k-1}$ since there are p^{k-1} numbers in $0, 1, 2, \ldots, p^k - 1$ that are divisible by p. □

Lecture 14 Fri 10/06

$\mathbb{Z}/m\mathbb{Z}$ part 2, Fermat's little theorem

Question 4: What about Fermat's little Theorem?

Lemma 6.11 *Let R be a commutative ring. Let $a \in R$.*

(a) The map $x \mapsto x + a$ defines a bijection $R \to R$.

(b) The map $x \mapsto xa$ is a bijection $R \to R$ if and only if $a \in R^\times$.

Proof: The map $x \mapsto x + (-a)$ is the inverse of $x \mapsto x + a$. If $a \in R^\times$, then $x \mapsto xa^{-1}$ is the inverse of $x \mapsto xa$. Conversely, if $x \mapsto xa$ is surjective, then $ba = 1$ for some $b \in R$ and so $a \in R^\times$. □

Corollary 6.12 *Let R be an integral domain. Suppose R is finite. Then R is a field.*

Proof: Let a be a nonzero element. Then for any $x \neq y$, we have $x - y \neq 0$ and so $(x-y)a \neq 0$, implying that $xa \neq ya$. So the map $x \mapsto xa : R \to R$ is injective. An injective map between two finite sets of the same size is surjective (by the Pigeonhole principle) and so bijective. Hence a is a unit. □

For a finite ring R, we define its order $|R|$ to be the number of elements of R.

Theorem 6.13 *Let R be a finite commutative ring. Let $a \in R$.*

(a) Then $|R| \cdot a = 0$. In particular, the characteristic of R divides $|R|$.

(b) If $a \in R^\times$, then $a^{|R^\times|} = 1$.

Proof: Let $n = |R|$ and let $r_1, \ldots, r_n$ denote all the elements of R. Then $r_1 + a, r_2 + a, \ldots, r_n + a$ is a permutation of $r_1, r_2, \ldots, r_n$ since $x \mapsto x + a$ is a bijection. Hence

$$(r_1 + a) + \cdots + (r_n + a) = r_1 + \cdots + r_n.$$

Cancelling the $r_1 + \cdots + r_n$ from both sides gives $na = 0$. Applying this to $a = 1_R$ gives $f(n) = 0$ where $f : \mathbb{Z} \to R$ is the canonical homomorphism. We then have the characteristic of R dividing n by Lemma 6.7.

Statement (b) follows by essentially the same argument. Let $t = |R^\times|$ and let $s_1, \ldots, s_t$ denote all the elements of $R^\times$. Suppose $a \in R^\times$. By Lemma 6.1, we know that each $as_1, \ldots, as_t$ is a unit and by Lemma 6.11, we know they are all distinct, and so they are a permutation of $s_1, \ldots, s_t$. We now multiply them to get

$$a^t s_1 \cdots s_t = s_1 \cdots s_t.$$

Cancelling the $s_1 \cdots s_t$ from both sides by multiplying by $s_t^{-1} \cdots s_1^{-1}$ gives $a^t = 1$. □

Corollary 6.14 *(Euler's Theorem, Fermat's little Theorem) Let $m \in \mathbb{N}$. Let a be an integer coprime to m. Then $a^{\phi(m)} \equiv 1 \pmod{m}$. If $m = p$ is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

We write $o_+(a)$, the additive order of a in R, for the smallest positive integer d such that $da = 0$. Then by a standard division algorithm argument (see for example the proof of Proposition 4.3), we have $o_+(a) \mid |R|$. We write $o(a)$, the order of a in $R^\times$, for the smallest positive integer d such that $a^d = 1$ if $a \in R^\times$. Then $o(a) \mid |R^\times|$.

Question 5: When is a ring isomorphic to $\mathbb{Z}/m\mathbb{Z}$?

When thinking about isomorphic rings, we should think of them as essentially the same thing but labelled differently. So what are some intrinsic properties of $\mathbb{Z}/m\mathbb{Z}$? It was introduced as a ring of characteristic m. In other words, none of $0_R, 1_R, 2 \cdot 1_R, \ldots, (m-1) \cdot 1_R$ equals 0_R but $m \cdot 1_R = 0_R$. Note that this also implies that if $0 \leq i < j \leq m - 1$, then $i \cdot 1_R \neq j \cdot 1_R$, for if otherwise, $(j - i) \cdot 1_R = 0_R$ and $1 \leq j - i < m$. Hence, for a ring R of characteristic m, the m elements $0_R, 1_R, 2 \cdot 1_R, \ldots, (m-1) \cdot 1_R$ are distinct. In the case of $\mathbb{Z}/m\mathbb{Z}$, these are all the elements.

Proposition 6.15 *Let $m \geq 2$ be an integer and let R be a commutative ring with characteristic m. Then the following are equivalent:*

(a) The canonical map $f : \mathbb{Z} \to R$ is surjective;

(b) $|R| = m$;

(c) $R \cong \mathbb{Z}/m\mathbb{Z}$;

Proof: From the above discussion, we see that the image of f is exactly the set $\{0_R, 1_R, 2 \cdot 1_R, \ldots, (m-1) \cdot 1_R\}$ of m elements. Hence f is surjective if and only if these are all the elements of R if and only if $|R| = m$.

It is easy to check that the map $g : \mathbb{Z}/m\mathbb{Z} \to R$ sending $a = 0, 1, \ldots, m-1$ to $a \cdot 1_R$ is a ring homomorphism (similar to the proof of that $a \mapsto a \bmod 3$ is a ring homomorphism $\mathbb{Z}/69\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$), and injective by the above. It is surjective if and only if $|R| = m$. □

Corollary 6.16 *Let R be a commutative ring of order p where p is a prime. Then $R \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.*

Proof: By Theorem 6.13, we know that the characteristic of R has to divide p, and so equals p since p is a prime. Then by Proposition 6.15, we have $R \cong \mathbb{Z}/p\mathbb{Z}$. □

Since we assumed that $0 \neq 1$ in a ring, every ring has size at least 2. Corollary 6.16 then implies that there is only one commutative ring, up to isomorphism, of order 2 ($\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$), of order 3 ($\mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$), of order 5 ($\mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$), of order 7 ($\mathbb{Z}/7\mathbb{Z} = \mathbb{F}_7$). What about rings of order 4 or 6? There are at least 2 non-isomorphic commutative rings of order 4, namely $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$. The former has characteristic 2 while the latter has characteristic 4. If we try the same with 6, we will have $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$, but we know they are isomorphic by the Chinese Remainder Theorem. You will prove in HW 5 that if m is squarefree (so that it is not divisible by p^2 for any prime), then any commutative ring of order m is isomorphic to $\mathbb{Z}/m\mathbb{Z}$. This applies to rings of order 6.

For rings of order 4, there are two more! We will in fact be able to generalize this to rings of order p^2 for any prime p. In this case, one can actually brute-force it.

Let R be a commutative ring of order 4. Let's write $R = \{0, 1, \alpha, \beta\}$. The first main branching point is whether $1 + 1 \in \{0, 1\}$. Suppose first that $1 + 1 \notin \{0, 1\}$ and we write without loss of generality $1 + 1 = \alpha$. What is $1 + \alpha$ in this case? We know it can't be 1 or α. If $1 + \alpha = 0$, then this forces $1 + \beta = \beta$ which is not possible. Therefore, we must have $1 + \alpha = \beta$ and $1 + \beta = 0$. In other words, $\alpha = 1 + 1$ and $\beta = 1 + 1 + 1$ and so the canonical homomorphism $\mathbb{Z} \to R$ is surjective, implying that $R \cong \mathbb{Z}/4\mathbb{Z}$.

Suppose now $1 + 1 \in \{0, 1\}$, and so $1 + 1 = 0$. Note that we must have $\alpha + \alpha = \alpha(1 + 1) = 0$. The addition table is now uniquely determined.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times_1$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	0	α
β	0	β	α	1

$\times_2$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	α	0
β	0	β	0	β

$\times_3$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

There are now multiple options for the multiplication table. We note that it is determined by α^2 as

$$\alpha\beta = \alpha(\alpha + 1) = \alpha^2 + \alpha, \qquad \beta^2 = (\alpha + 1)^2 = \alpha^2 + 1.$$

There are now three isomorphism classes. If $\alpha^2 \in \{0, 1\}$, then either $\alpha^2 = 0$ or $\beta^2 = 0$ and so by renaming, we may assume $\alpha^2 = 0$ and we get the ring $\mathbb{F}_2[x]/(x^2)$. If $\alpha^2 = \alpha$, then we get the ring $\mathbb{F}_2[x]/(x^2 - x)$. If $\alpha^2 = \beta$, then we get the ring $\mathbb{F}_4$. We list the special property that they each have to show that they are all non-isomorphic.

1. $\mathbb{Z}/4\mathbb{Z}$ has an element a such that $a + a \neq 0$.
2. $\mathbb{F}_2[x]/(x^2)$ has a nonzero element a such that $a^2 = 0$.
3. $\mathbb{F}_2[x]/(x^2 - x)$ has the property that every element a is idempotent, that is $a^2 = a$.
4. $\mathbb{F}_4$ is an integral domain (and also a field).

Lecture 14.5 (Tutorial) Fri 10/06
What are real numbers?

Have you ever lay awake at night and wondered what really are real numbers and how does arithmetic work with them? For example, we learned in grade school how to add two numbers like 69 and 420, but what about irrational numbers like π and e?

$$\begin{array}{rr} & 69 \\ + & 420 \\ \hline & 489 \end{array} \qquad\qquad \begin{array}{rr} & 3.14159265358979323846264338327 95\ldots \\ + & 2.71828182845904523536028747135 27\ldots \\ \hline \end{array}$$

If we start adding from the first digits, how do we know we won't run into a sequence of 9's and then have to carry a 1 at some point? In this tutorial, I will define real numbers properly and prove that they form a field!

We start with the notion of equivalence relations. We have already seen this in the first tutorial. Let S be a set and we say a relation $\sim$ between elements of S is an equivalence relation if for every $a, b, c \in S$:

- (Reflexive) $a \sim a$
- (Symmetric) if $a \sim b$, then $b \sim a$
- (Transitive) if $a \sim b$ and $b \sim c$, then $a \sim c$.

For example, equality, congruence mod m, ring isomorphisms for some fixed set of rings are all equivalence relations. Given an equivalence relation, there is a well-defined notion of equivalence classes. For any $a \in S$, we define the equivalence class containing a as

$$[a] = \{b \in S \colon a \sim b\}.$$

For example, for equality, we have $[a] = \{a\}$; for congruence mod m, we have

$$[a] = \{b \in \mathbb{Z} \colon a \equiv b \pmod{m}\} = \{a + md \colon d \in \mathbb{Z}\}.$$

Note that a more precise definition of $\mathbb{Z}/m\mathbb{Z}$ is the set $\{[0], [1], \ldots, [m-1]\}$ with

$$[a] + [b] = [a + b] \qquad \text{and} \qquad [a] \cdot [b] = [ab].$$

Note that $a \in [a]$ since $a \sim a$. If $b \in [a] \cap [c]$, then $b \sim a$ and $b \sim c$, which implies that $a \sim c$. Then for any $d \in S$, we have $d \sim a$ if and only if $d \sim c$. So $[a] = [c]$. In other words, equivalence classes are either equal or disjoint.

Next we recall the definition of a Cauchy sequence from MATH 147. A Cauchy sequence $(x_n)_n$ in $\mathbb{Q}$ is a sequence where $x_n \in \mathbb{Q}$ and for every $\epsilon > 0$, there is some $N \in \mathbb{N}$ such that whenever $n, m > N$, we have $|x_n - x_m| < \epsilon$. For example, we can take x_n to be the first n digits in the decimal expansion of π:

$$x_1 = 3.1, \qquad x_2 = 3.14, \qquad x_3 = 3.141, \qquad x_4 = 3.1415, \text{ etc.}$$

We can also take the constant sequence $x_n = a$ where $a \in \mathbb{Q}$. The key idea is that we want the real numbers to arise as limits of Cauchy sequences in $\mathbb{Q}$ without even knowing what the limits are! Different Cauchy sequences can have the same "limits". For example, the constant sequence $x_n = 1$ and the sequence $y_n = 0.99\cdots9$ with n 9's both "converge" to 1. We don't want them to define different real numbers.

We define a relation on the set of Cauchy sequences in $\mathbb{Q}$. We say

$$(x_n)_n \sim (y_n)_n \qquad \iff \qquad \lim_{n\to\infty} (x_n - y_n) = 0.$$

That is, for every $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for $n > N$, we have $|x_n - y_n| < \epsilon$. It is easy to check that $\sim$ is an equivalence relation.

- (Reflexive) $\lim (x_n - x_n) = 0$.
- (Symmetric) if $\lim (x_n - y_n) = 0$, then $\lim (y_n - x_n) = 0$.
- (Transitive) if $\lim (x_n - y_n) = 0$ and $\lim (y_n - z_n) = 0$, then $\lim (x_n - z_n) = 0$.

We define $\mathbb{R}$ as the set of equivalence classes of Cauchy sequences in $\mathbb{Q}$. For every $a \in \mathbb{Q}$, the equivalence class of the constant sequence $(a, a, \ldots)$ is the real number a. Which real number corresponds to the equivalence class of the sequence $x_n = 1/n$? In this case, $\lim x_n = 0$, so it is equivalent to the constant sequence $(0, 0, \ldots)$. Hence it is the real number 0. We now define the ring operations.

Lemma 6.17 *If $(x_n)_n$ and $(y_n)_n$ are two Cauchy sequences, then $\lim_{n\to\infty} |x_n|$ exists and so $|x_n|$ is bounded. Furthermore, $(x_n + y_n)_n$ and $(x_n y_n)_n$ are both Cauchy sequences. If $\lim_{n\to\infty} |x_n| \neq 0$, then $(x_n^{-1})_n$ is a Cauchy sequence.*

Proof: This is a MATH 147 exercise/homework/result. □

We define addition and multiplication on $\mathbb{R}$ via

$$[(x_n)_n] + [(y_n)_n] = [(x_n + y_n)_n] \qquad \text{and} \qquad [(x_n)_n] \cdot [(y_n)_n] = [(x_n y_n)_n]$$

and the additive and multiplicative inverses by

$$-[(x_n)_n] = [(-x_n)_n] \qquad \text{and} \qquad [(x_n)_n]^{-1} = [(x_n^{-1})_n].$$

When defining operations on equivalence classes, we need to prove that it is independent on the choices of the representatives. For example, for multiplication to be well-defined, we need to prove that if $(x_n)_n \sim (z_n)_n$ and $(y_n)_n \sim (w_n)_n$, then $(x_n y_n)_n \sim (z_n w_n)_n$. That is, suppose $\lim x_n - z_n = 0$ and $\lim y_n - w_n = 0$. Then

$$x_n y_n - z_n w_n = x_n(y_n - w_n) + (x_n - z_n)w_n \to 0.$$

This process of taking a space $\mathbb{Q}$ equipped with an absolute value and then constructing the set of equivalence classes of Cauchy sequences is called completion. The resulting space $\mathbb{R}$ is complete in the sense that any Cauchy sequence in $\mathbb{R}$ has a limit in $\mathbb{R}$.

I won't ask you questions about Cauchy sequences and you can pretend that real numbers are what you thought they were! We will be using the idea of equivalence relations and equivalence classes.

Lecture 15 Mon 10/07
Ideals

It is time to stop beating around the bush and talk about what / means. Actually I am going to beat around the bush a bit longer! Let R be a commutative ring. An ideal is a subset $I \subseteq R$ such that

(a) $0 \in I$;

(b) for any $a, b \in I$, we have $a + b \in I$;

(c) for any $a \in I$ and any $r \in R$, we have $ra \in I$.

What are the ideals of $\mathbb{Z}$ that contain 69? Suppose I is one such. Then it contains 0 and 69. Then using (b) with $a = b = 69$, we get $69 \cdot 2 \in I$. Then with $a = 69 \cdot 2$ and $b = 69$, we get $69 \cdot 3 \in I$. Or we can be smart and use (c) with $a = 69$ and $r = 3$ directly to get $69 \cdot 3 \in I$. More generally, with $r = k$ any integer, we get $69k \in I$ for any integer k. Does I need to contain anything else?

Lemma 6.18 *Let R be a commutative ring. Let $a \in R$ be any element. Then the set*

$$aR = (a) = \{ra \colon r \in R\} = \{b \in R \colon a \mid b\}$$

is an ideal of R containing a, and is a subset of any ideal of R containing a.

Proof: Take $r = 0$ to get $0 \in (a)$. For any $r, r_1, r_2 \in R$, we have $r_1 a + r_2 a = (r_1 + r_2)a \in (a)$ and $r(r_1 a) = (r r_1)a \in (a)$. Hence (a) is an ideal of R. Any ideal I containing a contains ra for any $r \in R$ by (c). So $(a) \subseteq I$. □

We call (a) the ideal generated by a. In our example, we note that $69 \in d\mathbb{Z}$ if and only if $d \mid 69$. So 69 is also an element of the ideals $69\mathbb{Z}$, $23\mathbb{Z}$, $3\mathbb{Z}$ and $\mathbb{Z}$. What about the ideals $(-69)\mathbb{Z}$, $(-23)\mathbb{Z}$, $(-3)\mathbb{Z}$ and $(-1)\mathbb{Z}$?

Lemma 6.19 *Let R be a commutative ring. Let $a \in R$ be any element and let $u \in R^\times$ be a unit. Then $(a) = (au)$. In particular, $(u) = (1) = R$.*

Proof: For any $r \in R$, we have $ra = (ru^{-1})(au) \in (au)$ and $rau = (ru)a \in (a)$. □

Corollary 6.20 *Suppose R is a field. Then the only ideals are $(0) = \{0\}$ and $(1) = R$.*

Proof: Any nonzero ideal contains a nonzero element, which is a unit in a field. □

Lemma 6.21 *Let R be a commutative ring such that the only ideals are $\{0\}$ and R. Then R is a field.*

Proof: Let $a \in R$ be a nonzero element. Then $(a) \neq \{0\}$ since it contains a. Hence $(a) = R$ and so $1 = ab$ for some $b \in R$. □

Remark: It is possible for $(a) = (b)$ but $b \neq au$ for any unit u. See Exercise 6.6.

An ideal of the form (a) is called a principal ideal. An integral domain where every ideal is principal is called a Principal ideal domain or PID for short.

Proposition 6.22 *$\mathbb{Z}$ is a PID.*

Proof: Let I be an ideal of $\mathbb{Z}$. If $I = \{0\}$, then $I = (0)$ is principal. Suppose I contains a nonzero integer. Let d be a nonzero element of I such that $|d|$ is the smallest. Then we know that $(d) \subseteq I$ and it remains to prove that $I \subseteq (d)$. Let $n \in I$. We apply the division algorithm to obtain $n = dq + r$ for some integers q, r with $0 \leq r < |d|$. Then $r = n - dq \in I$ since $n, d \in I$. However, $|r| < |d|$. So by the minimality of d, we see that r can't be nonzero. So $r = 0$ and $d \mid n$, implying that $n \in (d)$. □

The key to the above argument is the division algorithm and the notion of size. A Euclidean domain is an integral domain R with a function $N : R\backslash\{0\} \to \mathbb{N} \cup \{0\}$ if $a, b \in R$ with $a \neq 0$, there exists $q, r \in R$ such that $b = aq + r$ where either $r = 0$ or $N(r) < N(a)$. In HW 6, you will repeat the proof of Proposition 6.22 to prove that every Euclidean domain is a PID. (The range of N being $\mathbb{N} \cup \{0\}$ is not important. Any well-ordered subset of $\mathbb{R}$ will do.)

Chellenge exercise: Prove that $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a Euclidean domain with $N(a + bi) = a^2 + b^2$.

What are the ideals of $\mathbb{Z}/69\mathbb{Z}$? As always, we have the zero ideal (0) and the full ring (1) as ideals. We can try to repeat the proof of Proposition 6.22 even though we don't even have an integral domain. Let $I \subseteq \{[0], [1], \ldots, [68]\} = \mathbb{Z}/69\mathbb{Z}$ be a nonzero proper (i.e. not the whole ring) ideal. Let $d = 2, \ldots, 68$ be smallest such that $[d] \in I$. Let $n \in \mathbb{Z}$ such that $[n] \in I$. (Note we can have $n = 69$ since $[69] = [0] \in I$.) Apply the division algorithm to get $n = dq + r$ for some integers q, r such that $0 \leq r < d$. Then $[r] = [n] - [d][q] \in I$. By minimality of d, we have $r = 0$ and so $d \mid n$ in $\mathbb{Z}$ and $[d] \mid [n]$ in $\mathbb{Z}/69\mathbb{Z}$. We therefore have $I = ([d])$. Applying the above to $n = 69$ also implies that $d \mid 69$, so $d = 3$ or 23. In other words, there are four ideals of $\mathbb{Z}/69\mathbb{Z}$:

$$\{[0]\} = ([0]), \quad \{[0], [23], [46]\} = ([23]), \quad \{[0], [3], [6], \ldots, [66]\} = ([3]), \quad \mathbb{Z}/69\mathbb{Z} = ([1]).$$

Note that they correspond exactly to the four ideals of $\mathbb{Z}$ containing 69:

$$69\mathbb{Z}, \quad 23\mathbb{Z}, \quad 3\mathbb{Z}, \quad \mathbb{Z}.$$

Coincidence?

Remark 1: I actually can't give you an example of an ideal that is not principal yet. Every ideal of every ring that we have looked at is principal!

Remark 2: Condition (c) of an ideal: $a \in I \wedge r \in R \Rightarrow ra \in I$ might seem a bit weird. Another way to think of $a \in I$ is to think of it as a division $I \mid a$. Then we can translate the 3 conditions as:

(a) $I \mid 0$;

(b) if $I \mid a$ and $I \mid b$, then $I \mid a+b$;

(c) if $I \mid a$ and $a \mid b$, then $I \mid b$.

Historically, it is a widely believed though incorrectly (but it makes a cool story) that ideals came to existence when Kummer tried to prove Fermat's Last Theorem! When he factored

$$x^n - z^n = \prod_{k=1}^{n} (x - \zeta_n^k z),$$

he ran into the ring $\mathbb{Z}[\zeta_n]$ where unique factorization can fail (for the first time when $n = 23$). Kummer realized that we should allow more "things" in our notion of division, and called them ideal numbers.

Lecture 16 Wed 10/09
kernel, image, R/I

There is another class of subset of R that deserves special attention. Recall that a commutative ring R comes with 5 operations: 0, 1, $-$, $+$, $\times$. A subring of R is a subset S closed under all the ring operations of R. In other words:

(a) $0 \in S$, $1 \in S$;

(b) if $a, b \in S$, then $-a \in S$, $a+b \in S$, $ab \in S$.

In other other words, S is a ring with the ring operations of R. In this case, the natural inclusion $S \to R$ (by viewing an element of S is an element of R) is a ring homomorphism.

For example, $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are all subrings in the next. The ring $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$. Can an ideal be a subring? Since a subring needs to contain 1 and an ideal that contains 1 is the whole ring, we see that only the entire ring can be both an ideal and a subring.

Suppose $\varphi : R_1 \to R_2$ is a ring homomorphism between two commutative rings R_1 and R_2. We define the kernel and image of φ by:

$$\ker(\varphi) = \{a \in R_1 : \varphi(a) = 0\} \subseteq R_1 \qquad \text{and} \qquad \operatorname{im}(\varphi) = \{\varphi(a) : a \in R_1\} \subseteq R_2.$$

Proposition 6.23 *Suppose $\varphi : R_1 \to R_2$ is a ring homomorphism between two commutative rings R_1 and R_2. Then:*

(a) $\ker(\varphi)$ *is a proper ideal of* R_1*;*

(b) $\ker(\varphi) = \{0\}$ *if and only if* φ *is injective;*

(c) $\operatorname{im}(\varphi)$ *is a subring of* R_2

(d) $\operatorname{im}(\varphi) = R_2$ *if and only if* φ *is surjective.*

Proof: By the definition of homomorphism and our convention that $1 \neq 0$, we have

$$0 \in \ker(\varphi), \qquad \text{and} \qquad 1 \notin \ker(\varphi).$$

For any $a, b \in \ker(\varphi)$, we have $a+b \in \ker(\varphi)$ since

$$\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$$

and for any $r \in R_1$, we have $ra \in \ker(\varphi)$ since

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0.$$

This proves that $\ker(\varphi)$ is a proper ideal of R_1. Note that for $a, b \in R_1$, we have

$$\varphi(a) = \varphi(b) \quad \iff \quad \varphi(a-b) = 0 \quad \iff \quad a - b \in \ker(\varphi).$$

Hence $\ker(\varphi) = \{0\}$ if and only if φ is injective.

Next we consider $\mathrm{im}(\varphi)$. Since $\varphi(0) = 0$ and $\varphi(1) = 1$, we see that $\mathrm{im}(\varphi)$ contains 0 and 1. Given $a, b \in \mathrm{im}(\varphi)$, there exists $\alpha, \beta \in R_1$ such that $a = \varphi(\alpha)$ and $b = \varphi(\beta)$. Then

$$-a = \varphi(-\alpha), \qquad a + b = \varphi(\alpha + \beta), \qquad ab = \varphi(\alpha\beta)$$

are all in $\mathrm{im}(\varphi)$. Hence $\mathrm{im}(\varphi)$ is a subring of R_2. Statement (d) is simply the definition of surjectivity. □

Corollary 6.24 *Suppose $\varphi : R_1 \to R_2$ is a ring homomorphism between two commutative rings R_1 and R_2. Suppose R_1 is a field. Then φ is injective.*

Proof: The only proper ideal of a field is (0). □

Note that in the above proof, we saw that

$$\varphi(a) = \varphi(b) \quad \iff \quad a - b \in \ker(\varphi) \quad \iff \quad \ker(\varphi) \mid a - b \quad \iff \quad a \equiv b \pmod{\ker(\varphi)}.$$

In other words, the value of $\varphi(a)$ depends only on the "equivalence class of a mod $\ker(\varphi)$". This is essentially the idea of quotients.

Let R be a commutative ring and let I be a proper ideal. We define a relation $\sim$ on R by:

$$a \sim b \quad \iff \quad a - b \in I \quad \iff \quad a \equiv b \pmod{I}.$$

Then just like congruences mod m, this is an equivalence relation. The equivalence classes are also called cosets:

$$[a] = \{b \in R \colon b - a \in I\} = \{a + c \colon c \in I\} = a + I.$$

Two equivalence classes $[a]$ and $[b]$ are equal if and only if $a - b \in I$. We define the set R/I as the set of equivalence classes:

$$R/I = \{[a] \colon a \in R\} = \{a + I \colon a \in R\}.$$

It is worth remarking that so far, all we need is that I is closed under addition and contains 0, in order for $\sim$ to be an equivalence relation. In other words, all of the above works if I is a subring instead. We now define the ring structure exactly mimicing $\mathbb{Z}/m\mathbb{Z}$:

$$\begin{aligned} 0 &= [0] \\ 1 &= [1] \\ [a] + [b] &= [a + b] \\ [a] \cdot [b] &= [ab] \\ -[a] &= [-a]. \end{aligned}$$

We need to check that the above operations are well-defined, in the sense that they don't depend on the choice of the representatives. In other words, if $a \sim c$ and $b \sim d$, then

$$a + b \sim c + d \qquad \text{and} \qquad ab \sim cd \qquad \text{and} \qquad -a \sim -c.$$

These follow exactly like the case of congruences mod m. For example,

$$ab - cd = a(b - d) + d(a - c).$$

From $I \mid b - d$ and $I \mid a - c$, we have $I \mid ab - cd$.

Proposition 6.25 *(Universal property of quotients) Let R be a commutative ring and let I be a proper ideal. Then R/I with the above operations is a commutative ring. It is the unique ring structure on R/I for which the natural map $R \to R/I$ sending a to $[a]$ is a ring homomorphism. Moreover, given any ring homomorphism $\varphi : R \to S$ for which $I \subseteq \ker(\varphi)$, there is a unique ring homomorphism $\psi : R/I \to S$ for which the composition $R \to R/I \to S$ is φ.*

Proof: Exercise. This is a very tedious definition check. It is worth doing exactly once in your life. Note that $\psi([a]) = \varphi(a)$. □

Lecture 17 Fri 10/11

First isomorphism theorem, Chinese remainder theorem

Recall that for a ring homomorphism $\varphi : R \to S$, its kernel $\ker(\varphi)$ is an ideal of R and its image $\mathrm{im}(\varphi)$ is a subring of S. Since $\mathrm{im}(\varphi)$ itself is a ring and φ only "see" its image, we may view $\varphi : R \to \mathrm{im}(\varphi)$. Now the kernel of φ contains (in fact, equals) $\ker(\varphi)$. Hence by the universal property (Proposition 6.25), φ "factors through"

$$R/\ker(\varphi) \to \mathrm{im}(\varphi).$$

There is now no more redundant information left.

Theorem 6.26 *(First isomorphism theorem) Let $\varphi : R \to S$ be a homomorphism of rings. Then the natural map $\psi : R/\ker(\varphi) \to \mathrm{im}(\varphi)$ sending the coset $[a] = a + \ker(\varphi)$ to $\varphi(a)$ is an isomorphism.*

Proof: We only need to check that ψ is bijective. For every $\varphi(a) \in \mathrm{im}(\varphi)$, we have $\varphi(a) = \psi([a]) \in \mathrm{im}(\psi)$, so the map is surjective. If $\psi([a]) = 0$, then $\varphi(a) = 0$ and so $a \in \ker(\varphi)$ but then $[a] = [0]$. Hence $\ker(\psi) = 0$ and so ψ is injective. □

Let's apply the first isomorphism theorem to the canonical homomorphism $f : \mathbb{Z} \to R$. Let m denote the characteristic of R. Then Lemma 6.7 implies that $\ker(f) = m\mathbb{Z}$. The image of f is then a subring of R isomorphic to $\mathbb{Z}/m\mathbb{Z}$. This is called the prime subring of R. Note also that if f is surjective, then $R \cong \mathbb{Z}/m\mathbb{Z}$.

Our next goal is to use the similarity between congruence classes mod I and congruences mod m to come up with and prove a ring theoretic version of the Chinese Remainder Theorem: Let m and n be coprime integers. Let a and b be integers. Then there exist a unique integer x mod mn such that

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

We want to replace the integers a, b, m, n by elements a, b, r, s of a commutative ring R. Now

$$x \equiv a \pmod{r} \iff r \mid x - a \iff x - a \in (r) \iff x + (r) = a + (r).$$

The existence of a solution is saying that the natural homomorphism

$$\begin{aligned} \varphi : R &\longrightarrow R/(r) \times R/(s) \\ x &\longmapsto (x + (r), x + (s)) \end{aligned}$$

is surjective. The uniqueness of a solution mod mn then says that the kernel of φ is exactly (rs), so that the first isomorphism theorem implies that

$$R/(rs) \cong R/(r) \times R/(s).$$

What does it mean for r, s to be coprime? Two integers m, n are coprime if and only if 1 is the only positive integer d such that $d \mid m$ and $d \mid n$. Using our philosophy of generalizing numbers to ideals, it is then natural to say two elements $r, s \in R$ are coprime if and only if $(1) = R$ is the only ideal I such that $I \mid r$ and $I \mid s$, where recall that the ideal divisions mean that $r \in I$ and $s \in I$. What is the smallest ideal containing r and s? We define

$$(r, s) = (r) + (s) = \{rx + sy \colon x, y \in R\}.$$

In the setting of general rings, we will use the ideal (r, s) to replace the notion of $\gcd(r, s)$.

Theorem 6.27 *(Chinese remainder theorem) Let R be a commutative ring. Let $r, s \in R$ such that $(r, s) = R$. Then*

$$R/(rs) \cong R/(r) \times R/(s).$$

There is in fact a more general version replacing (r) and (s) by two ideals I and J. We define

$$\begin{aligned} I + J &= \{a + b \colon a \in I, b \in J\} \\ IJ &= \{a_1 b_1 + \cdots + a_m b_m \colon a_i \in I, b_i \in J, m \geq 0\}. \end{aligned}$$

Theorem 6.28 *(Chinese remainder theorem) Let R be a commutative ring. Let I and J be two proper ideals of R such that $I + J = R$. Then the natural map*

$$\varphi : r \mapsto (r + I, r + J) \colon R \to R/I \times R/J$$

is a surjective homomorphism with kernel IJ. In other words,

$$R/(IJ) \cong R/I \times R/J.$$

Proof: The assumption $I + J = R$ means that there exist $a \in I$ and $b \in J$ such that $a + b = 1$. We prove φ is surjective. Take any $s, t \in R$. We need to find an $r \in R$ such that $r - s \in I$ and $r - t \in J$. Let $r = ta + sb$. Then

$$\begin{aligned} r - s &= ta + s(b - 1) = ta - sa \in I, \\ r - t &= t(a - 1) + sb = -tb + sb \in J. \end{aligned}$$

The kernel of φ is clearly $I \cap J$. It is easy to see by definition that $IJ \subseteq I \cap J$, so it remains to prove $I \cap J \subseteq IJ$. Let $r \in I \cap J$. Then $r = r(a + b) = ra + rb \in IJ$. □

Lecture 17.5 Fri 10/11
Tutorial
Correspondence, 3rd isomorphism theorems

We saw previously that the ideals of $\mathbb{Z}/69\mathbb{Z}$ correspond exactly to the ideals of $\mathbb{Z}$ containing 69, which is the same containing $69\mathbb{Z}$. This is no coincidence!

Theorem 6.29 *(Correspondence Theorem) Let R be a commutative ring and let I be a proper ideal of R. Then there is a bijection between the set of ideals of R/I, and the set of ideals of R containing I.*

Proof: Consider the natural map $\varphi : R \to R/I$ sending a to $[a] = a + I$.

- For any ideal J of R containing I, its image $\varphi(J) =: J/I = \{[a] \colon a \in J\}$ is an ideal of R/I.

  It clearly contains $[0]$. If $a, b \in J$, then $a + b \in J$ and so $[a] + [b] = [a + b] \in J/I$. If $a \in J$ and $r \in R$, then $ra \in J$ and so $[r][a] = [ra] \in J/I$.

- For any ideal J' of R/I, its preimage $\varphi^{-1}(J') = \{a \in R \colon [a] \in J'\}$ is an ideal of R containing I.

  For any $a \in I$, we have $[a] = [0] \in J'$ and so $I \subseteq \varphi^{-1}(J')$. If $a, b \in R$ such that $[a], [b] \in J'$, then $[a + b] = [a] + [b] \in J'$ and so $a + b \in \varphi^{-1}(J')$. If $a, r \in R$ such that $[a] \in J'$, then $[ra] = [r][a] \in J'$ and so $ra \in \varphi^{-1}(J')$.

We need to check that the above maps between sets of ideals are bijections. That is, for any ideal J of R containing I,

$$\varphi^{-1}(\varphi(J)) = \{a \in R \colon [a] \in \varphi(J)\} = \{a \in R \colon [a] = [b] \text{ for some } b \in J\} = J$$

and for any ideal J' of R/I,

$$\varphi(\varphi^{-1}(J')) = \{[a]\colon a \in \varphi^{-1}(J')\} = \{[a]\colon [a] \in J'\} = J'.$$

In the first equality, we had $a - b \in I$ and since $I \subseteq J$, we have $a - b \in J$ and so $a = (a - b) + b \in J$. □

Recall also that we have a homomorphism $\mathbb{Z}/69\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ sending $a + 69\mathbb{Z}$ to $a + 3\mathbb{Z}$. This map is surjective with kernel $\{a + 69\mathbb{Z}\colon 3 \mid a\} = \{a + 69\mathbb{Z}\colon a \in 3\mathbb{Z}\}$. In the above notation, this is $3\mathbb{Z}/69\mathbb{Z}$ with $I = 69\mathbb{Z}$ and $J = 3\mathbb{Z}$. The first isomorphism theorem now gives

$$(\mathbb{Z}/69\mathbb{Z})/(3\mathbb{Z}/69\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z}.$$

It's like we can "cancel the denominators"!

Theorem 6.30 *(Third isomorphism theorem) Let R be a commutative ring and let I be a proper ideal of R. Let J be a proper ideal of R containing I. Then*

$$(R/I)/(J/I) \cong R/J.$$

Proof: There are multiple ways to do this. We take the composition of the natural maps:

$$\psi : R \to R/I \to (R/I)/(J/I).$$

Since both quotient maps are surjective, so is ψ. By the first isomorphism theorem, it suffices to prove that $\ker(\psi) = J$. This is now just a definition check. We write $[a] = a + I \in R/I$. Then

$$\ker(\psi) = \{a \in R\colon [a] \in J/I\} = \varphi^{-1}(J/I) = \varphi^{-1}(\varphi(J)) = J$$

where $\varphi : R \to R/I$. □

The third isomorphism theorem is typically used to study quotients of the form $R/(a, b)$. Let $J = (a, b)$ and $I = (a)$. We can first consider the quotient $\varphi : R \to R/(a)$. Then we look at the image $\varphi(J) = J/I$ of J. Note that the map φ "kills" one of the generators of J. So $\varphi(J)$ is simply the principal ideal $(\varphi(b))$ of $R/(a)$.

As an example, we have the ring $R = \mathbb{Z}[x]$ of polynomials with integer coefficients. We will start discussing rings of this form in more detail next time. Consider the ideal

$$J = (2, x) = \{2f(x) + xg(x)\colon f, g \in \mathbb{Z}[x]\} = \{h(x) \in \mathbb{Z}[x]\colon 2 \mid h(0)\}.$$

To find $\mathbb{Z}[x]/(2, x)$, we can first mod out by x, and then mod out by 2. When modding out by x, we are basically setting $x = 0$ so we have $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. Under the quotient map $\mathbb{Z}[x] \to \mathbb{Z}[x]/(x) \cong \mathbb{Z}$, the other generator 2 gets send to 2. So

$$\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/(2) = \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2.$$

We can also mod out by 2 first, and then mod out by x. When modding out by 2, we are essentially reducing the coefficients mod 2 but aren't touching the x. So $\mathbb{Z}[x]/(2) \cong (\mathbb{Z}/2\mathbb{Z})[x] = \mathbb{F}_2[x]$ is the ring of polynomials with coefficients in $\mathbb{F}_2$. Under the quotient map $\mathbb{Z}[x] \to \mathbb{F}_2[x]$, the other generator x gets send to x. So

$$\mathbb{Z}[x]/(2, x) \cong \mathbb{F}_2[x]/(x) \cong \mathbb{F}_2.$$

Exercise: Prove all of the above isomorphisms.

Here is a more complicated example. What is $\mathbb{Z}[i]/(2 + i)$? You will prove in HW 6 that

$$\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2 + 1).$$

More explicitly, the quotient map $\mathbb{Z}[x] \to \mathbb{Z}[i]$ sends x to i. It will then send $2 + x$ to $2 + i$. Hence, we have

$$\mathbb{Z}[i]/(2 + i) \cong \mathbb{Z}[x]/(x^2 + 1, x + 2).$$

We can now compute this quotient by modding out $x + 2$ first. When modding out $x + 2$, we are basically setting $x + 2 = 0$, i.e. setting $x = -2$. So $\mathbb{Z}[x]/(x + 2) \cong \mathbb{Z}$ with the quotient map $\mathbb{Z}[x] \to \mathbb{Z}$ sending $f(x)$ to $f(-2)$. Under this map, the other generator $x^2 + 1$ gets send to 5. So we have

$$\mathbb{Z}[i]/(2 + i) \cong \mathbb{Z}[x]/(x^2 + 1, x + 2) \cong \mathbb{Z}/(5) = \mathbb{F}_5.$$

Exercises

6.1 Let R be a commutative ring with $a, b, c \in R$. Prove that if $ab = 1 = ac$, then $b = c$.

6.2 Let $f : R \to R'$ be an isomorphism between two commutative rings. Prove that its inverse $f^{-1} : R' \to R$ is a ring homomorphism, and so is also an isomorphism. (Recall that f^{-1} is defined so that for any $b \in R'$, $f^{-1}(b)$ is the unique $a \in R$ such that $f(a) = b$.)

6.3 Prove that $\mathbb{R}$ and $\mathbb{C}$ are not isomorphic.

6.4 Let $R = \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$. Let $r = (0, 1)$. Prove that:

(a) whenever $r \mid ab$ for some $a, b \in R$, we have $r \mid a$ or $r \mid b$;

(b) there exist $a, b \in R \backslash R^\times$ such that $r = ab$.

6.5 Let $R = \mathbb{Q} + x\mathbb{R}[x] = \{f(x) \in \mathbb{R}[x] \colon f(0) \in \mathbb{Q}\}$. Prove that:

(a) there exist $a, b \in R$ such that $x \mid ab$ but $x \nmid a$ and $x \nmid b$;

(b) there do not exist $a, b \in R \backslash R^\times$ such that $x = ab$.

6.6 Let R be the ring of continuous (real-valued) functions on $[0, 3]$ with pointwise addition and multiplication, and the constant functions 0 and 1 as 0 and 1. Consider

$$a(x) = \begin{cases} 1 - x & \text{if } 0 \le x \le 1 \\ 0 & \text{if } 1 \le x \le 2 \\ x - 2 & \text{if } 2 \le x \le 3 \end{cases}, \qquad b(x) = \begin{cases} 1 - x & \text{if } 0 \le x \le 1 \\ 0 & \text{if } 1 \le x \le 2 \\ 2 - x & \text{if } 2 \le x \le 3 \end{cases}.$$

Prove that $a(x)R = b(x)R$ but there does not exist a unit $u(x) \in R^\times$ such that $b(x) = a(x)u(x)$.

Lecture 18 Mon 10/21
$R[x]$

7 Polynomial ring

For any commutative ring R, we let $R[x]$ denote the ring of polynomials with coefficients in R very similar to $\mathbb{Z}[x]$. That is,

$$R[x] = \{a_n x^n + \cdots + a_0 \colon a_i \in R, n \ge 0\}.$$

Two polynomials $a_n x^n + \cdots + a_0$ and $b_m x^m + \cdots + b_0$ are said to be equal if $n = m$ and $a_i = b_i$ for all i. Addition and multiplication of polynomials are exactly what you expected: multiply things out and then collect terms with the same degree. For example, in $(\mathbb{Z}/69\mathbb{Z})[x]$, we have

$$\begin{aligned} & ([23]x^2 + [3]x + [1])([3]x^3 + [4]x) \\ = \; & [69]x^5 + [92]x^3 + [9]x^4 + [12]x^2 + [3]x^3 + [4]x \\ = \; & [9]x^4 + [26]x^3 + [12]x^2 + [4]x. \end{aligned}$$

We define the degree of a polynomial $a_n x^n + \cdots + a_0 \in R[x]$ as the largest index n such that $a_n \neq 0$. We then say a_n is the leading coefficient. If $a_n = 1$, we say the polynomial is monic. We follow the convention of $\deg(0) = -\infty$. Note that

$$(a_n x^n + \cdots)(b_m x^m + \cdots) = a_n b_m x^{m+n} + \cdots$$

has no terms of exponent higher than $m + n$. Hence, we see that

$$\deg(fg) \le \deg(f) + \deg(g).$$

In our example above, we see that equality might not hold because we could have $a_n \neq 0$ and $b_m \neq 0$ but $a_n b_m = 0$. This is clearly not possible if R is an integral domain.

Lemma 7.1 *Let R be an integral domain. Then for any $f, g \in R[x]$, we have* $\deg(fg) = \deg(f) + \deg(g)$.

We may view R as a subring of $R[x]$ by viewing every $r \in R$ as the degree 0 constant polynomial $r \in R[x]$. Conversely, it is easy to see that the degree 0 polynomials are exactly the nonzero constants.

Lemma 7.2 *Let R be an integral domain. Then $R[x]^\times = R^\times$.*

Proof: In order for $fg = 1$, we have $\deg(f) + \deg(g) = 0$ and so both $\deg(f) = \deg(g) = 0$ implying that f and g are nonzero elements of R that multiply to 1. □

One of the most fundamental property of polynomials is the existence of a division algorithm.

Proposition 7.3 *(Division algorithm for polynomials) Let R be a commutative ring. Let $f(x) \in R[x]$ and let $g(x) \in R[x]$ such that the leading coefficient of g is a unit in R. Then there exist polynomials $q(x), r(x) \in R[x]$ such that*

$$f(x) = g(x)q(x) + r(x), \qquad \text{and} \qquad \deg(r) < \deg(g).$$

Proof: Just long division. Let a denote the leading coefficient of $g(x)$. So $a \in R^\times$. If $g(x) = a$ has degree 0, then we take $q(x) = a^{-1}f(x)$ and $r(x) = 0$. Suppose now $\deg(g) > 0$. We prove by induction on $\deg(f)$. If $\deg(f) < \deg(g)$, we simply take $q = 0$ and $r = f$. Suppose now $\deg(f) \geq \deg(g)$. Let $b \in R$ be the leading coefficient of $f(x)$. Then

$$f(x) - ba^{-1}x^{\deg(f)-\deg(g)}g(x)$$

is a polynomial with less degree than f. By the induction hypothesis, this can be written $gq_1 + r_1$ with $\deg(r_1) < \deg(g)$. Then $f = gq + r$ with $q = ba^{-1}x^{\deg(f)-\deg(g)} + q_1$. □

When $R = \mathbb{Z}$, the condition that the leading coefficient of g is unit means that it is ± 1. In general, we can always divide by monic polynomials.

For any commutative ring R and any $\alpha \in R$, there is an evaluation homomorphism $\mathrm{ev}_\alpha : R[x] \to R$ sending

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \quad \longmapsto \quad a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0.$$

We write $f(\alpha) \in R$ for the image of f under this map. For any constant polynomial $r \in R$, we have $\mathrm{ev}_\alpha(r) = r$. Hence ev_α is surjective. Its kernel is given

$$\ker(\mathrm{ev}_\alpha) = \{f(x) \in R[x] \colon f(\alpha) = 0\}.$$

It is clear that $x - \alpha \in \ker(\mathrm{ev}_\alpha)$. So $(x - \alpha) \subseteq \ker(\mathrm{ev}_\alpha)$.

Proposition 7.4 *Let R be a commutative ring. Let $f(x) \in R[x]$ and let $c \in R$. The remainder when $f(x)$ is divided by $x - c$ is the constant polynomial $f(c)$.*

Proof: The remainder $r(x)$ satisfies $\deg(r) < \deg(x - c) = 1$. So $r(x) = r_0$ is a constant. Apply ev_c to $f(x) = (x - c)q(x) + r_0$ to get $r_0 = f(c)$. □

As a consequence, we have $\ker(\mathrm{ev}_\alpha) = (x - \alpha)$ since $f(\alpha) = 0$ implies that $f(x)$ is divisible by $x - \alpha$. Hence by the first isomorphism theorem, we have

$$R[x]/(x - \alpha) \cong R.$$

Corollary 7.5 *Let R be an integral domain. Let $f(x) \in R[x]$ and let $c_1, \ldots, c_n \in R$ be distinct. Then $c_1, \ldots, c_n$ all are roots of $f(x)$ if and only if $(x - c_1)(x - c_2)\cdots(x - c_n) \mid f(x)$.*

Proof: Only the forwards direction needs to be proved. We prove by induction on n. The case $n = 1$ follows immediately from Proposition 7.4. Suppose now $n \geq 2$. By induction using $c_1, \ldots, c_{n-1}$, we see that there exists $g(x) \in R[x]$ such that $f(x) = (x - c_1)\cdots(x - c_{n-1})g(x)$. Apply ev_{c_n} to get

$$0 = (c_n - c_1)\cdots(c_n - c_{n-1})g(c_n).$$

Since each $c_n - c_i \neq 0$ and R is an integral domain, we see that $g(c_n) = 0$. Then $g(x) = (x - c_n)h(x)$ for some $h \in R[x]$. So $f(x) = (x - c_1)\cdots(x - c_n)h(x)$. □

Corollary 7.6 *Let R be an integral domain. Let $f(x) \in R[x]$ with degree $d \geq 0$. Then $f(x)$ has at most d distinct roots in R.*

We say $c \in R$ is a repeated root of $f(x)$ if $(x-c)^2 \mid f(x)$. Repeated roots can be checked using the formal derivative of $f(x)$ defined as

$$f'(x) = na_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

The word "formal" is referring to the fact that this has nothing to do with taking limits. The same rules of derivatives in calculus apply here:

$$(f+g)'(x) = f'(x) + g'(x), \qquad (fg)'(x) = f(x)g'(x) + f'(x)g(x), \qquad (f \circ g)'(x) = f'(g(x))g'(x).$$

Additivity is easy to check from the definition. Then one can use it to reduce the product rule and the chain rule to the case $f(x) = a_n x^n$.

As an example, consider $R = \mathbb{F}_p$ and the polynomials $f(x) = x^p - x$ and $g(x) = x^p - 1$. Then,

$$f'(x) = px^{p-1} - 1 = -1, \qquad g'(x) = px^{p-1} = 0.$$

Proposition 7.7 *Let R be a commutative ring. Let $f(x) \in R[x]$ and let $c \in R$. Then c is a repeated root of $f(x)$ if and only if $f(c) = f'(c) = 0$.*

Proof: For both directions, we may assume c is a root. So $f(x) = (x-c)g(x)$ for some $g(x) \in R[x]$. Differentiate it to get $f'(x) = g(x) + (x-c)g'(x)$. Hence $f'(c) = g(c)$. So $g(x)$ has another factor of $x - c$ if and only if $f'(c) = 0$. □

The polynomial $x^p - x$ has derivative -1, which has no root. Hence $x^p - x$ has no repeated roots in $\mathbb{F}_p$. In fact, every $a \in \mathbb{F}_p^\times$ satisfies $a^{p-1} = 1$ by Fermat's little theorem (or by $|\mathbb{F}_p^\times| = p - 1$). Hence the p elements $0, 1, \ldots, p-1 \in \mathbb{F}_p$ are distinct and are all roots of $x^p - x$. Since $\deg(x^p - x) = p$, we have the factorization

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

The polynomial $x^p - 1$ has derivative 0 and has 1 as a root. Hence it has 1 as a repeated root. In fact

$$x^p - 1 = (x-1)^p.$$

Lemma 7.8 *Let R be a commutative ring of characteristic p where p is a prime. Then for any $a, b \in R$ and any $n \in \mathbb{N}$, we have*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Proof: By the Binomial Theorem, we have

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \cdots + b^p.$$

We saw before that for $k = 1, \ldots, p-1$ (Lemma 3.10), the binomial coefficient $\binom{p}{k}$ is divisible by p, which makes it 0 in R. Hence, we have $(a+b)^p = a^p + b^p$. Repeated raising p-th power gives the desired result. □

Lecture 19 Wed 10/23

$F[x]$

We now focus on the case where $R = F$ is a field. Recall that in the division algorithm of $f(x)$ by $g(x)$, we needed the leading coefficient of $g(x)$ to be a unit. When $R = F$ is a field, this condition is just that $g(x) \neq 0$ as the leading coefficient of $g(x)$ would then be nonzero and so a unit in F. In other words, $F[x]$ is a Euclidean domain with deg as the function $N : F[x]\backslash\{0\} \to \mathbb{N} \cup \{0\}$ and so is a PID! That is, every ideal is principal.

We now define irreducible polynomials in $F[x]$ similar to prime numbers in $\mathbb{Z}$. A polynomial $f(x) \in F[x]$ is irreducible if $\deg(f) \geq 1$ and there does not exist polynomials $a(x), b(x) \in F[x]$ of degree at least 1 such that $a(x)b(x) = f(x)$. By Proposition 7.4, if $f(x)$ has a root $c \in F$, then $x - c \mid f(x)$. So if $f(x)$ is irreducible of degree at least 2, then $f(x)$ has no roots in F. Conversely, if $f(x) = a(x)b(x)$ is reducible and has degree at most 3, then at least one of $a(x)$ and $b(x)$ has degree 1 and $f(x)$ will have a root.

Lemma 7.9 *Let F be a field. Linear (degree 1) polynomials in $F[x]$ are all irreducible. Quadratic (degree 2) and cubic (degree 3) polynomials in $F[x]$ are irreducible if and only if they don't have a root in F.*

For example, $x^2 + 1$ is irreducible in $\mathbb{Q}[x]$ and in $\mathbb{R}[x]$ because it doesn't have roots in $\mathbb{Q}$ or $\mathbb{R}$, but is reducible in $\mathbb{C}[x]$ because $i \in \mathbb{C}$ is a root and so $x^2 + 1 = (x + i)(x - i)$. Is $x^2 + 1$ irreducible in $\mathbb{F}_2[x]$? No, because 1 is a root and in fact $x^2 + 1 = (x + 1)^2$ in $\mathbb{F}_2[x]$. What about $\mathbb{F}_3[x]$? There are only three elements in $\mathbb{F}_3$: 0, 1, 2; and we can check that none of them are roots:

$$0^2 + 1 = 1, \qquad 1^2 + 1 = 2, \qquad 2^2 + 1 = 5 = 2.$$

So $x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$. If we try this with $\mathbb{F}_5$, then we find that

$$2^2 + 1 = 5 = 0 \qquad \text{and} \qquad 3^2 + 1 = 10 = 0.$$

Hence $x^2 + 1 = (x - 2)(x - 3) \in \mathbb{F}_5[x]$ is not irreducible. For which prime p is $x^2 + 1$ irreducible in $\mathbb{F}_p[x]$? We saw before that if $x^2 \equiv -1 \pmod{p}$ has a solution, then $p \equiv 1 \pmod{4}$. We will see very soon that the converse is true: if $p \equiv 1 \pmod{4}$, then -1 is a square mod p. So $x^2 + 1$ is irreducible in $\mathbb{F}_p[x]$ if and only if $p \equiv 3 \pmod{4}$.

A degree 4 polynomial can be reducible without having a root. For example, we can simply take the product of two irreducible polynomials of degree 2. Here is a more interesting one. The polynomial $x^4 + 1$ has no root in $\mathbb{F}_3[x]$ by plug-and-check. Note that in $\mathbb{F}_3[x]$, we have

$$(x^2 - 1)^2 = x^4 - 2x^2 + 1 = x^4 + x^2 + 1$$

and so

$$x^4 + 1 = (x^2 - 1)^2 - x^2 = (x^2 + x - 1)(x^2 - x - 1).$$

Challenge question: For which prime p is $x^4 + 1$ irreducible in $\mathbb{F}_p[x]$? Depending on your background, this may or may not be doable yet. Try asking Wolfram Alpha! We will discuss this later.

Note that $x^2 + 1$ has very different factorization behavior in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$ or $\mathbb{F}_5[x]$. Namely, $x^2 + 1$ has a repeated factor in $\mathbb{F}_2[x]$, is irreducible in $\mathbb{F}_3[x]$, and is the product of two distinct monic linear polynomial in $\mathbb{F}_5[x]$. What can we say about the quotients $\mathbb{F}_2[x]/(x^2 + 1)$, $\mathbb{F}_3[x]/(x^2 + 1)$ and $\mathbb{F}_5[x]/(x^2 + 1)$?

Let's consider $\mathbb{F}_2[x]/(x^2 + 1)$ first. How many elements does it have? We write $[f(x)]$ for the coset $f(x) + (x^2 + 1)$. Recall that

$$[f(x)] = [g(x)] \iff f(x) - g(x) \in (x^2 + 1) \iff x^2 + 1 \mid f(x) - g(x).$$

For $\deg(f) \leq 0$, we have $[0]$ and $[1]$. For $\deg(f) = 1$, we have $[x]$ and $[x + 1]$. All of these four elements are distinct, because their differences have degree at most 1 and so can't be divisible by $x^2 + 1$. What about $[x^2]$? This is the same as $[1]$ since $x^2 - 1 = x^2 + 1 \in (x^2 + 1)$. Similarly, for any $f(x)$ with $\deg(f) \geq 2$, we can apply the division algorithm to divide $f(x)$ by $x^2 + 1$ to find that $f(x) = (x^2 + 1)q(x) + r(x)$ for some $q, r \in \mathbb{F}_2[x]$ with $\deg(r) < \deg(x^2 + 1) = 2$. Then $[f(x)] = [r(x)]$ and $r = 0, 1, x, x + 1$. Hence

$$\mathbb{F}_2[x]/(x^2 + 1) = \{[0], [1], [x], [x + 1]\}$$

is a ring of order 4. Is this isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = \mathbb{F}_2 \times \mathbb{F}_2$? No. Since $2 = 0$ in $\mathbb{F}_2$, this ring has characteristic 2 and so can't be $\mathbb{Z}/4\mathbb{Z}$. Note that $[x + 1]^2 = [(x + 1)^2] = [x^2 + 1] = [0]$. In the language of HW 7 P1, $\mathbb{F}_2[x]/(x^2 + 1)$ has a nonzero nilpotent element, but $\mathbb{F}_2 \times \mathbb{F}_2$ doesn't. In fact, $\mathbb{F}_2 \times \mathbb{F}_2$ has the special property that every element squares to itself! You will explore this in HW 7 P2.

We consider $\mathbb{F}_5[x]/(x^2+1)$ next. In this case,

$$\mathbb{F}_5[x]/(x^2+1) = \mathbb{F}_5[x]/((x-2)(x-3)).$$

We can now apply the Chinese Remainder Theorem (Theorem 6.27). We need to check that $x-2$ and $x-3$ are coprime. Note that $1 = (x-2) + (-1)(x-3) \in (x-2, x-3)$. So $(x-2, x-3) = \mathbb{F}_5[x]$. Hence

$$\mathbb{F}_5[x]/((x-2)(x-3)) \cong \mathbb{F}_5[x]/(x-2) \times \mathbb{F}_5[x]/(x-3) \cong \mathbb{F}_5 \times \mathbb{F}_5.$$

The ring $\mathbb{F}_3[x]/(x^2+1)$ is the most interesting. Note that the same argument for $\mathbb{F}_2[x]/(x^2+1)$ gives the following general result.

Lemma 7.10 *Let F be a field. Let $g(x) \in F[x]$ be a polynomial of degree $d \geq 1$. Then*

$$F[x]/(g(x)) = \{[f(x)] \colon f(x) \in F[x], \deg(f) < d\}.$$

If F is finite, then

$$|F[x]/(g(x))| = |F|^d.$$

Applying this, we have

$$\mathbb{F}_3[x]/(x^2+1) = \{[0], [1], [2], [x], [x+1], [x+2], [2x], [2x+1], [2x+2\}$$

is a ring of order 9. Strongly recommended exercise: Work out its multiplication table. For example,

$$[x][2x+1] = [2x^2+x] = [2x^2+x-2(x^2+1)] = [x-2] = [x+1].$$

Lecture 20 Fri 10/25

$\mathbb{F}_{p^2}$

After working out the multiplication table, you would find that $\mathbb{F}_3[x]/(x^2+1)$ is a field of order 9. Two natural questions arise. Is there a way to figure this out without doing the calculation? Can we do something similar to construct a field of order 4?

Imagine trying to show that $[x+1]$ is a unit in $\mathbb{F}_3[x]/(x^2+1)$. This amounts to proving the existence of some $f(x) \in \mathbb{F}_3[x]$ such that

$$(x+1)f(x) - 1 \in (x^2+1).$$

In other words, we want to show that there exists $f(x), g(x) \in \mathbb{F}_3[x]$ such that

$$(x+1)f(x) + (x^2+1)g(x) = 1.$$

This is the same as proving that the ideal $(x+1, x^2+1)$ is the entire ring, since we want it to contain 1. Now $\mathbb{F}_3[x]$ is a PID, so we know $(x+1, x^2+1) = (h(x))$ for some polynomial $h(x) \in \mathbb{F}_3[x]$. Note that this implies $h(x) \mid x^2+1$. However, x^2+1 is irreducible! So either $h(x)$ is a unit, or $h(x)$ is a unit times x^2+1. If $h(x)$ is a unit, then $(x+1, x^2+1)$ is the entire ring as desired. If $h(x)$ is a unit times x^2+1, then from $h(x) \mid x+1$, we get $x^2+1 \mid x+1$, which is not possible for degree reasons, but more intrinsically contradicts $[x+1] \neq 0$. We have thus given a proof by example of $(a) \Rightarrow (b)$ below:

Proposition 7.11 *Let F be a field and let $g(x) \in F[x]$ with degree at least 1. Then the following are equivalent:*

(a) $g(x)$ is irreducible.

(b) $F[x]/(g(x))$ is a field;

(c) $F[x]/(g(x))$ is an integral domain;

Proof: $(b) \Rightarrow (c)$ follows because fields are integral domains (Lemma 6.1(c)). To prove $(c) \Rightarrow (a)$, we consider its contrapositive. Suppose $g(x)$ is reducible. (This is essentially the $\mathbb{F}_2[x]/(x^2+1)$ and $\mathbb{F}_5[x]/(x^2+1)$ example.) By definition, $g(x) = a(x)b(x)$ for some $a(x), b(x) \in F[x]$ with degrees between 1 and $\deg(g) - 1$. Then $[a(x)]$ and $[b(x)]$ are nonzero in $F[x]/(g(x))$ but their product is $[g(x)] = [0]$. Hence $F[x]/(g(x))$ is not an integral domain. This proves $(b) \Rightarrow (c)$. □

We can now answer our second question. To construct a field of order 4, we can try finding an irreducible polynomial $g(x) \in \mathbb{F}_2[x]$ of degree 2 so that $\mathbb{F}_2[x]/(g(x))$ is a field of order $2^2 = 4$. We need $g(0) \neq 0$ so $g(x) = x^2 + ax + 1$. We need $g(1) \neq 0$, so $g(1) = a \neq 0$. Then $g(x) = x^2 + x + 1$ is the unique irreducible polynomial of $\mathbb{F}_2[x]$ of degree 2. We then have our $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$.

Let's find all irreducible polynomials in $\mathbb{F}_2[x]$ of degree 3. The same characterization using roots applies. From $g(0) \neq 0$, we have $g(x) = x^3 + ax^2 + bx + 1$ for some $a, b \in \mathbb{F}_2$. From $g(1) \neq 0$, we have $a + b \neq 0$. So there are two choices: $a = 1, b = 0$ or $a = 0, b = 1$. i.e

$$x^3 + x^2 + 1 \qquad \text{and} \qquad x^3 + x + 1.$$

Then both $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ and $\mathbb{F}_2[x]/(x^3 + x + 1)$ are fields of order 8. Are they isomorphic?

What about irreducible polynomials in $\mathbb{F}_2[x]$ of degree 4? We can list out all polynomials $x^4 + ax^3 + bx^2 + cx + 1$ with $a + b + c \neq 0$ (so that it has no root in $\mathbb{F}_2$), and then remove the any polynomial that is a product of two irreducible quadratic polynomials. Since $x^2 + x + 1$ is the only irreducible quadratic polynomial, we just need to remove $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. So we have

$$x^4 + x^3 + x^2 + x + 1 \qquad \text{and} \qquad x^4 + x^3 + x \qquad \text{and} \qquad x^4 + x + 1.$$

Challenging question: Note that $x^4 + x^3 + x^2 + x + 1 = \Phi_5(x)$ and $x^2 + x + 1 = \Phi_3(x)$. When is $\Phi_m(x)$ irreducible in $\mathbb{F}_2[x]$? Given a prime p and a degree $d \geq 1$, is there always an irreducible polynomial in $\mathbb{F}_p[x]$ of degree d? I can't write down an irreducible polynomial in $\mathbb{F}_2[x]$ of degree 69, but

$$x^{420} + x^{419} + \cdots + x + 1 = \Phi_{421}(x)$$

is irreducible of degree 420.

Proposition 7.12 *Let $p > 2$ be a prime. Then there exists $r \in \mathbb{F}_p$ such that $x^2 - r$ is irreducible in $\mathbb{F}_p[x]$. We can then take $\mathbb{F}_{p^2} \cong \mathbb{F}_p[x]/(x^2 - r)$.*

Proof: We need to show the existence of some $r \in \mathbb{F}_p$ that is not the square of some element of $\mathbb{F}_p$. We can simply count the squares in $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$. Note that for any $a = 1, 2, \ldots, (p-1)/2$, we have

$$a^2 = (-a)^2 = (p-a)^2$$

while $p - a$ covers all the values $(p+1)/2, \ldots, p-1$. So there are at most $(p+1)/2 = (p-1)/2 + 1$ squares in $\mathbb{F}_p$. Now $p - (p+1)/2 = (p-1)/2 \geq 1$ and so we may take r to be one of the non-squares. Then $x^2 - r$ has no root in $\mathbb{F}_p$. □

It is easy to check that the squares $1^2, 2^2, \ldots, ((p-1)/2)^2$ are distinct in $\mathbb{F}_p$, as $a^2 = b^2$ iff $a^2 - b^2 = (a-b)(a+b) = 0$ iff $a = \pm b$. So there are exactly $(p-1)/2$ nonzero squares. It turns out (which we will prove later) that if r and s are two non-squares, then r/s is a square. For example, in $\mathbb{F}_7$, the nonzero squares are $1, 2, 4$ and the non-squares are $3, 5 = 3 \cdot 4, 6 = 3 \cdot 2$. Let's prove that $\mathbb{F}_7[x]/(x^2 - 3)$ and $\mathbb{F}_7[x]/(x^2 - 5)$ are isomorphic.

- Since $\mathbb{F}_7[x]/(x^2 - 5)$ is a field, any homomorphism from it is automatically injective (Corollary 6.24).
- Since $\mathbb{F}_7[x]/(x^2 - 5)$ and $\mathbb{F}_7[x]/(x^2 - 3)$ have the same size 49, any injective homomorphism between them is automatically surjective and so an isomorphism.
- To write down a homomorphism $\mathbb{F}_7[x]/(x^2 - 5) \to \mathbb{F}_7[x]/(x^2 - 3)$, it is the same to write down a homomorphism $\varphi : \mathbb{F}_7[x] \to \mathbb{F}_7[x]/(x^2 - 3)$ such that $\varphi(x^2 - 5) = 0$ (Proposition 6.25).

- Since $\varphi(1) = 1$, it must be the identity map on $\mathbb{F}_7$ and so is completely determined by $\beta = \varphi(x)$ because for $a_i \in \mathbb{F}_7$,

$$\varphi(a_n x^n + \cdots + a_0) = a_n \varphi(x)^n + \cdots + a_0 = a_n \beta^n + \cdots + a_0.$$

- The condition $\varphi(x^2 - 5) = 0$ translates to $\beta^2 - 5 = 0$. So we just need to find an element β of $\mathbb{F}_7[x]/(x^2 - 3)$ such that $\beta^2 = 5$.
- We write $[f(x)]$ for an element of $\mathbb{F}_7[x]/(x^2 - 3)$. Then $[x]^2 = [x^2] = [x^2 - 3 + 3] = [3] = 3$. Since $5 = 3 \cdot 4 = 3 \cdot 2^2$, we see that $[2x]^2 = [x]^2 \cdot 2^2 = 5$. Hence we may take $\beta = [2x]$. This concludes the proof that

$$\mathbb{F}_7[x]/(x^2 - 5) \cong \mathbb{F}_7[x]/(x^2 - 3)$$

Exercise: Find an isomorphism $\mathbb{F}_2[x]/(x^3 + x^2 + 1) \cong \mathbb{F}_2[x]/(x^3 + x + 1)$.

Lecture 20.5 Fri 10/25
Tutorial
Classification of commutative rings of order p^2

We have seen that there are 4 commutative rings of order 4:

$$\mathbb{Z}/4\mathbb{Z}, \qquad \mathbb{F}_2 \times \mathbb{F}_2, \qquad \mathbb{F}_2[x]/(x^2 + 1), \qquad \mathbb{F}_2[x]/(x^2 + x + 1) = \mathbb{F}_4.$$

Recall also that $\mathbb{F}_5[x]/((x-2)(x-3)) \cong \mathbb{F}_5 \times \mathbb{F}_5$, so we can view $\mathbb{F}_2 \times \mathbb{F}_2$ as $\mathbb{F}_2[x]/(x^2 + x)$ using the factorization $x^2 + x = x(x+1)$ and the Chinese Remainder Theorem:

$$\mathbb{F}_2[x]/(x^2 + x) \cong \mathbb{F}_2[x]/(x) \times \mathbb{F}_2[x]/(x+1) \cong \mathbb{F}_2 \times \mathbb{F}_2.$$

The only missing degree 2 polynomial is x^2, but it is easy to check that

$$\mathbb{F}_2[x]/(x^2) \cong \mathbb{F}_2[x]/((x+1)^2) = \mathbb{F}_2[x]/(x^2 + 1),$$

via the homomorphism $\mathbb{F}_2[x] \to \mathbb{F}_2[x]/((x+1)^2)$ sending $x \mapsto x + 1 + ((x+1)^2)$.

Proposition 7.13 *Let p be a prime. There are exactly four commutative rings of order p^2 up to isomorphism:*

$$\mathbb{Z}/p^2\mathbb{Z}, \qquad \mathbb{F}_p \times \mathbb{F}_p, \qquad \mathbb{F}_p[x]/(x^2), \qquad \mathbb{F}_{p^2}.$$

Proof: We will prove soon that finite fields of the same order are isomorphic (spoiler!), so we only classify commutative rings of order p^2 that are not fields. Let R be a commutative ring of order p^2 that is not a field. We know from Lemma 6.7 that the characteristic of R divides p^2. Hence it is either p or p^2. If the characteristic of R is p^2, then by Proposition 6.15, we have $R \cong \mathbb{Z}/p^2\mathbb{Z}$.

Suppose now R has characteristic p. Then the prime subring (image of the canonical map $\mathbb{Z} \to R$) is isomorphic to $\mathbb{F}_p$. We will use this to view $\mathbb{F}_p$ as a subring of R. Since $|R| > p$, we may take some $\beta \in R \backslash \mathbb{F}_p$. We claim that

$$R = \{a + b\beta \colon a, b \in \mathbb{F}_p\}.$$

The RHS is clearly a subset of R. There are p^2 possible choices for (a, b). We claim that they give distinct elements. Suppose $a_1, b_1, a_2, b_2 \in \mathbb{F}_p$ such that

$$a_1 + b_1\beta = a_2 + b_2\beta.$$

Then $a_1 - a_2 = (b_2 - b_1)\beta$. If $b_1 \neq b_2$, then $b_2 - b_1 \neq 0$ and we can divide to find

$$\beta = (a_1 - a_2)(b_2 - b_1)^{-1} \in \mathbb{F}_p.$$

Contradiction. Hence $b_1 = b_2$ and then $a_1 - a_2 = 0$ implying that $a_1 = a_2$. Thus, $\{a + b\beta \colon a, b \in \mathbb{F}_p\}$ is a subset of R containing the same number of elements as R and so equals R.

Now that we know that R is generated by $\mathbb{F}_p$ and β, we look at the evaluation homomorphism $\mathrm{ev}_\beta : \mathbb{F}_p[x] \to R$. Note that $\mathrm{ev}_\beta(a+bx) = a + b\beta$ for any $a, b \in \mathbb{F}_p$. Hence ev_β is surjective. By the first isomorphism theorem, we have $R \cong \mathbb{F}_p[x]/\ker(\mathrm{ev}_\beta)$. Since $\mathbb{F}_p[x]$ is a PID, we see that $\ker(\mathrm{ev}_\beta) = (g(x))$ for some polynomial $g(x) \in F[x]$. By dividing by the leading coefficient of $g(x)$, which is a unit in $F[x]$, we may assume $g(x) = x^d + \cdots$ is monic of degree d. By Lemma 7.10, we have

$$p^2 = |R| = |\mathbb{F}_p[x]/(g(x))| = p^d \qquad \Longrightarrow \qquad d = 2.$$

Since we assumed that R is not a field, we know that $g(x)$ is not irreducible. Since $g(x)$ has degree 2, we have

$$g(x) = (x-c)(x-d) \qquad \text{for some } c, d \in \mathbb{F}_p.$$

If $c \neq d$, then we use the Chinese Remainder Theorem to obtain

$$R \cong \mathbb{F}_p[x]/((x-c)(x-d)) \cong \mathbb{F}_p[x]/(x-c) \times \mathbb{F}_p[x]/(x-d) \cong \mathbb{F}_p \times \mathbb{F}_p.$$

If $c = d$, then we have

$$R \cong \mathbb{F}_p[x]/((x-c)^2) \cong \mathbb{F}_p[x]/(x^2).$$

This completes the proof. □

Exercise

7.1 Prove that the ideal $(2, x)$ in $\mathbb{Z}[x]$ is not principal.

7.2 What are the irreducible polynomials in $\mathbb{C}[x]$? What are the irreducible polynomials in $\mathbb{R}[x]$?

7.3 Let R be a commutative ring and let I be a proper ideal of R. We say I is a **maximal ideal** of R if there does not exist a proper ideal J such that I is a proper subset of J. Prove that I is maximal if and only if R/I is a field.

7.4 Give an example of a commutative ring R, a maximal ideal I, and a subring S such that $S \cap I$ is not maximal in S.

7.5 Let R be a commutative ring and let S be a subring. Let I be a prime ideal of R. Prove that $S \cap I$ is a prime ideal of S.

8 Finite fields

The main theorem in the theory of finite fields is:

Theorem 8.1 *(Classification of finite fields)*

(a) Every finite field has order p^d for some prime p and positive integer d.

(b) Any two finite fields of the same order are isomorphic.

(c) For every prime p and every positive integer d, there exists a polynomial $g(x) \in \mathbb{F}_p[x]$ irreducible of degree d. We write $\mathbb{F}_{p^d} \cong \mathbb{F}_p[x]/(g(x))$.

(d) There exists a homomorphism $\mathbb{F}_{p^d} \to \mathbb{F}_{p^n}$ if and only if $d \mid n$.

The key steps to prove the above are:

Theorem 8.2 *Let F be a finite field of size p^n for some prime p and some positive integer n. Then there exists $a \in F^\times$ such that $o(a) = p^n - 1$.*

Theorem 8.3 *Let p be a prime and let $n \in \mathbb{N}$. Then $x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree dividing n.*

Lecture 21 Mon 10/28
Finite fields I

We will assume Theorem 8.2 and Theorem 8.3 first and see how much we can understand fields. We have actually used most of the techniques last week! Let F be a finite field of order q. We know from Lemma 6.4 and Lemma 6.7 that the characteristic of F is some prime p dividing q. Secretly, $q = p^n$ for some n. Moreover, $|F^\times| = q - 1$, so we know from Theorem 6.13(b) that

$$\forall a \in F^\times, \quad a^{q-1} = 1 \qquad \text{and} \qquad o(a) \mid q - 1.$$

In particular, all q elements of F is a root of $x^q - x$, which is a polynomial of degree q. So we have the factorization

$$x^q - x = \prod_{a \in F} (x - a).$$

We say the polynomial $x^q - x$ splits completely in F. This lends some credit as to why we should care about polynomials of the form $x^{p^n} - x$.

Theorem 8.2 gives the existence of some $a \in F^\times$ such that $o(a) = q - 1$. Such an element is said to be primitive. This means that the $q - 1$ elements $a, a^2, \ldots, a^{q-1}$ are all distinct (see for example Lemma 4.5). Hence, they are all the elements of $F^\times$. So

$$F = \{0, a, a^2, \ldots, a^{q-1}\}.$$

Corollary 8.4 *Let F be a finite field and let E be a subfield (a subring that is a field) of F. Then $F \cong E[x]/(f(x))$ for some irreducible polynomial $f(x) \in E[x]$.*

Proof: (Assuming Theorem 8.2:) Let a be a primitive element of F. Then the evaluation homomorphism $\mathrm{ev}_a : E[x] \to F$ sending $g(x)$ to $g(a)$ is surjective, because $\mathrm{ev}_a(x^m) = a^m$ hits every nonzero element of F. Hence by the first isomorphism theorem, we have $F \cong E[x]/\ker(\mathrm{ev}_a)$. Since $E[x]$ is a PID, we have $\ker(\mathrm{ev}_a) = (g(x))$ for some polynomial $g(x) \in E[x]$, which is irreducible by Proposition 7.11. □

Proof of Theorem 8.1(a) and (d, $\Rightarrow$): Let p be the characteristic of a finite field F. Then the prime subring of F is $\mathbb{F}_p$. Applying Corollary 8.4 with $E = \mathbb{F}_p$ gives that

$$F \cong \mathbb{F}_p[x]/(g(x))$$

for some irreducible polynomial $g(x)$. Let $d = \deg(g)$. Then by Lemma 7.10, we have $|F| = p^d$.

Suppose now there is a homomorphism $\varphi : \mathbb{F}_{p^d} \to \mathbb{F}_{p^n}$. Since a homomorphism from a field is automatically injective, we apply Corollary 8.4 to $F = \mathbb{F}_{p^n}$ and $E = \mathrm{im}(\varphi) \cong \mathbb{F}_{p^d}$. We get $F \cong E[x]/(g(x))$ for some polynomial $g(x) \in E[x]$ of degree m. Then by Lemma 7.10, we have $|F| = p^n = |E|^m = p^{dm}$. So $n = dm$ is divisible by d. □

Note in the above proof, we also showed that every finite field of characteristic p is of the form $\mathbb{F}_p[x]/(g(x))$ for some irreducible polynomial $g(x) \in \mathbb{F}_p[x]$ of degree d. By dividing by the leading coefficient of $g(x)$, which is a unit in $\mathbb{F}_p[x]$, we may assume $g(x)$ is monic. Suppose R is a ring of characteristic p, so that the prime subfield of R is $\mathbb{F}_p$. We saw previously that to define a ring homomorphism $\mathbb{F}_p[x]/(g(x)) \to R$, it is enough to specify the image $\beta \in R$ of x, which must satisfy $g(\beta) = 0$ in order for the map $\mathrm{ev}_\beta : \mathbb{F}_p[x] \to R$ to "factor through" $\mathbb{F}_p[x]/(g(x))$.

Suppose now $R = F$ is a field of order p^n where $d \mid n$. We saw earlier that $x^{p^n} - x$ splits completely in F. Theorem 8.3 tells us that $g(x)$ is a factor of $x^{p^n} - x$. Write $x^{p^n} - x = g(x)h(x)$ for some polynomial $h(x) \in \mathbb{F}_p[x]$ of degree $p^n - d$. Then $h(x)$ has at most $p^n - d$ roots in F but every element of F is a root of $g(x)h(x)$. Hence $g(x)$ has at least d roots in F. Since $g(x)$ has degree d, we see that $g(x)$ also splits completely in F. We have thus proved (assuming Theorem 8.3:)

Corollary 8.5 *If $g(x) \in \mathbb{F}_p[x]$ is irreducible of degree d and $d \mid n$, then $g(x)$ splits completely in any field F of order p^n.*

Proof of Theorem 8.1(b) and (d, $\Leftarrow$): Suppose $g(x) \in \mathbb{F}_p[x]$ is irreducible of degree d and $d \mid n$. Corollary 8.5 says that $g(x)$ splits completely in $\mathbb{F}_{p^n}$. In particular, it has a root β in $\mathbb{F}_{p^n}$, using which we obtain a homomorphism $\mathbb{F}_p[x]/(g(x)) \to \mathbb{F}_{p^n}$. This gives the desired homomorphism of (d, $\Leftarrow$). Applying Corollary 8.5 with $n = d$ gives a homomorphism $\mathbb{F}_p[x]/(g(x)) \to F$ for any field F of order p^d. Such a homomorphism is automatically injective and also surjective since $\mathbb{F}_p[x]/(g(x))$ also has order p^d. Hence, any field of order p^d is isomorphic to $\mathbb{F}_p[x]/(g(x))$, and so also to each other. □

Lecture 22 Wed 10/30
Finite fields II

Proof of Theorem 8.1(c): Let $S_p(n)$ denote the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree n. We prove $S_p(n) > 0$. In fact, we will prove a very nice formula for $S_p(n)$. By Theorem 8.3, $x^{p^n} - x$ is the product of all the monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree $d \mid n$. We take degrees to get

$$p^n = \sum_{d|n} dS_p(d).$$

We recall the Mobius inversion formula from HW 3 P4. Let $\mu : \mathbb{N} \to \{-1, 0, 1\}$ denote the Mobius function defined by

$$\mu(n) = \begin{cases} (-1)^{d(n)} & \text{if } n \text{ is squarefree} \\ 0 & \text{otherwise} \end{cases}$$

where $d(n)$ denotes the number of distinct prime divisors of n. You proved that if $f, g : \mathbb{N} \to \mathbb{C}$ satisfy $f(n) = \sum_{d|n} g(d)$, then $g(n) = \sum_{d|n} \mu(d) f(n/d)$. We now use this with $f(n) = p^n$ and $g(n) = nS_p(n)$ to get

$$nS_p(n) = \sum_{d|n} \mu(d) p^{n/d}.$$

For example

$$S_2(6) = \frac{1}{6}\left(2^6 - 2^3 - 2^2 + 2^1\right) = 9 > 0.$$

This example illustrates the main idea: the term $d = 1$ gives p^n, which dominates all other terms. Note that if $d > 1$, then $n/d \le n/2$. Hence

$$|p^n - nS_p(n)| = \left| \sum_{d|n, d>1} \mu(d) p^{n/d} \right| \le p^{\lfloor n/2 \rfloor} + p^{\lfloor n/2 \rfloor - 1} + \cdots + 1 < p^{\lfloor n/2 \rfloor + 1} \le p^n.$$

This implies that $nS_p(n) > 0$. □

Here are the proofs of Theorem 8.2 and Theorem 8.3.

Proof of Theorem 8.2: Let F be a field of q elements. We want an element a with $o(a) = m = q - 1$. Every element of $F^\times$ has order dividing m. For any positive divisor d of m, let N_d denote the number of elements in F with order exactly d. Then we have

$$m = \sum_{d|m} N_d.$$

Recall that we also have

$$m = \sum_{d|m} \phi(d)$$

from the factorization of $x^m - 1$ in cyclotomic polynomials (Corollary 5.2). We first prove that $N_d = 0$ or $N_d = \phi(d)$. Suppose $N_d > 0$ and let α be an element of order d. Can we express all elements of order d in terms of α? Any element of order d is a root of the degree d polynomial $x^d - 1 \in F[x]$ and $\alpha, \alpha^2, \ldots, \alpha^d$ already give d of them, which are all distinct since $d = o(\alpha)$. In other words, any element of order d must be one of these d powers of α. Recall from HW 4 P1(a) that for any integer k,

$$o(\alpha^k) = \frac{o(\alpha)}{\gcd(k, o(\alpha))}.$$

Hence we see that $o(\alpha^k) = d$ if and only if $\gcd(k, o(\alpha)) = 1$. Therefore, $N_d = \phi(d)$.

Note that in both cases, we have $N_d \leq \phi(d)$ so $\phi(d) - N_d \geq 0$. Now

$$0 = \sum_{d|m} (\phi(d) - N_d).$$

Hence, we must have $\phi(d) = N_d$ for all $d \mid m$. In particular, $N_m = \phi(m) > 0$. □

Proof of Theorem 8.3: In order to prove Theorem 8.3, it suffices to prove:

(a) Let $f(x) \in \mathbb{F}_p[x]$ be a monic irreducible polynomial of degree d. Then $f(x) \mid x^{p^n} - x$ if and only if $d \mid n$.

(b) The polynomial $x^{p^n} - x$ has no repeated factors in $\mathbb{F}_p[x]$.

(c) Prime factorization in $\mathbb{F}_p[x]$: every monic polynomial in $\mathbb{F}_p[x]$ can be written as a product of monic irreducible polynomials in $\mathbb{F}_p[x]$.

Recall that to check whether a polynomial $h(x)$ in $\mathbb{F}_p[x]$ has repeated factors, we can use its derivative. Suppose $h(x) = g(x)^2 j(x)$. Then $h'(x) = 2g(x)g'(x)j(x) + g(x)^2 j'(x)$ is divisible by $g(x)$. So if $h(x)$ and $h'(x)$ share no common factors, then $h(x)$ has no repeated factors. Here $(x^{p^n} - x)' = p^n x^{p^n - 1} - 1 = -1$ in $\mathbb{F}_p[x]$, which has no factors, so statement (b) follows. Statement (c) is a straightforward induction on the degree of the polynomial to be factored.

For statement (a), we recall a result observed in HW 1:

$$\gcd(p^k - 1, p^\ell - 1) = p^{\gcd(k,\ell)} - 1.$$

In particular,

$$p^k - 1 \mid p^\ell - 1 \quad \Longleftrightarrow \quad k \mid \ell.$$

Let $F = \mathbb{F}_p[x]/(f(x))$ and let $\beta = [x] \in F$. Then we first note that

$$f(x) \mid x^{p^n} - x \iff [x^{p^n}] = [x] \iff \beta^{p^n} = \beta.$$

We will assume without loss of generality that $f(x) \neq x$. So we have $\beta \in F^\times$.

Suppose first that $d \mid n$ so that $p^d - 1 \mid p^n - 1$. Then since F is a field of order p^d, we have

$$o(\beta) \mid p^d - 1 \mid p^n - 1.$$

Hence $\beta^{p^n - 1} = 1$ and so $\beta^{p^n} = \beta$.

Suppose now conversely that $\beta^{p^n} = \beta$, and so $\beta^{p^n - 1} = 1$. If we knew $o(\beta) = p^d - 1$, then we would have $p^d - 1 \mid p^n - 1$ immediately. We let $\alpha \in F^\times$ be an element with $o(\alpha) = p^d - 1$. It then suffices to prove that $\alpha^{p^n} = \alpha$. As an element of F, we have

$$\alpha = [a_m x^m + \cdots + a_0] = a_m \beta^m + \cdots + a_0$$

for some $a_0, \ldots, a_m \in \mathbb{F}_p$. By Lemma 7.8, we have

$$\alpha^{p^n} = a_m^{p^n} \beta^{m p^n} + a_{m-1}^{p^n} \beta^{(m-1)p^n} + \cdots + a_0^{p^n}.$$

Since each $a_i \in \mathbb{F}_p$, we have $a_i^{p^n} = a_i$. Moreover, each $\beta^{ip^n} = (\beta^{p^n})^i = \beta^i$. Hence

$$\alpha^{p^n} = a_m\beta^m + a_{m-1}\beta^{m-1} + \cdots + a_0 = \alpha.$$

This completes the proof of Theorem 8.3. □

It is worth noting that $F[x]$ and $\mathbb{Z}$ are very similar. We have the division algorithm so that both are Euclidean domains and PIDs. We have a notion of irreducible/prime elements. We can pretend that monic polynomials are like positive integers. We have unique factorizations into irreducible/primes. However, $F[x]$ has an extra operation, namely differentiation, that allows one to prove more. For example, the versions of the abc conjecture (Mason's Theorem) and Fermat's last theorem over $F[x]$ are much easier. One can also test for the existence of repeated roots by applying the Euclidean algorithm to find the gcd of $h(x)$ and $h'(x)$. However, testing for squarefree integers is as difficult as factorization.

Lecture 23 Fri 11/01
Using finite fields

For $n = 1$, we have the factorization

$$x^p - x = x(x-1)\cdots(x-(p-1)).$$

Canceling the x gives

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)),$$

which we already knew from Fermat's little theorem. Setting $x = 0$ gives

$$-1 = (-1)^{p-1}(p-1)! \qquad \text{in } \mathbb{F}_p.$$

Translating it to integer congruences gives Wilson's Theorem

$$(p-1)! \equiv -1 \pmod{p}.$$

The fact that $x^p - x$ has all of its roots in $\mathbb{F}_p$ is also very useful for determining when an element $\alpha \in \mathbb{F}_{p^n}$ actually belongs to $\mathbb{F}_p$.

Corollary 8.6 *Let F be a field of order p^n for some prime p and positive integer n. Then $\alpha \in F$ belongs to the prime subfield $\mathbb{F}_p$ if and only if $\alpha^p = \alpha$.*

When $n = 2$, we note that every quadratic polynomial over $\mathbb{F}_p$ splits completely in $\mathbb{F}_{p^2}$. Indeed, if a quadratic polynomial $f(x) \in \mathbb{F}_p[x]$ is reducible, then it already splits completely in $\mathbb{F}_p$; if $f(x)$ is irreducible, then it splits completely in $\mathbb{F}_{p^2}$ by Corollary 8.5.

Corollary 8.7 *Let p be a prime and $n \in \mathbb{N}$. Then any degree n polynomial in $\mathbb{F}_p[x]$ splits completely in $\mathbb{F}_{p^{L_n}}$ where $L_n = \operatorname{lcm}(1, 2, \ldots, n)$. The statement is false if $\mathbb{F}_{p^{L_n}}$ is replaced by any smaller field.*

Proof: Let $f(x) \in \mathbb{F}_p[x]$ be an arbitrary polynomial of degree n. Let $g(x) \in \mathbb{F}_p[x]$ be any irreducible factor of $f(x)$. Then $\deg(g) \le n$ and so $\deg(g) \mid L_n$. By Corollary 8.5, we have that $g(x)$ splits completely in $\mathbb{F}_{p^{L_n}}$. Since $f(x)$ is a product of its irreducible factors (with multiplicities), we see that $f(x)$ also splits completely in $\mathbb{F}_{p^{L_n}}$.

We now prove the second statement. Suppose any degree n polynomial splits completely in $\mathbb{F}_{p^N}$ for some $N \in \mathbb{N}$. It suffices to prove $L_n \mid N$. Let $q \le n$ be any prime and let $k = \lfloor \log_q n \rfloor = \nu_q(L_n)$. Then $q^k \le n$. Let $h(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree q^k and let $f(x) = h(x)x^{n-q^k}$. Since $f(x)$ splits completely in $\mathbb{F}_{p^N}$, we see that $h(x)$ splits completely in $\mathbb{F}_{p^N}$. In particular, $h(x)$ has a root in $\mathbb{F}_{p^N}$ and so we have an homomorphism $\mathbb{F}_p[x]/(h(x)) \to \mathbb{F}_{p^N}$ which is only possible if $\deg(h) \mid N$ by Theorem 8.1(d). So $q^k \mid N$. Since this is true for all primes $q \le n$, we have $L_n \mid N$. □

We now use the field $\mathbb{F}_{49}$ to prove the infinitude of primes $\equiv -1 \pmod 7$.

Theorem 8.8 *Let p be a prime divisor of n^3+n^2-2n-1 for some integer n. Then $p=7$ or $p\equiv\pm1 \pmod 7$.*

Proof: We have some $n\in\mathbb{F}_p$ such that $n^3+n^2-2n-1=0$. Let $\alpha\in\mathbb{F}_{p^2}$ be a root of x^2-nx+1 since any quadratic polynomial splits completely in $\mathbb{F}_{p^2}$. Then $\alpha\neq 0$ and $n=\alpha+\alpha^{-1}$. Now

$$\begin{aligned} 0 &= (\alpha+\alpha^{-1})^3+(\alpha+\alpha^{-1})^2-2(\alpha+\alpha^{-1})-1 \\ &= \alpha^3+3\alpha+3\alpha^{-1}+\alpha^{-3}+\alpha^2+2+\alpha^{-2}-2(\alpha+\alpha^{-1})-1 \\ &= \alpha^3+\alpha^2+\alpha+1+\alpha^{-1}+\alpha^{-2}+\alpha^{-3}. \end{aligned}$$

Multiplying by α^3 gives

$$\Phi_7(\alpha)=\alpha^6+\alpha^5+\alpha^4\alpha^3+\alpha^2+\alpha+1=0.$$

If $p\neq 7$, then by HW 7 P3, we have $o(\alpha)=7$. Since $o(\alpha)\mid|\mathbb{F}_{p^2}^\times|$, we get $7\mid p^2-1$. So $7\mid(p-1)(p+1)$ and hence $7\mid p-1$ or $7\mid p+1$ since 7 is a prime. So $p\equiv\pm1 \pmod 7$. □

We can now prove the infinitude of primes that are -1 mod 7. Let

$$g(x)=(7x)^3+(7x)^2-2(7x)-1.$$

Then for any integer n, we have that $g(n)\equiv -1 \pmod 7$. Hence $g(n)$ is not divisible by 7 and can't be a product of primes that are all 1 mod 7. Hence by the above theorem, if $g(n)>0$, then it has a prime divisor that is -1 mod 7. Then by taking the sequence

$$a_1=g(69),\qquad a_n=g(69a_1\cdots a_{n-1}),\ \text{for } n\geq 2,$$

we have a sequence of pairwise coprime integers each of which has a prime divisor that is -1 mod 7.

The key to this cute result is that for the polynomial $f_7(x)=x^3+x^2-2x-1$, we have

$$f_7(x+x^{-1})=x^{-3}\,\Phi_7(x).$$

It follows from the fact that $\Phi_m(x)$ is palindromic (HW 4 P1) that for any $m\geq 3$, there exists a (unique) monic polynomial $f_m(x)\in\mathbb{Z}[x]$ of degree $\phi(m)/2$ such that

$$f_m(x+x^{-1})=x^{-\phi(m)/2}\,\Phi_m(x).$$

For example, one finds

$$f_{11}(x)=x^5+x^4-4x^3-3x^2+3x+1.$$

However, we can't use this polynomial as above to prove the infinitude of primes that are -1 mod 11 because the constant coefficient of $f_{11}(x)$ is 1 instead of -1 so we have $f_{11}(11n)\equiv 1 \pmod{11}$. So it is possible that all the prime divisors of $f_{11}(11n)$ are 1 mod 11. The trick here is to notice that the degree of f_{11} is odd. So we can use

$$-f_{11}(-x)=x^5-x^4-4x^3+3x^2+3x-1,$$

for a polynomial with positive leading coefficient (so that it is at least 2 when x is large enough) with $-f_{11}(-11n)\equiv -1 \pmod{11}$. Hence for large enough n, the positive integer $-f_{11}(-11n)$ will have a prime divisor $\equiv -1 \pmod{11}$.

This trick works for all $m=q$ prime. By computing $\Phi_q(i)$ (https://arxiv.org/pdf/1611.06783.pdf, Lemma 23), we find that

$$f_q(0)=\begin{cases} 1 & \text{if } q\equiv 3 \pmod 8,\\ -1 & \text{if } q\equiv 1,5,7 \pmod 8.\end{cases}$$

When $q\equiv 1,3,7 \pmod 8$, the constant coefficient is -1 so we can use the same argument as f_7. When $q\equiv 3 \pmod 8$, the degree $\phi(q)/2=(q-1)/2$ of $f_q(x)$ is odd and so we may use the same argument as f_{11} by taking $-f_q(-x)$.

Repeating the argument as in the proof of Theorem 8.8 would lead to some $\alpha \in \mathbb{F}_{p^2}$ with

$$\Phi_m(\alpha) = 0.$$

When $p \nmid m$, we have by HW 7 P3 that $o(\alpha) = m$ and so $m \mid p^2 - 1$. When $m = q$ is a prime, we again obtain $q \mid p - 1$ or $q \mid p + 1$ and so $p \equiv \pm 1 \pmod{q}$.

When m is composite, this last step may not hold. For example, when $m = 15$, we would have $p \equiv \pm 1, \pm 4 \pmod{15}$. It is still possible to split these congruences apart, but we won't get into it in this class. In HW 8 P3, you will work this out in full detail for $m = 9$.

Lecture 23.5 Fri 11/01
Tutorial
Discriminant of $\Phi_q(x)$ in $\mathbb{F}_p[x]$

Let p, q be two distinct odd primes. In HW 7 and HW 8, you explored the factorization of $\Phi_q(x)$ in $\mathbb{F}_p[x]$. As a concrete example, consider

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^2 + 3x + 1)(x^2 + 5x + 1)(x^2 + 6x + 1) \in \mathbb{F}_{13}[x].$$

- Let $d = o_q(p)$ so that $q \mid p^d - 1$. Then $\mathbb{F}_{p^d}$ is the smallest field containing an element ζ with $o(\zeta) = q$. In this example, we have $13^2 = 169 = 1 + 7 \cdot 24 \equiv 1 \pmod{7}$. So $d = 2$ and we can find ζ with $o(\zeta) = 7$ in $\mathbb{F}_{169}$.
- The roots of $\Phi_q(x)$ in a field F of characteristic not dividing q are exactly the ones with order q, and $\Phi_q(x)$ splits completely in $\mathbb{F}_{p^d}$. In this example, we have all 6 roots of $\Phi_7(x)$ in $\mathbb{F}_{169}$, namely $\zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6$.
- Let $r = \phi(q)/d$. Then $\Phi_q(x) = f_1(x) \cdots f_r(x)$ factors into a product of r irreducible polynomials in $\mathbb{F}_p[x]$ of degree d. In this example, $r = \phi(7)/2 = 3$ and $\Phi_7(x)$ factors into a product of 3 irreducible quadratics.
- The roots of an irreducible polynomial of degree d in $\mathbb{F}_p[x]$ are of the form $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$. In this example, note that $\zeta^7 = 1$. So $\zeta^{13} = \zeta^6$ and $\zeta^{169} = \zeta$. We may group the roots as:

$$\begin{aligned} f_1(x) &= (x - \zeta)(x - \zeta^6) \\ f_2(x) &= (x - \zeta^2)(x - \zeta^5) \\ f_3(x) &= (x - \zeta^3)(x - \zeta^4). \end{aligned}$$

- For $\beta = \prod_{0 \le i < j \le d-1} (\alpha^{p^i} - \alpha^{p^j})$, we have $\beta^p = (-1)^{d-1}\beta$. For $\ell = 1, \ldots, r$, let α_ℓ be a root of $f_\ell(x)$ and define β_ℓ for $f_\ell(x)$. Then $\beta_\ell^p = (-1)^{d-1}\beta_\ell$ and $(\beta_1 \cdots \beta_r)^p = (-1)^{(d-1)r}\beta_1 \cdots \beta_r$. In this case, we have

$$\beta_1 = \zeta - \zeta^6, \qquad \beta_2 = \zeta^2 - \zeta^5, \qquad \beta_3 = \zeta^3 - \zeta^4.$$

  Since $d = 2$ in this case, they all satisfy $\beta_i^{13} = -\beta_i$ and we have $(\beta_1\beta_2\beta_3)^{13} = -\beta_1\beta_2\beta_3$, in $\mathbb{F}_{169}$.

Note that

$$\beta_1 \cdots \beta_r = \prod_{\ell=1}^{r} \prod_{0 \le i < j \le d-1} (\alpha_\ell^{p^i} - \alpha_\ell^{p^j}).$$

We can similarly define β for the entire $\Phi_q(x)$ as

$$\beta = \prod_{1 \le i < j \le q-1} (\zeta^i - \zeta^j)$$

as $\zeta, \ldots, \zeta^{q-1}$ are all the roots of $\Phi_q(x)$. In this example, we have

$$\begin{aligned}\beta &= \pm(\zeta-\zeta^6)(\zeta^2-\zeta^5)(\zeta^3-\zeta^4)(\zeta-\zeta^2)(\zeta-\zeta^5)(\zeta^6-\zeta^2)(\zeta^6-\zeta^5)\\ &\quad\cdot(\zeta-\zeta^3)(\zeta-\zeta^4)(\zeta^6-\zeta^3)(\zeta^6-\zeta^4)(\zeta^2-\zeta^3)(\zeta^2-\zeta^4)(\zeta^5-\zeta^3)(\zeta^5-\zeta^4).\end{aligned}$$

Note that the first piece is exactly $\beta_1 \cdots \beta_r$. Each colored piece is

$$\beta_{\ell_1\ell_2} := \prod_{\delta \text{ root of } f_{\ell_1}} \prod_{\eta \text{ root of } f_{\ell_2}} (\delta - \eta).$$

The key observation now is that the p-th power of a root of f_ℓ is another root of f_ℓ. So

$$\beta_{\ell_1\ell_2}^p = \prod_{\delta \text{ root of } f_{\ell_1}} \prod_{\eta \text{ root of } f_{\ell_2}} (\delta^p - \eta^p) = \prod_{\delta' \text{ root of } f_{\ell_1}} \prod_{\eta' \text{ root of } f_{\ell_2}} (\delta' - \eta') = \beta_{\ell_1\ell_2}.$$

In this example,

$$\begin{aligned}((\zeta-\zeta^2)(\zeta-\zeta^5)(\zeta^6-\zeta^2)(\zeta^6-\zeta^5))^{13} &= (\zeta^{13}-\zeta^{26})(\zeta^{13}-\zeta^{65})(\zeta^{78}-\zeta^{26})(\zeta^{78}-\zeta^{65})\\ &= (\zeta^6-\zeta^5)(\zeta^6-\zeta^2)(\zeta-\zeta^5)(\zeta-\zeta^2).\end{aligned}$$

As a consequence, we have

$$\frac{\beta^p}{\beta} = \frac{(\beta_1 \cdots \beta_r)^p}{\beta_1 \cdots \beta_r} = (-1)^{(d-1)r}.$$

So $\beta \in \mathbb{F}_p$ if and only if $(d-1)r$ is even, which by HW 8 P1 is equivalent to p being a square in $\mathbb{F}_q$. In this example, $(d-1)r = 3$ is odd and $13 = 6$ is not a square mod 7, as the squares mod 7 are $0, 1, 2, 4$.

On the other hand, we can actually compute β^2 directly and find that

$$\beta^2 = (-1)^{(q-1)/2} q^{q-2}.$$

Let $q^* = (-1)^{(q-1)/2} q$. Then

$$\beta^2 = q^* q^{q-3} = q^* (q^{(q-3)/2})^2.$$

Hence $\beta \in \mathbb{F}_p$ is and only if q^* is a square in $\mathbb{F}_p$. This is quadratic reciprocity!

$$p \text{ is a square in } \mathbb{F}_q \quad \Longleftrightarrow \quad q^* \text{ is a square in } \mathbb{F}_p.$$

In this case, 13 is not a square mod 7 and so $7^* = -7 = 6$ is not a square mod 13. The squares mod 13 are $0, 1, 4, 9, 3, 12, 10$.

We now give a proof for the formula

$$\beta^2 = (-1)^{(q-1)/2} q^{q-2}.$$

Note that we have the factorization

$$x^{q-1} + \cdots + x + 1 = \Phi_q(x) = \prod_{i=1}^{q-1} (x - \zeta^i).$$

Setting $x = 1$ gives

$$q = \prod_{i=1}^{q-1} (1 - \zeta^i).$$

Note also that

$$\beta^2 = \prod_{1 \le i < j \le q-1} (\zeta^i - \zeta^j)^2 = (-1)^{(q-1)(q-2)/2} \prod_{1 \le i \ne j \le q-1} (\zeta^i - \zeta^j).$$

This follows because given any pair (i,j) with $i \neq j$, we pick up a negative sign from

$$(\zeta^i - \zeta^j)(\zeta^j - \zeta^i) = -(\zeta^i - \zeta^j)^2$$

and there are $\binom{q-1}{2}$ possible pairs. Now for a fixed $i = 1, \ldots, q-1$,

$$\prod_{\substack{1 \leq j \leq q-1 \\ j \neq i}} (\zeta^i - \zeta^j) = (\zeta^i)^{q-2} \prod_{\substack{1 \leq k \leq q-1 \\ k+i \neq q}} (1 - \zeta^k) = \frac{(\zeta^i)^{q-2}}{1 - \zeta^{q-i}} \prod_{k=1}^{q-1} (1 - \zeta^k) = \frac{(\zeta^i)^{q-2}}{1 - \zeta^{q-i}} q.$$

Multiply over all $i = 1, \ldots, q-1$:

$$\prod_{i=1}^{q-1} (\zeta^i)^{q-2} = \zeta^{q(q-1)(q-2)/2} = 1 \qquad \text{and} \qquad \prod_{i=1}^{q-1} (1 - \zeta^{q-i}) = \prod_{k=1}^{q-1} (1 - \zeta^k) = q.$$

Hence, we have

$$\beta^2 = (-1)^{(q-1)(q-2)/2} \frac{q^{q-1}}{q} = (-1)^{(q-1)/2} q^{q-2},$$

since $q-2$ is odd so $(-1)^{q-2} = -1$.

Exercise

8.1 Let F be a finite field and let $k \in \mathbb{N}$ such that $\gcd(k, |F| - 1) = 1$. Prove that every element in F is the k-th power of some element in F.

8.2 Let F be a finite field and let $k \in \mathbb{N}$. Let S be the subset of F consists of sums of k-th powers. (Note that an empty sum is 0.) Prove that S is a subfield of F.

8.3 Prove that for any positive integer $n \neq 2$, every element in $\mathbb{F}_{2^n}$ is a sum of cubes. Note that the cubes in $\mathbb{F}_4$ are precisely 0 and 1 and so the subfield of sums of cubes in $\mathbb{F}_4$ is $\mathbb{F}_2$.

8.4 Let F be a finite field with $3 \mid |F| - 1$. Suppose there exist $u, v \in F^\times$ such that $u^3 + v^3 = 1$. Let w be an arbitrary element of F. Let

$$A = \{a^3 : a \in F\}, \quad B = \{w + b^3 : b \in F\}, \quad C = \{u^3 w + c^3 : c \in F\}.$$

(a) Prove that A, B, C are not pairwise disjoint.

(b) Prove that w is a sum of two cubes. In other words, every element of F is a sum of two cubes.

8.5 Let F be a finite field with $3 \mid |F| - 1$ and $|F| > 7$. Suppose there does not exist $u, v \in F^\times$ such that $u^3 + v^3 = 1$. Let $\alpha \in F^\times$ be a primitive element. Let

$$A = \{\alpha^{3k} : k \in \mathbb{Z}\}, \quad D = \{\alpha^{3k+1} : k \in \mathbb{Z}\}, \quad E = \{\alpha^{3k+2} : k \in \mathbb{Z}\}.$$

(a) Prove that at least one of $\alpha^3 - 1$, $\alpha^3 + 1$, $\alpha^6 - 1$ belongs to D, and at least one of them belongs to E.

(b) Prove that every element of F is a sum of two cubes.

8.6 Exercises 10.1, 10.4, 10.5 imply that for any finite field except $\mathbb{F}_4$ and $\mathbb{F}_7$, every element is a sum of two cubes. Prove that for $F = \mathbb{F}_7$, every element is a sum of three cubes, and not every element is a sum of two cubes.

8.7 Prove that for any $\alpha \in \mathbb{F}_7$, the polynomial $x^4 - \alpha \in \mathbb{F}_7[x]$ is reducible.

8.8 Let $q = p^n$ be a power of a prime. Let $\alpha \in \mathbb{F}_q$ be a primitive element. Suppose $q \equiv 1 \pmod{d}$ for some positive integer d. Prove that $x^d - \alpha \in \mathbb{F}_q[x]$ is irreducible.

Lecture 24 Mon 11/04
Quadratic reciprocity

9 Quadratic reciprocity

Now that we have proved quadratic reciprocity, let's talk about what it is.

An element $a \in \mathbb{F}_p$ is a square in $\mathbb{F}_p$ if $a = b^2$ for some $b \in \mathbb{F}_p$. Recalling that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, we can state this in terms of congruences: $x^2 \equiv a \pmod{p}$ has a solution. More generally, we say an integer a is a quadratic residue mod m (or in $\mathbb{Z}/m\mathbb{Z}$) if the equation $x^2 \equiv a \pmod{m}$ has an integer solution. Otherwise, we say it is a quadratic non-residue. Our eventual goal will be to give an algorithm for determining whether a is a quadratic residue mod m. For example, is 69 a square mod 420? We factor $420 = 4 \cdot 3 \cdot 5 \cdot 7$ into coprime factors so we can use the Chinese Remainder Theorem to say that

$$b^2 \equiv 69 \pmod{420} \iff \begin{cases} b^2 \equiv 69 \pmod{4} \\ b^2 \equiv 69 \pmod{3} \\ b^2 \equiv 69 \pmod{5} \\ b^2 \equiv 69 \pmod{7} \end{cases}$$

In other words, 69 is a square mod 420 if and only if 69 is square mod all of $4, 3, 5, 7$. The latter can be checked directly because the numbers are small: $69 \equiv 1 \pmod{4}$ is a square; $69 \equiv 0 \pmod{3}$ is a square; $69 \equiv 4 \pmod{5}$ is a square; $69 \equiv 6 \pmod{7}$ is not a square. Hence 69 is not a square mod 420.

Exercise: For any odd positive integer m, prove that 69 is an m-th power mod 420. In fact,

$$69^m \equiv 69 \pmod{420}.$$

More generally, we see that applying the Chinese Remainder Theorem allows us to reduce to the case $m = p^k$ using the prime factorization $p_1^{k_1} \cdots p_r^{k_r}$ of m. In the above example, the numbers are small enough that we can calculate directly, but what if we need to determine if 69 is a square mod 101^{420}? Here is the general algorithm.

- Chinese Remainder Theorem allows us to reduce to the case $m = p^k$.
- Hensel's Lemma (to be discussed later) allows us to reduce to the case $m = p$.
- Quadratic reciprocity allows us to handle the $m = p$ case.

We consider the case where $m = p$ is a prime first. When $p = 2$, every integer is a quadratic residue. So we assume p is odd. Let's use $p = 7$ as an example. Recall by Theorem 8.2 that there exists a primitive element $\alpha \in \mathbb{F}_7^\times$, so that all the elements of $\mathbb{F}_7$ are given by $0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$. (Even more explicitly, we can take $\alpha = 3$.) Let's square them to find the squares, recalling that $\alpha^6 = 1$.

b	0	α	α^2	α^3	α^4	α^5	α^6
b^2	0	α^2	α^4	α^6	α^2	α^4	α^6
Is b a square	✓	×	✓	×	✓	×	✓
b^3	0	α^3	α^6	α^3	α^6	α^3	α^6
$b^{(p-1)/2}$	0	-1	1	-1	1	-1	1

We collect some important observations:

- $b = \alpha^k$ is a square if and only if k is even. This is essentially because $p-1$ is even, so there is no funny wrapping around. If $k = 2\ell$ is even, then $\alpha^k = (\alpha^\ell)^2$. Conversely, if $\alpha^k = (\alpha^\ell)^2$ for some $\ell \in \mathbb{Z}$, then $p - 1 \mid k - 2\ell$ and so k is even since p is odd.
- $\alpha^{(p-1)/2} = -1$. This is because $\alpha^{(p-1)/2} \neq 1$ but its square is 1. In a field, the only roots of $x^2 = 1$ are ± 1.

Corollary 9.1 *Let p be an odd prime. Let $a \in \mathbb{F}_p$, then*

$$a^{(p-1)/2} = \begin{cases} 1 & \text{if } a \text{ is a nonzero quadratic residue} \\ -1 & \text{if } a \text{ is a quadratic non-residue} \\ 0 & \text{if } a = 0. \end{cases}$$

Proof: Let α be a primitive element. Write $a = \alpha^k$ for some $k = 0, \ldots, p-2$. If $k = 2\ell$ is even, then $a^{(p-1)/2} = \alpha^{(p-1)\ell} = 1$. If $k = 2\ell + 1$ is odd, then $a^{(p-1)/2} = \alpha^{(p-1)\ell + (p-1)/2} = -1$. □

We define the Legendre symbol $\left(\frac{a}{p}\right)$ to be the integer 1, -1 or 0 depending on if a is a nonzero quadratic residue, quadratic non-residue, or 0 in $\mathbb{F}_p$. In other words,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p},$$

from which we see that it is multiplicative:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

so that the product/quotient of two quadratic non-residues is a quadratic residue. The result

$$p \text{ is a square in } \mathbb{F}_q \qquad \Longleftrightarrow \qquad q^* \text{ is a square in } \mathbb{F}_p$$

that we proved (where $q^* = (-1)^{(q-1)/2}q$) can be expressed as

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right).$$

We now state the full quadratic reciprocity (and its complementary laws).

Theorem 9.2 *The Legendre symbols satisfy:*

(a) -1 *is a quadratic residue mod* p *if and only if* $p = 2$ *or* $p \equiv 1 \pmod 4$. *In other words, for* $p \neq 2$,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

(b) 2 *is a quadratic residue mod* p *if and only if* $p = 2$ *or* $p \equiv \pm 1 \pmod 8$. *In other words, for* $p \neq 2$,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

(c) If p, q *are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

In particular

$$\begin{aligned} \left(\frac{p}{q}\right) &= -\left(\frac{q}{p}\right), \text{ if both } p, q \equiv 3 \pmod 4; \\ \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right), \quad \text{otherwise.} \end{aligned}$$

For example, suppose we want to find $\left(\frac{69}{101}\right)$. We first use multiplicativity to get

$$\left(\frac{69}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{23}{101}\right).$$

Then we apply (c):

$$\left(\frac{3}{101}\right) = \left(\frac{101}{3}\right) = \left(\frac{2}{3}\right) = -1$$
$$\left(\frac{23}{101}\right) = \left(\frac{101}{23}\right) = \left(\frac{9}{23}\right) = 1.$$

So $\left(\frac{69}{101}\right) = -1$ and 69 is not a square mod 101.

Lecture 25 Wed 11/06

Some proofs

Theorem 9.2(a) follows almost immediately from the definition of the Legendre symbol. We know

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}.$$

Since both sides are ± 1 and $1 \not\equiv -1 \pmod{p}$ since $p \nmid 2$, we see that they must be equal. Theorem 9.2(c) then follows from what we proved and multiplicativity:

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{-1}{p}\right)^{(q-1)/2} = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}$$

and then multiplying both sides by $\left(\frac{q}{p}\right)$ noting that $\left(\frac{q}{p}\right) = \pm 1$ so it squares to 1. Theorem 9.2(b) requires some work. The key idea is

$$\zeta_8 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \qquad \text{and} \qquad \zeta_8^{-1} = \bar{\zeta}_8 = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i, \qquad \text{so} \qquad \zeta_8 + \zeta_8^{-1} = \sqrt{2},$$

except we need to do this in $\mathbb{F}_p$, not $\mathbb{C}$. In which $\mathbb{F}_{p^d}$ can we find an element α with $o(\alpha) = 8$? Any d such that $8 \mid p^d - 1$. We can always take $d = \phi(8) = 4$, but we can also take $d = 2$ since any odd number squared is 1 mod 8. Now we take $\beta = \alpha + \alpha^{-1}$. Then

$$\beta^2 = \alpha^2 + 2 + \alpha^{-2}.$$

Since $\alpha^8 = 1$ and $\alpha^4 \neq 1$, we have $\alpha^4 = -1$, and so $\alpha^2 = -\alpha^{-2}$. Hence $\beta^2 = 2$. Since we are in characteristic p, we have $\beta^p = \alpha^p + \alpha^{-p}$. Since $\alpha^8 = 1$, we see that β^p depends only on what p is mod 8. It is now easy to check that if $p \equiv \pm 1 \pmod{8}$, then

$$\beta^p = \alpha^1 + \alpha^{-1} = \beta$$

and when $p \equiv \pm 3 \pmod{8}$,

$$\beta^p = \alpha^3 + \alpha^{-3} = -\alpha^{-1} - \alpha = -\beta.$$

Therefore, $\beta \in \mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod{8}$. □

Remark: There is another proof of (b) using the complex ζ_8. We consider $(1+i)^2 = 2i$. Then

$$(1+i)^p = ((1+i)^2)^{(p-1)/2}(1+i) = 2^{(p-1)/2} i^{(p-1)/2}(1+i).$$

On the other hand, we have

$$(1+i)^p \equiv 1 + i^p \pmod{p}.$$

By considering the possible values of p mod 8, we can compute $2^{(p-1)/2}$ mod p, which is exactly $\left(\frac{2}{p}\right)$.

Corollary 9.3 *We have that -2 is a quadratic residue mod p if and only if $p = 2$ or $p \equiv 1$ or 3 mod 8.*

Proof: Suppose $p \neq 2$. We know that -2 is a quadratic residue precisely when both -1 and 2 are quadratic residues or when they are both non-residues. The first case corresponds to $p \equiv 1 \pmod{8}$ and the second case corresponds to $p \equiv 3 \pmod{8}$. □

Corollary 9.4 *We have*

(a) 3 is a quadratic residue mod p if and only if $p = 3$ or $p \equiv \pm 1 \pmod{12}$.

(b) 5 is a quadratic residue mod p if and only if $p = 5$ or $p \equiv \pm 1, \pm 9 \pmod{20}$.

(c) 7 is a quadratic residue mod p if and only if $p = 7$ or $p \equiv \pm 1, \pm 9, \pm 25 \pmod{28}$.

(d) Suppose p, q are distinct odd primes. Then q is a quadratic residue mod p if and only if $p \equiv \pm a^2 \pmod{4q}$ for some odd integer a.

There are over 200 proofs of Quadratic reciprocity (usually referring to Theorem 9.2(c))! Here is another proof similar to (b). Let $\alpha \in \mathbb{F}_{p^{q-1}}$ be an element with $o(\alpha) = q$. We define

$$\beta = \sum_{m \in \mathbb{F}_q} \left(\frac{m}{q}\right) \alpha^m.$$

Then one proves that

$$\beta^2 = q^* \qquad \text{and} \qquad \beta^p = \left(\frac{p}{q}\right)\beta.$$

As a running example, we take $p = 5$ and $q = 3$. Then $\alpha \in \mathbb{F}_{25}$ is a primitive cube root of unity. In fact, we may take $\alpha = x + (x^2 + x + 1)$ in $\mathbb{F}_5[x]/(x^2 + x + 1)$. Then

$$\beta = \left(\frac{0}{3}\right)\alpha^0 + \left(\frac{1}{3}\right)\alpha^1 + \left(\frac{2}{3}\right)\alpha^2 = \alpha - \alpha^2 = \alpha - (-\alpha - 1) = 2\alpha + 1.$$

We can now compute

$$\beta^2 = 4\alpha^2 + 4\alpha + 1 = 4(-\alpha - 1) + 4\alpha + 1 = -3 = 3^*.$$

Note also that

$$\beta^5 = \alpha^5 - \alpha^{10} = \alpha^2 - \alpha = -\beta = \left(\frac{3}{5}\right)\beta.$$

If we were to try this with $p = 7$ and $q = 3$, then in fact we may take $\alpha = 2 \in \mathbb{F}_7$. Then $\beta = \alpha - \alpha^2 = -2$ and $\beta^2 = 4 = -3$ in $\mathbb{F}_7$.

Back to the general case, we square β to get

$$\beta^2 = \sum_{m \in \mathbb{F}_q} \sum_{n \in \mathbb{F}_q} \left(\frac{m}{q}\right)\left(\frac{n}{q}\right)\alpha^{m+n} = \sum_{m \in \mathbb{F}_q} \sum_{n \in \mathbb{F}_q} \left(\frac{mn}{q}\right)\alpha^{m+n}.$$

Now we collect terms with the same power of α. Note that $t = m + n$ takes arbitrary values in $\mathbb{F}_q$:

$$\beta^2 = \sum_{t \in \mathbb{F}_q} \left(\sum_{m \in \mathbb{F}_q} \left(\frac{m(t-m)}{q}\right) \right) \alpha^t = \sum_{t \in \mathbb{F}_q} \left(\sum_{m \in \mathbb{F}_q^\times} \left(\frac{m(t-m)}{q}\right) \right) \alpha^t$$

where we removed the $m = 0$ term because the legendre symbol $\left(\frac{m(t-m)}{q}\right)$ is 0. Let's see what the inner sum is equal to in our example:

$$\begin{aligned}
t = 0 \quad &: \quad \left(\frac{1(-1)}{3}\right) + \left(\frac{2(-2)}{3}\right) = \left(\frac{-1}{3}\right) \cdot 2 \\
t = 1 \quad &: \quad \left(\frac{1(0)}{3}\right) + \left(\frac{2(-1)}{3}\right) = \left(\frac{-1}{3}\right) \cdot (-1) \\
t = 2 \quad &: \quad \left(\frac{1(1)}{3}\right) + \left(\frac{2(0)}{3}\right) = \left(\frac{-1}{3}\right) \cdot (-1)
\end{aligned}$$

If we then factor out the $\left(\frac{-1}{3}\right)$, we get

$$2 - \alpha - \alpha^2 = 3 - (1 + \alpha + \alpha^2) = 3.$$

In general, as a primitive q-th root of unity, α satisfies

$$1 + \alpha + \cdots + \alpha^{q-1} = 0.$$

This suggests that we should prove

$$t=0 \quad : \quad \sum_{m\in\mathbb{F}_q^\times}\Big(\frac{m(t-m)}{q}\Big)=\Big(\frac{-1}{q}\Big)\cdot(q-1),$$
$$t\neq 0 \quad : \quad \sum_{m\in\mathbb{F}_q^\times}\Big(\frac{m(t-m)}{q}\Big)=\Big(\frac{-1}{q}\Big)\cdot(-1),$$

which would imply that

$$\beta^2=\Big(\frac{-1}{q}\Big)\left((q-1)-\alpha-\alpha^2-\cdots-\alpha^{q-1}\right)=\Big(\frac{-1}{q}\Big)q=q^*.$$

Since $m\neq 0$, we have

$$\Big(\frac{m(t-m)}{q}\Big)=\Big(\frac{-m^2(1-tm^{-1})}{q}\Big)=\Big(\frac{-m^2}{q}\Big)\Big(\frac{1-tm^{-1}}{q}\Big)=\Big(\frac{-1}{q}\Big)\Big(\frac{1-tm^{-1}}{q}\Big).$$

If $t=0$, then we get $\left(\frac{-1}{q}\right)$ for each $m\in\mathbb{F}_q^\times$. There are $q-1$ of them, so we get the desired formula for $t=0$. When $t\neq 0$, tm^{-1} runs through every element in $\mathbb{F}_q^\times$ and so $1-tm^{-1}$ runs through every element in $\mathbb{F}_q$ that is not 1. Hence

$$\sum_{m\in\mathbb{F}_q^\times}\Big(\frac{1-tm^{-1}}{q}\Big)=\sum_{s\in\mathbb{F}_q}\Big(\frac{s}{q}\Big)-\Big(\frac{1}{q}\Big)=\sum_{s\in\mathbb{F}_q^\times}\Big(\frac{s}{q}\Big)+\Big(\frac{0}{q}\Big)-\Big(\frac{1}{q}\Big)=-1.$$

Here the first sum is 0 because half the elements of $\mathbb{F}_q^\times$ are quadratic residues and the other halfs are quadratic nonresidues. We have therefore proved that

$$\beta^2=q^*.$$

We next compare β^p with β to see if β lies in $\mathbb{F}_p$. Since we are in characteristic p and since $\left(\frac{m}{q}\right)$ only takes value in $0,1,-1$, all of which are fixed by raising to the power p, we have

$$\beta^p=\sum_{m\in\mathbb{F}_q}\Big(\frac{m}{q}\Big)^p\alpha^{mp}=\sum_{m\in\mathbb{F}_q}\Big(\frac{m}{q}\Big)\alpha^{mp}.$$

Since $p\neq q$, as m varies in $\mathbb{F}_q$, mp runs through all values of $\mathbb{F}_q$. Setting $t=mp$, we get

$$\beta^p=\sum_{t\in\mathbb{F}_q}\Big(\frac{tp^{-1}}{q}\Big)\alpha^t=\Big(\frac{p^{-1}}{q}\Big)\sum_{t\in\mathbb{F}_q}\Big(\frac{t}{q}\Big)\alpha^t=\Big(\frac{p}{q}\Big)\beta.$$

Therefore, we conclude that q^* is a quadratic residue in $\mathbb{F}_p$ if and only if $\left(\frac{p}{q}\right)=1$. In other words,

$$\Big(\frac{q^*}{p}\Big)=\Big(\frac{p}{q}\Big).$$

Multiplicativity of the Legendre symbol and quadratic reciprocity allow us to determine whether a is a square mod p for any prime p. We will talk about Hensel's lemma next time which upgrades this to mod p^k. We first reduce to the case $p\nmid a$.

We start with an example: is 69 a square mod 23^2? Suppose there is an integer c such that

$$c^2\equiv 69 \pmod{23^2}.$$

Hence $23^2\mid c^2-69$. So $\nu_{23}(c^2-69)\geq 2$ but $\nu_{23}(69)=1$. Hence $\nu_{23}(c^2)=1$. (Recall that if $\nu_p(m)\neq\nu_p(n)$, then $\nu_p(m+n)=\min\{\nu_p(m),\nu_p(n)\}$. However, this is impossible because $\nu_{23}(c^2)=2\nu_{23}(c)$ is odd.

Lemma 9.5 *Suppose $p \mid a$. Then $x^2 \equiv a \pmod{p^k}$ has a solution if and only if $\nu_p(a) \geq k$ or if $\nu_p(a)$ is even and*

$$x^2 \equiv a/p^{\nu_p(a)} \pmod{p^{k-\nu_p(a)}}$$

has a solution.

Proof: Suppose $\nu_p(a) < k$ and $k \geq 2$. Suppose $c \in \mathbb{Z}$ such that $c^2 \equiv a \pmod{p^k}$. Then $\nu_p(c^2 - a) \geq k$ but $\nu_p(a) < k$. So $2\nu_p(c) = \nu_p(c^2) = \nu_p(a)$ is even. Moreover, dividing by $p^{\nu_p(a)}$ gives

$$\nu_p((c/p^{\nu_p(c)})^2 - a/p^{\nu_p(a)}) \geq k - \nu_p(a).$$

Hence $x^2 \equiv a/p^{\nu_p(a)} \pmod{p^{k-\nu_p(a)}}$ has a solution.

Conversely, given a solution $b^2 \equiv a/p^{\nu_p(a)} \pmod{p^{k-\nu_p(a)}}$ with $\nu_p(a) = 2d$ even, we easily obtain a solution to the original equation by taking bp^d. □

We now assume that $p \nmid a$. The punchline is that the question can be reduced to $m = p$ for p odd, or to $m = 8$ when $p = 2$.

Lecture 26 Fri 11/08

Hensel's Lemma

Theorem 9.6 *(Hensel's lemma) Suppose $f(x) \in \mathbb{Z}[x]$. Let p be a prime and let $\alpha \in \mathbb{Z}$. Suppose*

$$\nu_p(f(\alpha)) > 2\nu_p(f'(\alpha)).$$

Then for any $n \in \mathbb{N}$, there exists $\alpha_n \in \mathbb{Z}$ such that

(a) $\nu_p(f(\alpha_n)) \geq \nu_p(f(\alpha)) + n - 1$,

(b) $\nu_p(\alpha_n - \alpha) = \nu_p(f(\alpha)) - \nu_p(f'(\alpha)) > \nu_p(f'(\alpha))$,

(c) $\nu_p(f'(\alpha_n)) = \nu_p(f'(\alpha))$.

Corollary 9.7 *Suppose $f(x) \in \mathbb{Z}[x]$. Let p be a prime and let $\alpha \in \mathbb{Z}$. Suppose $f(\alpha) \equiv 0 \pmod{p}$ and $p \nmid f'(\alpha)$. Then for any $n \in \mathbb{N}$, there exists $\alpha_n \in \mathbb{Z}$ such that $\alpha_n \equiv \alpha \pmod{p}$ and $f(\alpha_n) \equiv 0 \pmod{p^n}$.*

This process of "lifting" a root mod p to a root mod p^n is called Hensel lifting.

Corollary 9.8 *Let p be an odd prime and let $a \in \mathbb{Z}$ such that $p \nmid a$. Suppose $x^2 \equiv a \pmod{p}$ has a solution. Then $x^2 \equiv a \pmod{p^n}$ has a solution for any $n \in \mathbb{N}$.*

Proof: Consider $f(x) = x^2 - a \in \mathbb{Z}[x]$. Let $\alpha \in \mathbb{Z}$ be a solution to $x^2 \equiv a \pmod{p}$. Then we have $f(\alpha) = 0 \pmod{p}$. Now $f'(\alpha) = 2\alpha$. Since $p \nmid a$, we have $p \nmid \alpha$. Since p is odd, we have $p \nmid 2$. So $p \nmid f'(\alpha)$. Hence for any $n \in \mathbb{N}$, there exists $\alpha_n \in \mathbb{Z}$ such that $f(\alpha_n) \equiv 0 \pmod{p^n}$, which is the same as $\alpha_n^2 \equiv a \pmod{p^n}$. □

Corollary 9.9 *Let a be an odd integer. Suppose $x^2 \equiv a \pmod{8}$ has a solution. Then $x^2 \equiv a \pmod{2^n}$ has a solution for any integer $n \geq 3$.*

Proof: Consider $f(x) = x^2 - a \in \mathbb{Z}[x]$. Let $\alpha \in \mathbb{Z}$ be a solution to $x^2 \equiv a \pmod{8}$. Then we have $\nu_2(f(\alpha)) \geq 3$. Now $f'(\alpha) = 2\alpha$. Since a is odd, we have α is odd. So $\nu_2(f'(\alpha)) = 1$ which satisfies $\nu_2(f(\alpha)) > 2\nu_2(f'(\alpha))$. Hence by Theorem 9.6, for any integer $n \geq 3$, we have $n - 2 \geq 1$ and there exists $\alpha_{n-2} \in \mathbb{Z}$ such that

$$\nu_2(f(\alpha_{n-2})) = \nu_2(f(\alpha)) + (n-2) - 1 \geq n.$$

In other words, $\alpha_{n-2}^2 \equiv a \pmod{2^n}$. □

It is easy to check that the only odd quadratic residue mod 4 is 1, and the only odd quadratic residue mod 8 is also 1. Note that $x^2 \equiv 5 \pmod{8}$ has no solution but $x^2 \equiv 5 \pmod{4}$ does.

Proof of Theorem 9.6: The important observation is that for any integers a, m, we have

$$f(a+m) \equiv f(a) + f'(a)m \pmod{m^2}.$$

Since both sides are linear in $f(x)$, it is enough to check it for $f(x) = x^n$, in which case

$$f(a) + f'(a)m = a^n + na^{n-1}m \equiv (a+m)^n = f(a+m) \pmod{m^2}$$

follows from the binomial expansion for $(a+m)^n$.

We construct α_n by induction on n. When $n = 1$, we take $\alpha_1 = \alpha$. For $n \geq 2$, we define

$$\alpha_n = \alpha_{n-1} - \left[\frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\right]_p.$$

Here, for two integers a, b with $\nu_p(a) \geq \nu_p(b)$, we use $[\frac{a}{b}]_p$ to denote any integer c such that $\nu_p(a - bc) > \nu_p(a)$. (This is not standard notation!) To see such an integer always exist, we write $a = p^s u$ and $b = p^t v$ where $p \nmid uv$ and $s \geq t$. Let w be an integer such that $u \equiv vw \pmod{p}$. Then $p \mid u - vw$. We then take $[\frac{a}{b}]_p = p^{s-t}w$. Note that $\nu_p([\frac{a}{b}]_p) = \nu_p(a) - \nu_p(b)$. We now prove inductively that for $n \geq 2$,

- $\nu_p(f(\alpha_n)) > \nu_p(f(\alpha_{n-1}))$
- $\nu_p(f'(\alpha_n)) = \nu_p(f'(\alpha))$
- $\nu_p(f(\alpha_n)) > 2\nu_p(f'(\alpha_n))$.

Indeed, we have

$$f(\alpha_n) \equiv f(\alpha_{n-1}) - f'(\alpha_{n-1})\left[\frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\right]_p \pmod{\left[\frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\right]_p^2}$$

where

$$\nu_p\left(f(\alpha_{n-1}) - f'(\alpha_{n-1})\left[\frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\right]_p\right) > \nu_p(f(\alpha_{n-1}))$$

and

$$\nu_p\left(\left[\frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\right]_p^2\right) = 2\nu_p(f(\alpha_{n-1})) - 2\nu_p(f'(\alpha_{n-1})) > \nu_p(f(\alpha_{n-1}))$$

by induction. This proves $\nu_p(f(\alpha_n)) > \nu_p(f(\alpha_{n-1}))$. For the derivative, we have

$$f'(\alpha_n) \equiv f'(\alpha_{n-1}) - f''(\alpha_{n-1})\left[\frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\right]_p \pmod{\left[\frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\right]_p^2}$$

where

$$\nu_p\left(\left[\frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\right]_p\right) = \nu_p(f(\alpha_{n-1})) - \nu_p(f'(\alpha_{n-1})) > \nu_p(f'(\alpha_{n-1})).$$

This proves $\nu_p(f'(\alpha_n)) = \nu_p(f'(\alpha_{n-1})) = \nu_p(f'(\alpha))$ and

$$\nu_p(f(\alpha_n)) > \nu_p(f(\alpha_{n-1})) > 2\nu_p(f'(\alpha_{n-1})) = 2\nu_p(f'(\alpha_n)).$$

It now follows (by another easy induction) from $\nu_p(f(\alpha_n)) \geq \nu_p(f(\alpha_{n-1})) + 1$ that

$$\nu_p(f(\alpha_n)) \geq \nu_p(f(\alpha)) + n - 1$$

and

$$\alpha_n - \alpha = -\left[\frac{f(\alpha_1)}{f'(\alpha_1)}\right]_p - \left[\frac{f(\alpha_2)}{f'(\alpha_2)}\right]_p - \cdots - \left[\frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\right]_p$$

has the same valuation as the first term. □

If we go through the above proof, it is not hard to see that our construction was pretty much forced. In particular, we have the following uniqueness result.

Proposition 9.10 *(Uniqueness of Hensel's lemma) Suppose $f(x) \in \mathbb{Z}[x]$. Let p be a prime and let $\alpha \in \mathbb{Z}$. Suppose $\nu_p(f(\alpha)) > 2\nu_p(f'(\alpha))$. For any $n \in \mathbb{N}$, let α_n be constructed as above. Then if $\beta \in \mathbb{Z}$ such that*

(a) $\nu_p(f(\beta)) \geq \nu_p(f(\alpha)) + n - 1$,

(b) $\nu_p(\beta - \alpha) \geq \nu_p(f(\alpha)) - \nu_p(f'(\alpha))$.

Then

$$\nu_p(\beta - \alpha_n) \geq \nu_p(f(\alpha)) - \nu_p(f'(\alpha)) + n - 1.$$

Proof: Write $\beta = \alpha_n + m$. Then by condition (b) for β (and for α_n), we have

$$\nu_p(m) = \nu_p((\beta - \alpha) - (\alpha_n - \alpha)) \geq \nu_p(f(\alpha)) - \nu_p(f'(\alpha)) > \nu_p(f'(\alpha)).$$

Let $a = f(\beta) - f(\alpha_n)$, which we know has valuation at least $\nu_p(f(\alpha)) + n - 1$. Let $u = f'(\alpha_n)$ which we know has the same valuation as $f'(\alpha)$. Then from $f(\beta) \equiv f(\alpha_n) + f'(\alpha_n)m \pmod{m^2}$, we have

$$m^2 \mid a - um.$$

Hence

$$\nu_p(a - um) \geq 2\nu_p(m) > \nu_p(f'(\alpha)) + \nu_p(m) = \nu_p(um).$$

So

$$\nu_p(a) = \nu_p(a - um + um) = \nu_p(um) = \nu_p(f'(\alpha)) + \nu_p(m).$$

Hence

$$\nu_p(m) = \nu_p(a) - \nu_p(f'(\alpha)) \geq \nu_p(f(\alpha)) - \nu_p(f'(\alpha)) + n - 1,$$

as desired. □

Corollary 9.11 *Suppose $f(x) \in \mathbb{Z}[x]$. Let p be a prime and let $\alpha \in \mathbb{Z}$. Suppose $f(\alpha) \equiv 0 \pmod{p}$ and $p \nmid f'(\alpha)$. Then for any $n \in \mathbb{N}$, there exists $\alpha_n \in \mathbb{Z}$, unique mod p^n, such that $\alpha_n \equiv \alpha \pmod{p}$ and $f(\alpha_n) \equiv 0 \pmod{p^n}$.*

Remark: The notation $[\frac{a}{b}]_p$ is very awkward. In HW 9 P4 (bonus), you will see that in the correct ring, namely $\mathbb{Z}_p$, we can literally write $\frac{a}{b}$. Then Hensel's Lemma is exactly Newton's method but done in $\mathbb{Z}_p$.

Example: Consider $f(x) = (x^2 - 2)(x^2 - 17)(x^2 - 34) \in \mathbb{Z}[x]$. Then $f(x) = 0$ has no solution in $\mathbb{Z}$. We claim that it has a solution in $\mathbb{Z}/m\mathbb{Z}$ for any $m \in \mathbb{N}$. By the Chinese Remainder Theorem, it suffices to consider when $m = p^k$ is a power of p and show that at least one of $2, 17, 34$ is a quadratic residue mod m. If $p \neq 2, 17$, then at least one of $2, 17, 34$ is a quadratic residue mod p as

$$\left(\frac{34}{p}\right)\left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{2}{p}\right)^2\left(\frac{17}{p}\right)^2 = 1$$

and by Corollary 9.8 is a quadratic residue mod p^k. If $p = 17$, then $2 = 6^2$ is a quadratic residue mod 17 and also mod 17^k. Finally, since $17 \equiv 1 \pmod{8}$, it is a quadratic residue mod 8 and so is also mod 2^k.

Remark: It is a fairly nontrivial fact that if $f(x) \in \mathbb{Z}[x]$ is irreducible (in $\mathbb{Q}[x]$), then there are infinitely many primes p for which $f(x)$ has no roots mod p. An irreducible polynomial in $\mathbb{Z}[x]$ can be reducible mod p for all primes p. We have seen that $x^4 + 1$ satisfies this. As we will learn soon, most cyclotomic polynomials are reducible mod every prime but are irreducible in $\mathbb{Z}[x]$.

Lecture 26.5 Fri 11/08
Tutorial
Jacobi symbol

Our algorithm for determining whether a is a square mod m starts by factoring m. However, factorization is notoriously difficult. For example, let's see if 69 is a square mod 5338. We can quickly factor $5338 = 2 \times 2669$ so it suffices to check mod 2 and mod 2669. Everything is a square mod 2 but it takes some nontrivial effort to check whether 2669 is prime or not. If we pretend that we can use the Legendre symbol with composite "denominators" and that the same laws of quadratic reciprocity hold, then

$$\left(\frac{69}{2669}\right) = \left(\frac{2669}{69}\right) = \left(\frac{2600}{69}\right) = \left(\frac{26}{69}\right) = \left(\frac{2}{69}\right)\left(\frac{13}{69}\right) = -\left(\frac{69}{13}\right) = -\left(\frac{4}{13}\right) = -1.$$

We would then guess that 69 is not a square mod 2669. This in fact can be made precise using the Jacobi symbol.

Given two coprime integers a, b where b is a positive odd integer, we factor $b = p_1 \cdots p_r$ into a product of (possibly equal) odd primes. Then we define the Jacobi symbol

$$\left(\frac{a}{b}\right) := \prod_{j=1}^{r} \left(\frac{a}{p_j}\right).$$

Note that if $\left(\frac{a}{b}\right) = -1$, then that means some $\left(\frac{a}{p_j}\right) = -1$ so a is not a square mod p_j for some prime divisor p_j of b, which implies that a is not a square mod b. However, if $\left(\frac{a}{b}\right) = 1$, then we cannot deduce anything about whether a is a square mod b. It is not hard to use the usual laws of quadratic reciprocity for Legendre symbols to deduce the same laws of quadratic reciprocity for Jacobi symbols.

Theorem 9.12 *(Quadratic reciprocity for Jacobi symbols) Let b be a positive odd integer. Then:*

(a) $\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}$;

(b) $\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}$;

(c) if a is a positive odd integer coprime to b, then $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/4}$.

Proof: We write $b = p_1 \cdots p_r$. (a) Note that for any odd integer m, $(-1)^{(m-1)/2} \equiv m \pmod 4$. Hence

$$\left(\frac{-1}{b}\right) = \prod_{i=1}^{r} (-1)^{(p_i-1)/2} \equiv p_1 \cdots p_r \equiv b \equiv (-1)^{(b-1)/2} \pmod 4.$$

Hence they are equal as integers because they are ± 1.

(b) It suffices to prove that

$$\sum_{i=1}^{r} \frac{p_i^2 - 1}{8} \equiv \frac{(p_1 \cdots p_r)^2 - 1}{8} \pmod 2$$

by induction on r. It is clearly true for $r = 1$. Suppose $r \geq 2$. Then,

$$\begin{aligned}
\frac{(p_1 \cdots p_r)^2 - 1}{8} &= p_r^2 \frac{(p_1 \cdots p_{r-1})^2 - 1}{8} + \frac{p_r^2 - 1}{8} \\
&\equiv \frac{(p_1 \cdots p_{r-1})^2 - 1}{8} + \frac{p_r^2 - 1}{8} \pmod 2 \qquad \text{since } p_r \text{ is odd} \\
&\equiv \sum_{i=1}^{r-1} \frac{p_i^2 - 1}{8} + \frac{p_r^2 - 1}{8} \pmod 2 \qquad \text{by induction} \\
&\equiv \sum_{i=1}^{r} \frac{p_i^2 - 1}{8} \pmod 2.
\end{aligned}$$

(c) Let $b^* = (-1)^{(b-1)/2}b$. Then by (a) and multiplicativity, we have

$$\left(\frac{b^*}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}\left(\frac{b}{a}\right).$$

Note also by (a), we have $b^* = p_1^* \cdots p_r^*$. Note that

$$b^* = \left(\frac{-1}{b}\right)b = \prod_{i=1}^{r}\left(\frac{-1}{p_i}\right)p_i = \prod_{i=1}^{r} p_i^*.$$

Therefore, for $a = q_1 \cdots q_t$, we have

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{r}\left(\frac{a}{p_i}\right) = \prod_{i=1}^{r}\prod_{j=1}^{t}\left(\frac{q_j}{p_i}\right) = \prod_{j=1}^{t}\prod_{i=1}^{r}\left(\frac{p_i^*}{q_j}\right) = \prod_{j=1}^{r}\left(\frac{b^*}{q_j}\right) = \left(\frac{b^*}{a}\right).$$

The proof is now complete. □

Remark 1: It turns out that 2669 is a prime. So $\left(\frac{69}{2669}\right)$ is the actual Legendre symbol, but we could use Jacobi symbols to compute it. If it is 1, we would be able to say that the "numerator" is a square mod 2669.

Remark 2: It is very easy to write down examples where $\left(\frac{a}{b}\right) = 1$ but a is not a square mod b. For example, if b is a square, then $\left(\frac{a}{b}\right) = 1$ for any a coprime to b. Say $\left(\frac{2}{9}\right) = 1$ but 2 is not a square mod 3 and so not a square mod 9. Here is a more interesting example. Consider the Fermat numbers $F_n = 2^{2^n} + 1$. Suppose $m > n \geq 2$ so that $F_n, F_m \equiv 1 \pmod 8$. We saw before that the distinct Fermat numbers are coprime. Now

$$2^{2^m} = 2^{2^n 2^{m-n}} = (2^{2^n})^{2^{m-n}} \equiv (-1)^{2^{m-n}} \equiv 1 \pmod{F_n}.$$

Hence, we have

$$F_m \equiv 2 \pmod{F_n}.$$

Computing Jacobi symbols gives

$$\left(\frac{F_n}{F_m}\right) = \left(\frac{F_m}{F_n}\right) = \left(\frac{2}{F_n}\right) = 1.$$

However, using $F_2 = 17$ and the prime divisor 641 of F_5, we have

$$\left(\frac{17}{641}\right) = \left(\frac{641}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{3}{17}\right) = -1.$$

So F_2 is not a square mod F_5. Exercise: If $m > n \geq 2$, then F_m is a square mod F_n.

Recall that the Legendre symbol satisfies

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p.$$

This was in some sense the definition of Legendre symbols and it relies on the fact that $\mathbb{F}_p^\times$ has a primitive element. Suppose now n is a composite squarefree odd integer, say 69. Is it possible for all a coprime to 69 to satisfy

$$a^{34} \equiv \left(\frac{a}{69}\right) \pmod{69}?$$

Suppose it is true. Then we would also have

$$a^{34} \equiv \left(\frac{a}{69}\right) \pmod{23}.$$

Note that a^{34} mod 23 depends only on a mod 23, but

$$\left(\frac{a}{69}\right) = \left(\frac{a}{3}\right)\left(\frac{a}{23}\right)$$

depends both on a mod 23 and on a mod 3. So we would have a contradiction by taking $a_1 = 2$ and $a_2 = 25$. They are congruent mod 23, but

$$\left(\frac{a_1}{3}\right) = \left(\frac{2}{3}\right) = -1 \neq \left(\frac{1}{3}\right) = \left(\frac{a_2}{3}\right).$$

So we have a contradiction because

$$a_1^{34} \equiv a_2^{34} \pmod{23} \qquad \text{but} \qquad \left(\frac{a_1}{69}\right) \not\equiv \left(\frac{a_2}{69}\right) \pmod{23}.$$

It turns out in this case that

$$2^{34} \equiv 25^{34} \equiv 25 \not\equiv \pm 1 \pmod{69}.$$

Due to how easy it is to compute Jacobi symbols (essentially Euclidean algorithm) and how easy it is to compute a^k mod m (to be discussed later), the congruence equation

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

can be used to test whether n is a prime. More on this next!

Exercises

9.1 Let $p \geq 3$ be a prime and let a, b be two primitive elements mod p. Prove that ab is not primitive.

9.2 Is 91 a quadratic residue mod 253?

9.3 Prove that the polynomial $x^8 - 16$ has a root mod p for all primes p.

9.4 Find all solutions to $x^4 + x^3 + 2x^2 + x \equiv 13 \pmod{343}$.

9.5 Find all solutions to $x^3 - 2x - 1 \equiv 0 \pmod{125}$.

Lecture 27 Mon 11/11
Basic definition of Group theory

10 Group Theory

A group is a set G equipped with one binary operation, one unary operation and one nullary operation:

$$(a, b) \mapsto ab : G \times G \to G \qquad a \mapsto a^{-1} : G \to G, \qquad e \in G$$

such that for any $a, b, c \in G$,

(a) (Associative) $a(bc) = (ab)c$;

(b) (Multiplicative identity) $a \cdot e = a$ and $a \cdot a^{-1} = e$.

With a little bit of work, one can prove that $e \cdot a = a$ and $a^{-1} \cdot a = e$. If $ab = ba$ for all $a, b \in G$, we say G is an abelian group. All the groups that we will encounter in this class are abelian groups.

The advantage of doing rings first is that we now have a lot of examples of abelian groups. Suppose R is a commutative ring. Then we can associate to it two abelian groups:

- The additive group $(R, +)$ of a ring R, where we forget about multiplication and use addition as the binary operation, negation as inversion, and 0 as e.
- The multiplicative group $(R^\times, \cdot)$ of units $R^\times$ with multiplication, inversion and 1 from the ring R.

For example, we have the group $\mathbb{Z}/m\mathbb{Z}$ with addition, and the group $(\mathbb{Z}/m\mathbb{Z})^\times$ with multiplication.

A subgroup of a group G is a subset $H \subseteq G$ closed under all the group operations: $e \in H$ and for all $a, b \in H$, we have $a^{-1} \in H$ and $ab \in H$. The standard notation is $H \leq G$. Given any element $g \in G$, we write $\langle g \rangle$ for the subgroup of G generated by g. Namely,

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} = \{e, g, g^2, \ldots, g^{-1}, g^{-2}, \ldots\}.$$

For example, in $(\mathbb{Z}/69\mathbb{Z}, +)$, we have

$$\langle 23 \rangle = \{0, 23, 46\} \qquad \text{and} \qquad \langle 5 \rangle = \{0, 5, 10, 15, 20, 25, \ldots, 65, 1, 6, 11, \ldots\} = \mathbb{Z}/69\mathbb{Z}.$$

In $(\mathbb{Z}/69\mathbb{Z})^\times$, we find that

$$\langle 5 \rangle = \{1, 5, 25, 56, 4, 20, 31, 17, 16, 11, 55, 68, 64, 44, 13, 65, 49, 38, 52, 53, 58, 14\}$$

is a subgroup of order 22 while $(\mathbb{Z}/69\mathbb{Z})^\times$ has order $\phi(69) = 44$. As usual, we define the order $o(g)$ of an element g as the smallest positive integer d such that $g^d = e$, if it exists. Then $o(g) = |\langle g \rangle|$.

Theorem 10.1 *(Lagrange's Theorem) Suppose H is a subgroup of a finite group G. Then $|H| \mid |G|$.*

"Proof" by example: Note that

$$\begin{aligned} \langle 5 \rangle &= \{1, 5, 25, 56, 4, 20, 31, 17, 16, 11, 55, 68, 64, 44, 13, 65, 49, 38, 52, 53, 58, 14\} \\ 2 \cdot \langle 5 \rangle &= \{2, 10, 50, 43, 8, 40, 62, 34, 32, 22, 41, 67, 59, 19, 26, 61, 29, 7, 35, 37, 47, 28\}. \end{aligned}$$

They have the same size as $|\langle 5 \rangle|$ and form a partition of $(\mathbb{Z}/69\mathbb{Z})^\times$. □

Proof: Define a relation on G by $a \sim b$ if $a = bh$ for some $h \in H$. We check that it is an equivalence relation.

- $a \sim a$ follows because $e \in H$ and $a = ae$.
- If $a \sim b$, then $a = bh$ for some $h \in H$. Multiplying by $h^{-1} \in H$ gives $ah^{-1} = b$. So $b \sim a$.
- If $a \sim b$ and $b \sim c$, then $a = bh_1$ and $b = ch_2$ for some $h_1, h_2 \in H$. Then $a = ch_2h_1$ and $h_2h_1 \in H$. So $a \sim c$.

Each equivalence class is of the form

$$[a] = aH = \{ah : h \in H\}$$

which has the same number of elements as H. Since the equivalence classes form a partition of the entire G, we see that $|H| \mid |G|$ and the quotient $|G|/|H|$ is the number of distinct equivalence classes. □

Corollary 10.2 *Suppose G is a finite group and $g \in G$. Then $g^{|G|} = e$.*

Corollary 10.3 *Suppose G is a finite group and H is a proper subgroup ($H \leq G$ and $H \neq G$). Then $|H| \leq |G|/2$.*

If there is some $g \in G$ such that $G = \langle g \rangle$, then we say G is cyclic and call g a generator. In general, $\mathbb{Z}/m\mathbb{Z}$ is cyclic with 1 as a generator. If F is a finite field, then $F^\times$ is cyclic, generated by a primitive element. What about $(\mathbb{Z}/69\mathbb{Z})^\times$ and $(\mathbb{Z}/m\mathbb{Z})^\times$ in general? When $m = p$ is a prime, $\mathbb{Z}/p\mathbb{Z}$ is secretly $\mathbb{F}_p$ in which case we know $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Given two groups G_1 and G_2, a group homomorphism is a map $\varphi : G_1 \to G_2$ preserving all the group operations. That is,

$$\varphi(e_{G_1}) = e_{G_2} \qquad \text{and} \qquad \varphi(ab) = \varphi(a)\varphi(b).$$

By taking $b = a^{-1}$, we also get $\varphi(a^{-1}) = \varphi(a)^{-1}$. A group isomorphism is a group homomorphism that is a bijection, and we say the two groups are isomorphic, written $G_1 \cong G_2$. Any two cyclic groups of the same

order are isomorphic (by a map sending a generator of G_1 to a generator of G_2). We write C_m for a/the cyclic group of order m.

From the Chinese Remainder Theorem, we have the ring isomorphism

$$\mathbb{Z}/69\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}.$$

Taking the group of units gives

$$(\mathbb{Z}/69\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/23\mathbb{Z})^\times \cong C_2 \times C_{22}.$$

Is this secretly cyclic?

Lecture 28 Wed 11/13
$(\mathbb{Z}/m\mathbb{Z})^\times$

We note that for any $(a,b) \in C_2 \times C_{22}$, we have $a^2 = e$ and $b^{22} = e$. Then $(a,b)^{22} = (a^{22}, b^{22}) = (e,e)$. So $o(a,b) \mid 22$. Hence, no element in $C_2 \times C_{22}$ can have order 44, implying that it is not cyclic. Similarly, $C_4 \times C_{22}$ is not cyclic, because $(a,b)^{\text{lcm}(4,22)} = (e,e)$ and $\text{lcm}(4,22) < 4 \times 22$.

Lemma 10.4 *Let $m, n \in \mathbb{N}$. Then $C_m \times C_n$ is cyclic if and only if $\gcd(m,n) = 1$.*

Proof: We have proven by example above that if m, n are not coprime, then $\text{lcm}(m,n) < mn$ in which case $C_m \times C_n$ does not have an element of order mn. When m, n are coprime, we already know by the Chinese Remainder Theorem that $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as rings. Forgetting the multiplication gives a group isomorphism $C_{mn} \cong C_m \times C_n$. □

We now consider $(\mathbb{Z}/m\mathbb{Z})^\times$ in general. Suppose $m = p_1^{k_1} \cdots p_r^{k_r}$. Then by the Chinese Reminder Theorem, we have

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^\times.$$

Theorem 10.5 *For any positive integer t,*

$$\begin{aligned}
(\mathbb{Z}/p^t\mathbb{Z})^\times &\cong C_{p^{t-1}(p-1)}, && \text{if } p \text{ is odd,} \\
(\mathbb{Z}/2^t\mathbb{Z})^\times &\cong \begin{cases} 1 & \text{if } t = 1, \\ C_2 & \text{if } t = 2, \\ C_2 \times C_{2^{t-2}} & \text{if } t \geq 3. \end{cases}
\end{aligned}$$

For example, we have

$$\begin{aligned}
(\mathbb{Z}/2023\mathbb{Z})^\times &\cong (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/17^2\mathbb{Z})^\times \cong C_6 \times C_{17 \cdot 16}, \\
(\mathbb{Z}/2024\mathbb{Z})^\times &\cong (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times \times (\mathbb{Z}/23\mathbb{Z})^\times \cong C_2 \times C_2 \times C_{10} \times C_{22}, \\
(\mathbb{Z}/2025\mathbb{Z})^\times &\cong (\mathbb{Z}/3^4\mathbb{Z})^\times \times (\mathbb{Z}/5^2\mathbb{Z})^\times \cong C_{3^3 \cdot 2} \times C_{5 \cdot 4}.
\end{aligned}$$

Is any of them cyclic?

Proof: Suppose first that p is odd. To prove $(\mathbb{Z}/p^t\mathbb{Z})^\times$ is cyclic, we need to find some $a \in \mathbb{Z}$ such that $o_{p^t}(a) = p^{t-1}(p-1)$. A long time ago, in a tutorial far far away, we worked out $o_{49}(2)$ using... LTE! Let's prove by example by finding a generator a for $(\mathbb{Z}/17^3\mathbb{Z})^\times$.

We start with a generator a for $(\mathbb{Z}/17\mathbb{Z})^\times$, which we know exists from the theory of finite fields. Let's say $a = 3$ and we hope that it just works mod 17^3. Note

$$a^{o_{17^3}(a)} \equiv 1 \pmod{17^3} \quad \Rightarrow \quad a^{o_{17^3}(a)} \equiv 1 \pmod{17} \quad \Rightarrow \quad 16 = o_{17}(a) \mid o_{17^3}(a).$$

While it is not important for the proof, it is a fun to see how to find a in this case. Note that $(\mathbb{Z}/17\mathbb{Z})^\times$ has order 16. So a is a generator if and only if $a^8 \neq 1$. Recall that $a^8 = \left(\frac{a}{17}\right)$. So we just need to find a non-square mod 17. We can't take 2 because $17 \equiv 1 \pmod 8$. We can take 3 because $\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$.

We know $o_{17}(3) = 16$. So $\nu_{17}(3^{16}-1) \geq 1$. Suppose first $\nu_{17}(3^{16}-1) \geq 2$. Then we consider

$$(3+17)^{16} - 1 = (3^{16}-1) + 16 \cdot 3^{15} \cdot 17 + 17^2(\cdots).$$

Note that $\nu_{17}(16 \cdot 3^{15} \cdot 17) = 1$ while all the other terms have $\nu_{17} \geq 2$. Hence, we see that either $\nu_{17}(3^{16}-1) = 1$ or $\nu_{17}(20^{16}-1) = 1$. We take $a = 3$ or $a = 20$ depending on which gives $\nu_{17} = 1$. In this case, $\nu_{17}(3^8+1) = \nu_{17}(6562) = 1$ and we know $17 \nmid 3^8 - 1$, so $\nu_{17}(3^{16}-1) = 1$.

Now we can apply LTE (Proposition 3.7) to get

$$\nu_{17}(a^{16 \cdot 17} - 1) = \nu_{17}(a^{16} - 1) + \nu_{17}(17) = 2.$$

This implies that $17^3 \nmid a^{16 \cdot 17} - 1$. So $o_{17^3}(a) \nmid 16 \cdot 17$. However, we know that

$$o_{17^3}(a) \mid 16 \cdot 17^2 \qquad \text{and} \qquad 16 \mid o_{17^3}(a).$$

Combining these, we find that $o_{17^3}(a) = 16 \cdot 17^2$ is the maximal possible.

Suppose now $p = 2$. The cases $(\mathbb{Z}/2\mathbb{Z})^\times = 1$ and $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\} \cong C_2$ can be checked directly. Suppose now $t \geq 3$. We use the same LTE argument with $a = 5$. We have $\nu_2(5-1) = 2$. Since $5 \equiv 1 \pmod 4$, we can use LTE (Proposition 3.11) to get

$$\begin{aligned} \nu_2(5^{2^{t-3}} - 1) &= \nu_2(5-1) + t - 3 = t - 1, \\ \nu_2(5^{2^{t-2}} - 1) &= \nu_2(5-1) + t - 2 = t. \end{aligned}$$

So $o_{2^t}(5) = 2^{t-2}$. Since $5 \equiv 1 \pmod 4$, the same is true for every power of 5. Hence the subgroup $\langle 5 \rangle$ is missing all the elements in $(\mathbb{Z}/2^t\mathbb{Z})^\times$ that are congruent to 3 mod 4. It is easy to check that the map

$$\begin{aligned} \langle -1 \rangle \times \langle 5 \rangle &\to (\mathbb{Z}/2^t\mathbb{Z})^\times \\ (a, b) &\mapsto ab \end{aligned}$$

is a group isomorphism. Therefore,

$$(\mathbb{Z}/2^t\mathbb{Z})^\times \cong \langle -1 \rangle \times \langle 5 \rangle \cong C_2 \times C_{2^{t-2}}.$$

The proof is now complete. □

Now that we have a complete description of $(\mathbb{Z}/m\mathbb{Z})^\times$, which of them are cyclic? Note that if $(\mathbb{Z}/m\mathbb{Z})^\times$ is not cyclic, then for any prime p, we have $o_m(p) \neq \phi(m)$ in which case $\Phi_m(x)$ is not irreducible in any $\mathbb{F}_p[x]$.

Lecture 29 Fri 11/15
Shor's factorization

Recall the examples

$$\begin{aligned} (\mathbb{Z}/2023\mathbb{Z})^\times &\cong (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/17^2\mathbb{Z})^\times \cong C_6 \times C_{17 \cdot 16}, \\ (\mathbb{Z}/2024\mathbb{Z})^\times &\cong (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times \times (\mathbb{Z}/23\mathbb{Z})^\times \cong C_2 \times C_2 \times C_{10} \times C_{22}, \\ (\mathbb{Z}/2025\mathbb{Z})^\times &\cong (\mathbb{Z}/3^4\mathbb{Z})^\times \times (\mathbb{Z}/5^2\mathbb{Z})^\times \cong C_{3^3 \cdot 2} \times C_{5 \cdot 4}. \end{aligned}$$

We note that every cyclic factor has even order. As a result, similar to the $C_m \times C_n$ case with $\gcd(m, n) \neq 1$, we see that no element can have a big enough order to generate the full group. For example, every element in $(\mathbb{Z}/2024\mathbb{Z})^\times$ has order dividing $\operatorname{lcm}(2, 2, 10, 22) = 110$ but $(\mathbb{Z}/2024\mathbb{Z})^\times$ has order 880. In order for $(\mathbb{Z}/m\mathbb{Z})^\times$ to be cyclic, there can only be one cyclic factor of even order.

Corollary 10.6 *Let $m \in \mathbb{N}$. Then $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic if and only if $m = 2, 4, p^t, 2p^t$ for some odd prime p and positive integer t. In particular, if m is an odd composite integer, then $(\mathbb{Z}/m\mathbb{Z})^\times$ is not cyclic.*

We can use this observation to test for primality! The cause for $(\mathbb{Z}/m\mathbb{Z})^\times$ to be non-cyclic is the multitude of C_n factors with n even. Every such factor produces 2 elements a with $a^2 = e$, namely the identity e and $g^{n/2}$ where g is any generator. (In HW 10 P1, you will prove that a cyclic group has a unique subgroup of every possible order, which implies that there are no other elements of order 2.) In terms of the isomorphism

$$(\mathbb{Z}/p^t\mathbb{Z})^\times \cong C_{p^{t-1}(p-1)},$$

these two elements with $a^2 = 1$ are simply 1 and -1. When there are multiple cyclic factors of even order, for example for

$$(\mathbb{Z}/2023\mathbb{Z})^\times \cong (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/17^2\mathbb{Z})^\times \cong C_6 \times C_{17\cdot 16},$$

there are four elements with $a^2 = 1$, as they can be ± 1 mod 7 and ± 1 mod 17^2. Note that $288 = 289 - 1 = 287 + 1$. So the four elements of $(\mathbb{Z}/2023\mathbb{Z})^\times$ that square to 1 are $\pm 1, \pm 288$.

Corollary 10.7 *Suppose m is an odd composite integer. Then there exists an integer $a \not\equiv \pm 1 \pmod m$ such that $a^2 \equiv 1 \pmod m$. Given such an a, the two integers $\gcd(m, a-1)$ and $\gcd(m, a+1)$ are nontrivial divisors of m.*

Proof: Let $m = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization of m. Then $a \equiv \pm 1 \pmod{p_i^{k_i}}$ for $i = 1, \ldots, r$. Then $\gcd(m, a-1)$ is the product of $p_i^{k_i}$ for which $a \equiv 1 \pmod{p_i^{k_i}}$; and $\gcd(m, a+1)$ is the rest. Since $a \not\equiv \pm 1 \pmod m$, both 1 and -1 appear. □

The difficulty is now to find such a nontrivial solution to $x^2 \equiv 1 \pmod m$. We don't want to just check one-by-one (we might as well check for division directly in that case). In practice, m could be some 600 digits number and aint nobody got time for dat. We say a certain algorithm is in polynomial time if the number of arithmetic operations needed is bounded by some polynomial in the number of digits/bits, that is, polynomial in $\log m$. For example, computing gcd via the Euclidean algorithm is in polynomial time, because every time we take the remainder, we lower the number of bits. Finding a nontrivial solution to $x^2 \equiv 1 \pmod m$ by testing inputs one-by-one for division is in exponential time.

Shor's factorization algorithm

1. Pick $b = 1, \ldots, m-1$ at random.
2. Compute $\gcd(b, m)$. If $\gcd(b, m) > 1$, then it is a nontrivial divisor of m and we are done.
3. Suppose $\gcd(b, m) = 1$. Compute $d = o_m(b)$. Then $b^d \equiv 1 \pmod m$.
4. If d is odd, go back to step 1. If d is even, then $b^{d/2}$ is a solution to $x^2 \equiv 1 \pmod m$. If $b^{d/2} \equiv \pm 1 \pmod m$, then go back to step 1. If $b^{d/2} \not\equiv \pm 1 \pmod m$, then we have found a nontrivial solution. (Note that $b^{d/2} \equiv 1 \pmod m$ is not possible since $d = o_m(b)$.)

When m has at least 2 odd prime divisors, there are at most $\frac{1}{2}\phi(m)$ elements $b \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $o_m(b)$ is odd or $b^{o_m(b)/2} \equiv -1 \pmod m$. You will work this out for an example in HW 10. This means that for a randomly chosen b, there is at least a 50% probability that it produces a nontrivial divisor of m. Hence the probability that no answer is found after k iterations is at most $1/2^k$. For $k \geq 80$, this is less than 10^{-24} which is roughly the probability that a calculation error occurs from a cosmic ray hitting the cpu causing Mario to warp to a parallel universe.

There are two important computations in Shor's algorithm: computing $o_m(b)$; and computing $b^{d/2} \pmod m$. The latter (also known as discrete exponentiation), can be done very quickly using the Square and Multiply method. For example, suppose we want to calculate $452^{1563} \bmod 2023$. Then we first express the exponent 1563 as a sum of powers of 2, which it already was when working with a computer:

$$1563 = 1024 + 512 + 16 + 8 + 2 + 1.$$

Then we square 452 repeatedly to find

$$452, 452^2, 452^4, 452^8, \ldots, 452^{1024} \pmod{2023}.$$

Note that before computing the next square, we first reduce mod 2023, so that every step is simply the square of a number at most 2023. Finally we multiply the ones that show up in the binary representation of 1563. The number of squaring and multiplication operations needed is basically the number of bits of the exponent. Each step, we are multiplying numbers less than the modulus. So the whole computation is in polynomial time.

Lecture 29.5 Fri 11/15
Tutorial
RSA

One does not teach a first year intro to number theory course without mentioning RSA. (See also slides on RSA.) RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem, one of the oldest, that is widely used for secure data transmission. Let's discuss its setup:

1. Pick two large distinct primes p and q, say on the order of 2^{1024} or approximately 300 digits.
2. Let $n = pq$ so that $\phi(n) = (p-1)(q-1)$.

   Then for any integer M coprime to n, we have $M^{\phi(n)} \equiv 1 \pmod{n}$. Now if $N \equiv 1 \pmod{\phi(n)}$, then $N = 1 + \phi(n)k$ for some $k \in \mathbb{Z}$ so

   $$M^N = M \cdot M^{\phi(n)k} \equiv M \pmod{n}.$$

3. Pick an integer d coprime to $\phi(n)$.

   Then there exist integers e, t such that $de + t\phi(n) = 1$. The integer e can be easily found using the (Extended) Euclidean algorithm. Note that for any integer M coprime to n,

   $$de \equiv 1 \pmod{\phi(n)} \qquad \Longrightarrow \qquad M^{de} \equiv M \pmod{n}.$$

4. Publish (e, n) as the public key. Keep (d, n) (and p, q) hidden as the private key. It is also customary to replace e and d by their remainders mod $\phi(n)$.

Now when someone wants to send a message M to me, they would take my (e, n) and compute

$$C \equiv M^e \pmod{n}$$

and send C to me. When we receive C, we can recover M mod n via

$$C^d \equiv M^{de} \equiv M \pmod{n}.$$

If we further require that $M = 1, \ldots, n$, for example by restricting the size of the message or by breaking it up into multiple messages, we would recover M exactly.

The security of RSA relies on the following:

1. Given the public key (e, n), it is practically impossible to find the private key (d, n).

   Note that we can find d by solving $ex \equiv 1 \pmod{\phi(n)}$ but this requires finding p and q so we can compute $\phi(n) = (p-1)(q-1)$. In other words, factorization should be hard.
2. Given the message M and the encrypted C, it is practically impossible to find d such that $M \equiv C^d \pmod{n}$.

   This problem is known as discrete logarithm.

In the above, practically impossible means that the current best algorithm would take longer than say 100 years to complete. These algorithms' runtime are exponential in $\log n$, which is basically the number of bits that n has. Even something like e^{100} is already more than 10^{43}.

The efficiency of RSA relies on the ability to compute $M^e \pmod n$ and $C^d \pmod n$ in polynomial time, which we have already seen. It should also be "easy" to generate primes. The traditional sieve of Eratosthenes produces all the primes, but is too slow to generate 300 digit primes. From the prime number theorem, we know that roughtly 1 out of $\log n$ numbers up to n are primes. So it is much more efficient to take a bunch of random large numbers and test for primality.

The problem of discrete logarithm (for example, finding the smallest d such that $b^d \equiv 1 \pmod m$) is very slow on a classical computer but can be done in polynomial time on a quantum computer. A quantum computer can compute $b^n \bmod m$ for all non-negative integers $n < m$ at the same time, using the fact that a qubit can be 0 and 1 at the same time. In the above example, we can use 11 qubits to store $452^{2^k \cdot (0 \text{ or } 1)} \bmod 2023$ for $k = 0, \ldots, 10$. Then multiplying them together to find $452^n \bmod 2023$ at the same time for $n = 0, \ldots, 2047$. However, it will be a superposition of states $|n, b^n \bmod m\rangle$. Measuring the first registry gives a random n_0 and the value $b^{n_0} \bmod m$. Measuring the second registry gives a random c_0 and a superposition of states $|n\rangle$ such that $b^n \equiv c_0 \pmod m$.

The key is that there is a hidden period in this. In other words, the integers n such that $b^n \equiv c_0 \pmod m$ are of the form

$$n_1, n_1 + o_m(b), n_1 + 2o_m(b), \ldots$$

Quantum Fourier Transform can be used to find this hidden period.

For the rest of the semester, we will discuss:

1. Fermat, Miller-Rabin and Solovay-Strassen primality tests. These are polynomial time but probabilistic. However, similar to Shor's algorithm, the chance of them failing is lower than the chance of computation error.
2. AKS primality test. This is deterministic and in polynomial time.
3. Lucas-Lehmer primality test. This only works for Mersenne primes $2^p - 1$.
4. The Gaussian and cyclotomic integers $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta_3]$ and some history of Fermat's Last Theorem.

Lecture 30 Mon 11/18
Fermat primality test

11 Probabilistic primality test

In this section, we consider three probabilistic primality tests, the Fermat test, the Miller-Rabin test and the Solovay-Strassen test. They all build upon Fermat's little theorem: $a^{p-1} \equiv 1 \pmod p$ if p is a prime and $a = 1, \ldots, p-1$.

Lemma 11.1 *If $a^{n-1} \equiv 1 \pmod n$ for every $a = 1, \ldots, n-1$, then n is a prime.*

Proof: Every $a = 1, \ldots, n-1$ is invertible in $\mathbb{Z}/n\mathbb{Z}$. □

Similar to Shor's algorithm, it is not practical to test all integers less than n (we might as well just check for division in this case), so we use a probabilistic approach:

Fermat test

1. Pick $a = 1, \ldots, n-1$ at random.
2. Compute $\gcd(a, n)$. If it is bigger than 1, then n is not a prime.
3. Compute $a^{n-1} \bmod n$. If it is not 1, then n is not a prime. Otherwise, return to step 1.

Let's consider the set of bad inputs. Let

$$F_n = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^{n-1} = 1\}.$$

If a randomly chosen a lies in F_n, then we have to restart; otherwise, we would conclude that n is not a prime. How big is F_n?

Lemma 11.2 *The set F_n is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof: Clearly $1 \in F_n$. If $a, b \in F_n$, then $(ab)^{n-1} = a^{n-1}b^{n-1} = 1$ and $(a^{-1})^{n-1} = (a^{n-1})^{-1} = 1$. Note that by HW 10 P1(a), since $(\mathbb{Z}/n\mathbb{Z})^\times$ is finite, we don't need to check for a^{-1}. □

By Corollary 10.3, since the order of a subgroup divides the order of the group, we see that if $F_n \neq (\mathbb{Z}/n\mathbb{Z})^\times$, then $|F_n| \leq \frac{1}{2}\phi(n)$ and we have a probability of at least $1/2$ that a randomly chosen a can be used to prove that n is not a prime. Unfortunately, there exists (infinitely many) odd composite numbers n where $F_n = (\mathbb{Z}/n\mathbb{Z})^\times$. These numbers are called **Carmichael** numbers. The smallest Carmichael number is $561 = 3 \cdot 11 \cdot 17$. Note that

$$2 \mid 560, \qquad 10 \mid 560, \qquad 16 \mid 560.$$

Hence if a is an integer not divisible by $3, 11, 17$, then

$$\begin{aligned} a^2 \equiv 1 \pmod 3 &\implies a^{560} \equiv 1 \pmod 3 \\ a^{10} \equiv 1 \pmod{11} &\implies a^{560} \equiv 1 \pmod{11} \\ a^{16} \equiv 1 \pmod{17} &\implies a^{560} \equiv 1 \pmod{17} \end{aligned}$$

As another example, we have $1105 = 5 \cdot 13 \cdot 17$ and similarly $4 \mid 1104$, $12 \mid 1104$, $16 \mid 1104$. If we attempt to run the Fermat test on a Carmichael number, then we are just hoping to hit integers a that share a prime factor with n. If n is a product of very few large primes, we are in trouble. Carmichael numbers are all squarefree and so have at least 2 distinct prime divisors. In HW11, you will show that they have at least 3 distinct prime divisors.

Proposition 11.3 *If $p^2 \mid n$ for some prime $p \geq 3$, then n is not a Carmichael number.*

Proof: The key observation is that

$$(1+p)^{n-1} = 1 + (n-1)p + \sum_{r=2}^{n-1} \binom{n-1}{r} p^r \equiv 1 + (n-1)p \pmod{p^2}.$$

Since $p \mid n$, we have $p \nmid n-1$ and so $(1+p)^{n-1} \not\equiv 1 \pmod{p^2}$. Write $n = p^k m$ where $k = \nu_p(n) \geq 2$. By the Chinese Remainder Theorem, we can find an integer a coprime to n such that

$$\begin{cases} a \equiv 1 + p \pmod{p^k}, \\ a \equiv 1 \pmod{m}. \end{cases}$$

Then $a^{n-1} \equiv (1+p)^{n-1} \not\equiv 1 \pmod{p^2}$. Hence $a^{n-1} \not\equiv 1 \pmod{n}$. □

To deal with the Carmichael numbers, we can use the Solovay-Strassen test. Recall that we "proved" by example in the tutorial on Jacobi symbols that if n is a squarefree compositive odd integer, then the congruence equation

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod n$$

does not hold for all $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. The idea is that if p is a prime divisor of n, then $a^{(n-1)/2} \bmod p$ depends only on $a \bmod p$, but $\left(\frac{a}{n}\right)$ depends also on $a \bmod \frac{n}{p}$. It is easy to check that

$$J_n = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod n\}$$

is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ since both sides of the congruence equation are multiplicative in a. It is now a proper subgroup and so has size at most $\phi(n)/2$. So by randomly choosing 80 possible a's, we will be able to tell with high confidence whether n is prime or not.

Solovay-Strassen test

1. Pick $a = 1, \ldots, n-1$ at random.
2. Compute $\gcd(a, n)$. If it is bigger than 1, then n is not a prime.
3. Compute $a^{(n-1)/2} \bmod n$. Compute the Jacobi symbol $\left(\frac{a}{n}\right)$. If they are not equal, then n is not a prime. If they are equal mod n, return to step 1.

Lecture 31 Wed 11/20

Miller-Rabin test

When computing $a^{(n-1)/2} \bmod n$ in the Solovay-Strassen test, we find that a lot of times, it is not even ± 1. For example,

$$3^{280} \equiv 441 \pmod{561}.$$

However, $3^{560} \equiv 1 \pmod{561}$. This means that 441 is a nontrivial solution to $x^2 \equiv 1 \pmod{561}$, which also implies that 561 is not a prime. If we run this with 2, we actually have

$$2^{280} \equiv 1 \pmod{561}.$$

Is there some other power of 2 that we can try? We can try 2^{140} and see if that's ± 1 mod 561. As luck would have it, $2^{140} \equiv 67 \pmod{561}$. So now we have found another nontrivial solution, namely 67. If we run with 256, then we have

$$256^{280} \equiv 256^{140} \equiv 256^{70} \equiv 256^{35} \equiv 1 \pmod{561}.$$

Now there is no way to produce some nontrivial solution to $x^2 \equiv 1 \pmod{561}$ starting with 256. This is where we would "return to step 1". The above is exact the Miller-Rabin test:

Miller-Rabin test

Write $n - 1 = u \cdot 2^k$ where u is odd and $k = \nu_2(n-1)$.

1. Pick $a = 1, \ldots, n-1$ at random.
2. Compute $\gcd(a, n)$. If it is bigger than 1, then n is not a prime.
3. Compute $b_0 \equiv a^u \bmod n$. If $b_0 \equiv 1 \bmod n$, return to step 1.
4. Repeatedly compute $b_{i+1} \equiv b_i^2 \bmod n$. If $-1 \bmod n$ is reached before $1 \bmod n$, return to step 1. If $1 \bmod n$ is reached before $-1 \bmod n$, then n is not prime because we have a nontrivial solution to $x^2 \equiv 1 \pmod{n}$. If none of $b_0, \ldots, b_{k-1}$ equals $-1 \bmod n$, then n is not a prime. This last point follows because if $b_k \equiv 1$, then b_{k-1} is a nontrivial solution; and if $b_k \not\equiv 1$, then it fails the Fermat test.

We now consider the bad set for the Miller-Rabin test. Let

$$M_n = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^u = 1 \text{ or } a^{u2^i} = -1 \text{ for some } i = 0, \ldots, k-1\}.$$

There are a few ways to prove that $|M_n| \le \phi(n)/2$ when n has at least two distinct prime divisors. We prove that the bad set for the Miller-Rabin test is the same as the bad set for Shor's algorithm. Recall from HW 10 P3 the bad set for the Shor's algorithm:

$$S(n) = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : o(a) \text{ is odd or } a^{o(a)/2} = -1\}.$$

Lemma 11.4 *For any Carmichael number n, we have $M_n = S(n)$.*

Proof: With the notation $\mathbb{Z}/n\mathbb{Z}$, we will write $=$ instead of $\equiv \bmod n$. Let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ and we write $o(a) = v \cdot 2^t$ with v odd. Since n is Carmichael, we have $a^{n-1} = 1$ and so $o(a) \mid n-1$. Hence $u = vw$ for some positive odd integer w and $t \le k$. The condition $o(a)$ is odd is then equivalent to $o(a) \mid u$ which is equivalent to $a^u = 1$.

Suppose now $o(a)$ is even (i.e. $t \ge 1$). Suppose first that $a \in S(n)$. Then $a^{v2^{t-1}} = -1$. Since w is odd and $u = vw$, we can raise this to the power w to get $a^{u2^{t-1}} = (-1)^w = -1$ and so $a \in M_n$. Suppose now conversely that $a \in M_n$. Then $a^{u2^i} = -1$ for some $i = 0, 1, \ldots, k-1$. Since $a^{u2^i} = (a^{v2^i})^w$, we see that $a^{v2^i} \neq 1$ and so $i < t$. Note that

$$(a^{v2^i})^w = -1 \qquad \text{and} \qquad (a^{v2^i})^{2^{t-i}} = 1.$$

Since w is odd and is coprime to 2^{t-i}, there exist integers x, y such that

$$wx + 2^{t-i}y = 1.$$

Since $2^{t-i}y$ is even, we see that wx is odd and so x is odd. Now

$$a^{v2^i} = (a^{v2^i})^{wx}(a^{v2^i})^{2^{t-i}y} = (-1)^x \cdot 1^y = -1.$$

This implies that $a^{v2^{i+1}} = 1$. In other words, $o(a) = v2^{i+1}$ and $a^{o(a)/2} = -1$. So $a \in S(n)$. □

In HW 10 P3 bonus, you will find the size of $S(2023^{69} \cdot 2025^{420})$. You will essentially be giving a "proof" by example for the following formula.

Proposition 11.5 *Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be an integer where $p_1, \ldots, p_r$ are distinct odd primes and where $r \ge 2$ and $k_i \ge 1$. For $i = 1, \ldots, r$, write $p_i - 1 = m_i \cdot 2^{e_i}$ where m_i is odd. Let $e = \min\{e_1, \ldots, e_r\}$. Then*

$$|S(n)| = \frac{\phi(n)}{2^{e_1+\cdots+e_r}}\left(\frac{2^{re}-1}{2^r-1}+1\right) \le \frac{\phi(n)}{2^{r-1}}.$$

For example, for $n = 561 = 3 \cdot 11 \cdot 17$, we have $e_1 = 1$, $e_2 = 1$, $e_3 = 4$ and $e = 1$. Then

$$|S(561)| = \frac{2 \cdot 10 \cdot 16}{2^{1+1+4}}(1+1) = 10.$$

Note that when n is squarefree (for example when n is Carmichael), then

$$\frac{\phi(n)}{2^{e_1+\cdots+e_r}} = m_1 \cdots m_r = \text{odd part of } \phi(n).$$

For the inequality, we note that $e_1 + \cdots + e_r \ge re \ge r$. So

$$\frac{1}{2^{e_1+\cdots+e_r}}\left(\frac{2^{re}-1}{2^r-1}+1\right) \le \frac{1-2^{-r}}{2^r-1} + \frac{1}{2^r} = \frac{1}{2^{r-1}}.$$

When n is Carmichael, we have $r \ge 3$, so the Miller-Rabin test would fail with probability at most 25% each iteration.

We end by mentioning that testing for prime powers is very easy. Note also that by Proposition 11.3, prime powers are not Carmichael numbers so the Fermat test can also be applied. If $n = a^k$ for some $a, k \ge 2$, then $k \le \log_2 n$. For each $k \le \log_2 n$, we can do a binary search to see if $n = a^k$ for some integer a.

Binary search for testing for prime powers

1. Set $a_L = 2$ and $a_H = n - 1$. So any possible solution will lie in $[a_L, a_H)$.
2. If $a_H \le a_L + 1$, return True if $a_L^k = n$ and False if $a_L^k \neq n$.
   Else, let $c = \lfloor (a_L + a_H)/2 \rfloor$.
3. If $c^k = n$, then return True. If $c^k > n$, then c is too big and we replace a_H by c. If $c^k < n$, then c is too small and we replace a_L by c. Go back to step 2.

Exercises

11.1 Let $n > 1$ be an integer. Let $a \in \mathbb{N}$ and let p be a prime number such that:

- $a^{n-1} \equiv 1 \pmod{n}$;
- $p \mid n-1$ and $p > \sqrt{n} - 1$;
- $\gcd(a^{(n-1)/p} - 1, n) = 1$.

Prove that n is a prime.

This result can be used to recursively generate candidates for primes with deterministic proofs: given a large prime p, consider $n = 2pq + 1$ where q is some large random natural number less than $p/2$.

Lecture 32 Fri 11/22
AKS

12 Deterministic primality test

The Agrawal-Kayal-Saxena primality test is a deterministic primality test whose run time is polynomial in $\log n$.

For any commutative ring R and any $a, b, m_1, \ldots, m_r \in R$, we write

$$a \equiv b \pmod{m_1, \ldots, m_r} \qquad \Longleftrightarrow \qquad a - b \in (m_1, \ldots, m_r).$$

Recall that when $n = p$ is a prime, we have for any $a \in \mathbb{Z}$, the following congruence in $\mathbb{Z}[x]$,

$$(x + a)^p \equiv x^p + a^p \equiv x^p + a \pmod{p}.$$

Lemma 12.1 *Let $n \geq 2$ be an integer such that for some $a \in \mathbb{Z}$ coprime to n,*

$$(x + a)^n \equiv x^n + a \pmod{n}.$$

Then n is a prime.

Proof: Suppose for a contradiction that n is not a prime. Let $p < n$ be a prime divisor of n. Let k be a positive integer such that $p^k \leq n < p^{k+1}$. By Lemma 3.13, we have $p^k \binom{n}{p^k} \mid L_n$ where $L_n = \operatorname{lcm}(1, 2, \ldots, n)$ but $\nu_p(L_n) = k$. So we have $p \nmid \binom{n}{p^k}$. Since a is coprime to n, we have $p \nmid \binom{n}{p^k} a^{n-p^k}$. This gives a nonzero middle term if $p^k < n$. If $p^k = n$, then again from $p\binom{n}{p} \mid L_n$, we get $\nu_p(\binom{n}{p}) \leq k - 1 < \nu_p(n)$ and so $n \nmid \binom{n}{p} a^{n-p}$. □

The key idea of the AKS test is to check the congruence

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, n}$$

for a suitably chosen $r \leq (\log_2 n)^5$ and for positive integers $a \leq \sqrt{\phi(r)} \log_2 n \leq (\log_2 n)^{3.5}$. We can use the usual square and multiply method to compute $(x+a)^n \bmod (x^r - 1, n)$ in polynomial time for each a. Hence the full algorithm is in polynomial time. In what follows, we write $\log n$ for $\log_2 n$.

Lemma 12.2 *For $n \geq 4$, there exists a positive integer $r \leq (\log n)^5$ such that either $\gcd(r, n) > 1$ or $o_r(n) > (\log n)^2$.*

Proof: Suppose for a contradiction that for all positve integer $r \leq (\log n)^5$, we have $\gcd(r, n) = 1$ and $r \mid n^d - 1$ for some $d \leq (\log n)^2$. Let $m = \lfloor (\log n)^5 \rfloor$. Then $L_m = \operatorname{lcm}(1, 2, \ldots, m)$ divides

$$\prod_{1 \leq d \leq (\log n)^2} (n^d - 1) \leq n^{\sum_{1 \leq d \leq (\log n)^2} d} = n^{\frac{1}{2}\lfloor (\log n)^2 \rfloor (\lfloor (\log n)^2 \rfloor + 1)} = 2^{(\log n)(\frac{1}{2}\lfloor (\log n)^2 \rfloor (\lfloor (\log n)^2 \rfloor + 1))}.$$

Recall from HW 2 that $L_m \geq 2^m$ for any integer $m \geq 7$. From $n \geq 4$, we have $m \geq 32$, so from L_m dividing the above product, we have

$$m \leq (\log n)(\frac{1}{2}\lfloor(\log n)^2\rfloor(\lfloor(\log n)^2\rfloor + 1)).$$

Note the RHS grows like $\frac{1}{2}(\log n)^5$. Hence we have a contradiction by taking m roughly $(\log n)^5$. It is easy to check that $(\log n)^5$ works. □

Remark: The precise bound for r is not important. For theoretical purposes, any bound that is polynomial in $\log n$ is enough. In practice, one just tests r one-by-one to find one in polynomial time.

Step 1 of AKS: Find the smallest positive integer r such that $\gcd(r, n) > 1$ or $o_r(n) > (\log n)^2$.

We know we only need to test at most $(\log n)^5$ different r. For each r, we simply compute $r, r^2, r^3, \ldots r^{\lfloor(\log n)^2\rfloor} \bmod n$ to see if any of them is 1. Hence this step can be done in polynomial time. If $n < (\log n)^5$ is small (only happens when $n < 10^7$) so that this step does not terminate before $r \geq n$, then we have checked that $\gcd(r, n) = 1$ for all $r < n$ and so n is prime. If this step terminates at an r with $\gcd(r, n) > 1$, then n is composite. Suppose now we have found a positive integer $r \leq (\log n)^5$ coprime with n with $o_r(n) > (\log n)^2$. Note this also implies that $\phi(r) \geq o_r(n) > (\log n)^2$. Since $n \not\equiv 1 \pmod r$, we see that n has a prime divisor $p \not\equiv 1 \pmod r$ so that $o_r(p) > 1$.

Step 2 of AKS: For every positive integer $a \leq r$, check if $\gcd(a, n) = 1$.

Suppose Step 2 is passed. Then that means we may assume $p > r$. So we have

$$\sqrt{\phi(r)}\log n < \phi(r) < r < p.$$

Step 3 of AKS: For every positive integer $a \leq \sqrt{\phi(r)}\log n$, check the congruence

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, n}.$$

Theorem 12.3 *Suppose positive integers n, r and prime p satisfy:*

- $o_r(n) > (\log n)^2$
- $p \mid n$, $p > r$ *and* $o_r(p) > 1$
- *For all positive integers $a < \sqrt{\phi(r)}\log n$, the congruence $(x + a)^n \equiv x^n + a \pmod{x^r - 1, p}$.*

Then n is a power of p.

Note that we don't know what p is! So when running the test, we have to check mod n, not mod p.

Step 0 of AKS: Check if n is a perfect power.

Lecture 32.5 Fri 11/22
Tutorial
Sketch of the proof of AKS

It remains now to prove Theorem 12.3. We may assume that $n \geq 4$. The congruence

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, p}$$

translates to: for every $f(x) \in S := \{x, x + 1, \ldots, x + \ell\} \subseteq \mathbb{F}_p[x]$,

$$f(x)^n - f(x^n) = j(x)(x^r - 1)$$

for some $j(x) \in \mathbb{F}_p[x]$. To test whether $x^r - 1$ divides a polynomial in $\mathbb{F}_p[x]$, we consider r-th roots of unities in $\mathbb{F}_{p^d}$ where $d = o_r(p) > 1$. Let $\alpha_0 \in \mathbb{F}_{p^d}$ with $o(\alpha_0) = r$ and let

$$\mu_r = \langle\alpha_0\rangle = \{\alpha_0^k \colon k \in \mathbb{Z}/r\mathbb{Z}\}$$

be the subgroup of all r-th roots of unities. Then we have

$$x^r - 1 = \prod_{\alpha \in \mu_r} (x - \alpha).$$

Hence, in order for $x^r - 1$ to divide $f(x)^n - f(x^n)$, it is equivalence for every $\alpha \in \mu_r$ to be a root. In other words, we have for every $f(x) \in S$,

$$f(\alpha)^n = f(\alpha^n), \text{ for every } \alpha \in \mu_r.$$

Note since $\ell < p$, the set S contains $\ell + 1$ distinct linear polynomials.

We say a polynomial $g(x) \in \mathbb{F}_p[x]$ *commutes* with a positive integer m if

$$g(\alpha)^m = g(\alpha^m) \in \mathbb{F}_{p^d}, \text{ for every } \alpha \in \mu_r.$$

Hence, every element in S commutes with n. We have the following lemma about commuting polynomials and integers.

Lemma 12.4 *We have:*

(a) Any $g \in \mathbb{F}_p[x]$ commutes with p and 1.

(b) If $g_1, g_2 \in \mathbb{F}_p[x]$ both commute with m, then $g_1 g_2$ commutes with m

(c) If $g \in \mathbb{F}_p[x]$ commutes with m_1 and m_2, then g commutes with $m_1 m_2$.

(d) If $g \in \mathbb{F}_p[x]$ commutes with m and $p \mid m$, then g commutes with $\frac{m}{p}$.

Proof: (a) follows from the equality $g(x)^1 = g(x^1)$ and $g(x)^p = g(x^p)$ of polynomials in $\mathbb{F}_p[x]$. To see the latter, we have

$$g(x)^p = (a_n x^n + \cdots + a_0)^p = a_n^p x^{np} + \cdots + a_0^p = a_n x^{np} + \cdots + a_0 = g(x^p)$$

since each $a_i \in \mathbb{F}_p$. For (b), take any $\alpha \in \mu_r$. Then

$$((g_1 g_2)(\alpha))^m = g_1(\alpha)^m g_2(\alpha)^m = g_1(\alpha^m) g_2(\alpha^m) = (g_1 g_2)(\alpha^m).$$

For (c), we have

$$g(\alpha)^{m_1 m_2} = (g(\alpha^{m_1}))^{m_2} = g(\alpha^{m_1 m_2})$$

since $\alpha^{m_1} \in \mu_r$. For (d), we have

$$\big(g(\alpha)^{m/p}\big)^p = g(\alpha)^m = g(\alpha^m) = g(\alpha^{m/p})^p.$$

Hence $(g(\alpha)^{m/p} - g(\alpha^{m/p}))^p = 0$ and so $g(\alpha)^{m/p} = g(\alpha^{m/p})$. □

Let $\bar{S}$ denote the set of polynomials in $\mathbb{F}_p[x]$ that are products of elements in S. So

$$\bar{S} = \{x^{n_0}(x+1)^{n_1} \cdots (x+\ell)^{n_\ell} : n_0, \ldots, n_\ell \geq 0\}.$$

Then every element in $\bar{S}$ commutes with every positive integer of the form $(n/p)^i p^j$. Note that even though there are infinitely many m of the form $(n/p)^i p^j$, α_0^m only takes at most r possible values. In other words, the set

$$T = \{\alpha_0^{(n/p)^i p^j} : i, j \geq 0\} \subseteq \mu_r$$

is finite. Let $m_1 > m_2$ be two integers of the form $(n/p)^i p^j$ such that $\alpha_0^{m_1} = \alpha_0^{m_2}$. Note that this condition is equivalent to $m_1 \equiv m_2 \pmod{r}$.

Suppose for a contradiction that n is not a power of p. Then the integers $(n/p)^i p^j$ are all distinct for distinct pairs (i, j). This allows us to choose m_1 and m_2 so that $m_1 - m_2$ is fairly small. Let $N = |T|$. For

$i, j = 0, 1, \ldots, \lfloor\sqrt{N}\rfloor$, we have $(\lfloor\sqrt{N}\rfloor + 1)^2 > N$ distinct integers of the form $(n/p)^i p^j$. There are only N possible elements of the form $\alpha_0^{(n/p)^i p^j}$. Hence, by the Pigeonhole principle, there exist two distinct integers $m_1 > m_2$ among them such that $\alpha_0^{m_1} = \alpha_0^{m_2}$. Moreover,

$$m_1 - m_2 < m_1 \leq (n/p)^{\lfloor\sqrt{N}\rfloor} p^{\lfloor\sqrt{N}\rfloor} = n^{\lfloor\sqrt{N}\rfloor}.$$

Now for any $g \in \bar{S}$, we have

$$g(\alpha_0)^{m_1} = g(\alpha_0^{m_1}) = g(\alpha_0^{m_2}) = g(\alpha_0)^{m_2}.$$

Since $g \in \bar{S}$ splits completely in $\mathbb{F}_p$ and $\alpha_0 \notin \mathbb{F}_p$ (this is where we use $o_r(p) > 1$), we have $g(\alpha_0) \neq 0$ and so

$$g(\alpha_0)^{m_1 - m_2} = 1.$$

The idea now is that by taking ℓ large enough, the set $\{g(\alpha_0) \colon g \in \bar{S}\}$ is too large.

Suppose $g, h \in \bar{S}$ with $g(\alpha_0) = h(\alpha_0)$. We know that for every integer m of the form $(n/p)^i p^j$, we have

$$g(\alpha_0^m) = g(\alpha_0)^m = h(\alpha_0)^m = h(\alpha_0^m).$$

In other words, every $\alpha \in T$ is a root of $g(x) - h(x)$. Hence if we further require that $\deg(g)$ and $\deg(h)$ are less than $N = |T|$, then $\deg(g - h) < N$ so $g - h$ must be 0 in order for every $\alpha \in T$ to be root. Let $C(\ell + 1, N - 1)$ be the number of elements in $\bar{S}$ of degree at most $N - 1$. Then we have

$$|\{g(\alpha_0) \colon g \in \bar{S}\}| \geq C(\ell + 1, N - 1).$$

Therefore, it remains to prove that

$$n^{\lfloor\sqrt{N}\rfloor} \leq C(\ell + 1, N - 1).$$

Let's estimate the sizes of the variables involved. By taking $i = j$, we see that $(n/p)^i p^j = n^i$. So we have

$$\{n^i \bmod r \colon i \geq 0\} \subseteq \{(n/p)^i p^j \bmod r \colon i, j \geq 0\} \subseteq (\mathbb{Z}/r\mathbb{Z})^\times.$$

In other words,

$$(\log n)^2 < o_r(n) \leq N \leq \phi(r).$$

Let $M = \lfloor\lfloor\sqrt{N}\rfloor \log n\rfloor$. Then

$$\begin{aligned} n^{\lfloor\sqrt{N}\rfloor} &= 2^{\lfloor\sqrt{N}\rfloor \log n} \leq 2^{M+1}, \\ \ell + 1 &= \lfloor\sqrt{\phi(r)} \log n\rfloor + 1 \geq \lfloor\sqrt{N} \log n\rfloor + 1 \geq M + 1, \\ N - 1 &> \sqrt{N} \log n - 1 \geq M - 1, \\ C(\ell + 1, N - 1) &\geq C(M + 1, M). \end{aligned}$$

Hence, it is enough to prove that

$$C(M + 1, M) \geq 2^{M+1}.$$

Since $x, x + 1, \ldots, x + M$ are all distinct linear polynomials in $\mathbb{F}_p[x]$, $C(M + 1, M)$ is the same as the number of monomials of the form $x_1^{a_1} \cdots x_{M+1}^{a_{M+1}}$ in $M + 1$ variables of degree $a_1 + \cdots + a_{M+1}$ at most M. By adding in one more variable x_0 and setting $a_0 = M - (a_1 + \cdots + a_{M+1})$, this is the same as the number of monomials of the form $x_0^{a_0} x_1^{a_1} \cdots x_{M+1}^{a_{M+1}}$ in $M + 2$ variables of degree exactly M.

Theorem 12.5 *The number of monomials of the form $x_1^{a_1} \cdots x_k^{a_k}$ in k variables of degree $d = a_1 + \cdots + a_k$ is $\binom{d+k-1}{k-1}$.*

In particular, we have

$$C(M + 1, M) = \binom{2M + 1}{M + 1} = \binom{2M + 1}{M} > \frac{4^M}{M + 1} \geq 2^{M+1}$$

when $2^M \geq 2(M+1)$, which is true for $M \geq 3$. Since $n \geq 4$, we have $\log n \geq 2$ and $M \geq 4$.

The standard proof of Theorem 12.5 is the stars and bars method. Imagining placing d stars and $k-1$ bars in $d+k-1$ slots. The number of ways to do this is $\binom{d+k-1}{k-1}$. The number of stars before the first bar is the exponent of x_1. The number of stars between the i-th bar and the $(i+1)$-st bar is the exponent of x_{i+1} for $i = 1, \ldots, k-2$. The number of stars after the last bar is the exponent of x_k.

Lecture 33 Mon 11/25
Lucas-Lehmer

A Mersenne number is a number of the form $M_n = 2^n - 1$ for some $n \in \mathbb{N}$. Note since $2^d - 1 \mid 2^n - 1$ whenever $d \mid n$, in order for $2^n - 1$ to be a prime, n itself must be a prime. For example,

$$M_3 = 7, \qquad M_5 = 31, \qquad M_7 = 127$$

are all primes. However, $M_{11} = 2047 = 23 \times 89$ and $M_{23} = 47 \times 178481$ are not primes. The Lucas-Lehmer test is a very efficient test specifically for Mersenne numbers. The current record for the largest proved prime number is

$$2^{82589933} - 1.$$

The fact that $23 \mid M_{11}$ and $47 \mid M_{23}$ are not coincidences. Let's prove $47 \mid 2^{23} - 1$ without wolfram alpha. This amounts to proving that $2^{23} \equiv 1 \pmod{47}$. Since 47 is a prime and $23 = (47-1)/2$. We know that

$$2^{23} \equiv \left(\frac{2}{47}\right) \pmod{47} \qquad \text{and} \qquad \left(\frac{2}{47}\right) = 1$$

since $47 \equiv 7 \pmod 8$. What's special about the prime $p = 23$ in this proof by example? In order for $23 = (47-1)/2$, we need $47 = 2p+1$. We also need it to be a prime in order for $2^{(47-1)/2}$ to be given by the Legendre symbol. Finally, we need $47 \equiv \pm 1 \pmod 8$ in order for the Legendre symbol to be 1. This corresponds to $p \equiv 3 \pmod 4$.

A Sophie Germain prime is a prime p such that $2p+1$ is also prime. The primes $p = 3, 11, 23$ are all Sophie Germain primes that are 3 mod 4, while 5 is a Sophie Germain prime that is 1 mod 4. The infinitude of Sophie Germain primes is an open conjecture. The heuristic count for the number of them less than x is about $1.32032\, x/(\ln x)^2$.

Proposition 12.6 *Suppose $p \equiv 3 \pmod 4$ is a Sophie Germain prime. Then $2p+1 \mid M_p$ and so M_p is not prime for $p > 3$.*

Proof: From $p \equiv 3 \pmod 4$, we get $2p+1 \equiv 7 \pmod 8$. Hence 2 is a quadratic residue mod $2p+1$. Let a be an integer such that $2 \equiv a^2 \pmod{2p+1}$. Then

$$2^p \equiv a^{2p} \equiv 1 \pmod{2p+1}$$

by Fermat's little theorem. Then $2p+1 \mid 2^p - 1$. □

In the Lucas-Lehmer test, we define the sequence

$$a_0 = 4, \qquad a_{n+1} = a_n^2 - 2 \text{ for } n \geq 0.$$

Theorem 12.7 *Let p be an odd prime. The Mersenne number $M_p = 2^p - 1$ is prime if and only if $a_{p-2} \equiv 0 \pmod{M_p}$.*

For example, we have

$$\begin{aligned} a_0 &= 4 \\ a_1 &= 14 \equiv 0 \pmod 7 \\ a_2 &= 194 \\ a_3 &= 37634 = 2 \times 31 \times 607 \equiv 0 \pmod{31} \end{aligned}$$

Note that the a_n grows very quickly. However, since we only care about mod M_p, we can reduce mod M_p at every step so we only have a p bit number to deal with before computing a_{n+1}. Moreover, it is very easy to find the remainder of an integer a mod a number of the form $2^p - 1$. We apply the division algorithm to divide a by 2^p first to find

$$\begin{aligned} a &= 2^p q + r \\ &\equiv q + r \pmod{2^p - 1}. \end{aligned}$$

Finding the quotient q and remainder r are extremely easy, since the numbers are already in binary. So q is the simply the number after removing the last p bits from a, and r is the last p bits of a. Applying the same method to q, we find that a mod $2^p - 1$ is simply the sum of all p-bits chucks of a.

Proof of Theorem 12.7: Consider $\omega = 2 + \sqrt{3}$. Then

$$\omega^{-1} = \frac{1}{2+\sqrt{3}} = 2 - \sqrt{3}.$$

So $\omega + \omega^{-1} = 4 = a_0$. Now

$$\begin{array}{rclcrclcl} a_1 &=& a_0^2 - 2 &=& \omega^2 + 2 + \omega^{-2} - 2 &=& \omega^2 + \omega^{-2} \\ a_2 &=& a_1^2 - 2 &=& \omega^4 + 2 + \omega^{-4} - 2 &=& \omega^4 + \omega^{-4} \end{array}$$

It is then easy to check via induction that

$$a_n = \omega^{2^n} + \omega^{-2^n} = \omega^{-2^n}(\omega^{2^{n+1}} + 1).$$

All of the above are done in $\mathbb{R}$, but we can restrict to the more interesting subring

$$R = \mathbb{Z}[\sqrt{3}] = \{j(\sqrt{3})\colon j(x) \in \mathbb{Z}[x]\} = \{a + b\sqrt{3}\colon a, b \in \mathbb{Z}\} \cong \mathbb{Z}[x]/(x^2 - 3).$$

Since both ω and ω^{-1} are in R, we see that $\omega \in R^\times$ is a unit. Consider

$$a_{p-2} = \omega^{-2^{p-2}}(\omega^{2^{p-1}} + 1) = (\text{unit}) \cdot (\omega^{2^{p-1}} + 1).$$

Let $q = M_p$. Then we have the ideal $qR = \{qa + qb\sqrt{3}\colon a, b \in \mathbb{Z}\}$. Hence we see that

$$a_{p-2} \in q\mathbb{Z} \iff a_{p-2} \in qR \iff \omega^{2^{p-1}} + 1 \in qR \iff \omega^{2^{p-1}} = -1 \text{ in } R/qR.$$

Suppose first that $a_{p-2} \in q\mathbb{Z}$ and suppose for a contradiction that q is not a prime. Let $r \le \sqrt{q}$ be a prime divisor of q. Then we also have $a_{p-2} \in r\mathbb{Z}$ and so $\omega^{2^{p-1}} = -1$ in R/rR. Then $\omega^{2^p} = 1$ in R/rR. The order $o(\omega)$ of ω in $(R/rR)^\times$ is then a divisor of 2^p that doesn't divide 2^{p-1}. Hence it equals 2^p, which then must divide $|(R/rR)^\times|$. However, we have a contradiction now because

$$2^p \le |(R/rR)^\times| \le |R/rR| - 1 = r^2 - 1 \le q - 1 = 2^p - 2.$$

Lecture 34 Wed 11/27

The idea of norms

Suppose conversely that q is a prime. Note that $2^{p-1} = (q+1)/2$. So we need to compute $\omega^{(q+1)/2}$ in the ring R/qR. We first prove the following formula: for any $a, b \in \mathbb{Z}$, we have

$$(a + b\sqrt{3})^{q+1} = a^2 - 3b^2 \qquad \text{in } R/qR.$$

Since R/qR is a ring of characteristic q, we know that

$$(a + b\sqrt{3})^q = a^q + b^q\sqrt{3}\sqrt{3}^{q-1} \qquad \text{in } R/qR.$$

Since $a, b \in \mathbb{Z}$, we know that $a^q \equiv a \pmod{q}$ and $b^q \equiv b \pmod{q}$. Moreover, mod q, we have

$$\sqrt{3}^{q-1} = 3^{(q-1)/2} = \left(\frac{3}{q}\right) = -\left(\frac{q}{3}\right) = -\left(\frac{-2}{3}\right) = -1.$$

Here we note that $q = 2^p - 1 \equiv 3 \pmod{4}$ and $q \equiv (-1)^p - 1 = -2 \pmod{3}$. Hence,

$$(a + b\sqrt{3})^q = a - b\sqrt{3} \qquad \text{in } R/qR$$

and so

$$(a + b\sqrt{3})^{q+1} = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2 \qquad \text{in } R/qR.$$

Next we note the fact that

$$(1 + \sqrt{3})^2 = 4 + 2\sqrt{3} = 2\omega.$$

Hence

$$\omega^{(q+1)/2} = \frac{(1 + \sqrt{3})^{q+1}}{2^{(q-1)/2} \cdot 2} = \frac{1^2 - 3 \cdot 1^2}{2} = \frac{-2}{2} = -1,$$

where since $q = 2^p - 1 \equiv 7 \pmod{8}$, we have $2^{(q-1)/2} \equiv \left(\frac{2}{q}\right) = 1 \pmod{q}$. □

We can understand the quotient R/qR better where $R \cong \mathbb{Z}[x]/(x^2 - 3)$. Suppose q is a prime. We use the third isomorphism theorem (recall the Tutorial on Oct 11) to get

$$R/qR \cong \mathbb{Z}[x]/(x^2 - 3, q) \cong \mathbb{F}_q[x]/(x^2 - 3).$$

From the Legendre symbol calculation above, we saw that 3 is not a square mod q and so $x^2 - 3$ is irreducible in $\mathbb{F}_q[x]$. Hence, we have

$$R/qR \cong \mathbb{F}_{q^2}.$$

One can prove that there are two field homomorphisms (automatically isomorphisms) $\mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$: the identity map id and the Frobenius map $\tau(x) = x^q$. Our calculation above gives

$$\tau(a + b\sqrt{3}) = a - b\sqrt{3}$$

and

$$a^2 - 3b^2 = \mathrm{id}(a + b\sqrt{3}) \cdot \tau(a + b\sqrt{3}) = N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a + b\sqrt{3}).$$

This is a special case of the norm map. We will use the norm map $N_{\mathbb{C}/\mathbb{R}}$ next to prove some interesting results about representing integers as sums of squares next.

Remark: IMO 2003 N7 asks that if q is an odd prime divisor of a_n, then $2^{n+3} \mid q^2 - 1$. We can give a very quick proof of this! The assumption $q \mid a_n$ implies as above that $\omega^{2^{n+1}} = -1$ in R/qR. Note first that $a_n \equiv -1 \pmod{3}$ for $n \geq 1$. So $q \neq 3$. If $3 = \alpha^2$ is a quadratic residue mod q, then

$$R/qR \cong \mathbb{F}_q[x]/(x^2 - \alpha^2) \cong \mathbb{F}_q \times \mathbb{F}_q.$$

The image of ω in either of the $\mathbb{F}_q$ factor is an element whose 2^{n+1} power is -1. Hence $2^{n+2} \mid q - 1$, which implies that $2^{n+3} \mid q^2 - 1$. Suppose now 3 is not a quadratic residue mod q. Then $R/qR \cong \mathbb{F}_{q^2}$. Recall that $(1 + \sqrt{3})^2 = 2\omega$ and there exists $\beta \in \mathbb{F}_{q^2}$ such that $\beta^2 = 2$. Hence $((1 + \sqrt{3})/\beta)^{2^{n+2}} = -1$ in $\mathbb{F}_{q^2}$, which implies that $2^{n+3} \mid q^2 - 1$.

13 The Gaussian and Eisenstein integers

In this section, we consider the ring $\mathbb{Z}[i]$ of Gaussian integers and the ring $\mathbb{Z}[\zeta_3]$ of Eisenstein integers. Note that $i = \zeta_4$ is a root of $\Phi_4(x) = x^2 + 1$ and ζ_3 is a root of $\Phi_3(x) = x^2 + x + 1$. Both of these polynomials are irreducible in $\mathbb{Q}[x]$ and monic in $\mathbb{Z}[x]$. Hence by HW 6 P4, we have

$$\begin{aligned} \mathbb{Z}[i] &= \{a + bi \colon a, b \in \mathbb{Z}\} \cong \mathbb{Z}[x]/(x^2 + 1), \\ \mathbb{Z}[\zeta_3] &= \{a + b\zeta_3 \colon a, b \in \mathbb{Z}\} \cong \mathbb{Z}[x]/(x^2 + x + 1). \end{aligned}$$

Note that ζ_6 is a root of $\Phi_6(x) = x^2 - x + 1$, so we have a similar description for $\mathbb{Z}[\zeta_6]$. However,

$$\zeta_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \qquad \text{and} \qquad \zeta_6 = \frac{1}{2} + \frac{\sqrt{3}}{2}i = \zeta_3 + 1.$$

So $\mathbb{Z}[\zeta_6] = \mathbb{Z}[\zeta_3]$. We define the norm of an element in $\mathbb{Z}[i]$ or $\mathbb{Z}[\zeta_3]$ by

$$N(\alpha) = \alpha\overline{\alpha} = |\alpha|^2.$$

More explicitly, we have

$$\begin{aligned} N(a+bi) &= a^2 + b^2, \\ N(a+b\zeta_3) &= N((a - \frac{b}{2}) + \frac{\sqrt{3}}{2}bi) = a^2 - ab + b^2. \end{aligned}$$

Note that the norm function is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$. So from

$$(a+bi)(c+di) = ac - bd + (ad + bc)i$$

we have the well-known formula

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2;$$

and from

$$(a+b\zeta_3)(c+d\zeta_3) = ac + (bc + ad)\zeta_3 + bd(-1 - \zeta_3) = ac - bd + (bc + ad - bd)\zeta_3$$

we have the less-known formula

$$(a^2 - ab + b^2)(c^2 - cd + d^2) = (ac - bd)^2 - (ac - bd)(bc + ad - bd) + (bc + ad - bd)^2.$$

If we use the above formula with $a, b, c, d \in \mathbb{Z}$, we see that the sets

$$\begin{aligned} S_4 &= \{a^2 + b^2 \colon a, b \in \mathbb{Z}\} \\ S_3 &= \{a^2 - ab + b^2 \colon a, b \in \mathbb{Z}\} \end{aligned}$$

are closed under multiplication. Hence to understand what they are, it remains to understand which prime powers do S_4 and S_3 contain. They clearly contain p^2 for every prime p by taking $a = p$ and $b = 0$. It is easy to check that

$$2 \in S_4 \qquad \text{and} \qquad 2 \notin S_3 \qquad \text{and} \qquad 3 \in S_3.$$

In HW 9 P1, you proved that if $p \in S_4$, then $p = 2$ or $p \equiv 1 \pmod 4$; and if $p \in S_3$, then $p = 3$ or $p \equiv 1 \pmod 3$. Our main theorem is that the converse is also true.

Theorem 13.1 *If p is a prime congruent to 1 mod 4, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.*

Theorem 13.2 *If p is a prime congruent to 1 mod 3, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 - ab + b^2$.*

For example, $2023 = 7 \cdot 17^2 \in S_3$ since $7 \equiv 1 \pmod 3$, but $2023 \notin S_4$ since $7 \not\equiv 1 \pmod 4$. More explicitly,

$$7 = 3^2 - 3 \cdot 1 + 1^2 \qquad \text{and} \qquad 2023 = 51^2 - 51 \cdot 17 + 17^2.$$

Lecture 35 Fri 11/29
The rings $\mathbb{Z}[\zeta_4]$ and $\mathbb{Z}[\zeta_3]$

We give a ring-theoretic proof of these results. There is also a "descent"-type proof. They look different but really are the same. Let $m = 3$ or 4. We will treat them with the same argument. The key ring theoretic result is the following.

Proposition 13.3 *The rings $\mathbb{Z}[\zeta_m]$ for $m = 3, 4$ are Euclidean domains with respect to the norm function. As a consequence, $\mathbb{Z}[\zeta_m]$ is a PID for $m = 3, 4$.*

Proof: Let $\alpha, \beta \in \mathbb{Z}[\zeta_m]$ where $m = 3$ or 4 and $\alpha \neq 0$. We are looking for some $q \in \mathbb{Z}[\zeta_m]$ such that $N(\beta - \alpha q) < N(\alpha)$. In other words, we want

$$N\Big(\frac{\beta}{\alpha} - q\Big) < 1.$$

We divide β by α in $\mathbb{C}$ to get

$$\frac{\beta}{\alpha} = \frac{\beta\overline{\alpha}}{\alpha\overline{\alpha}} = \frac{\beta\overline{\alpha}}{N(\alpha)}.$$

Next we note that since $\alpha \in \mathbb{Z}[\zeta_m]$, we also have $\overline{\alpha} \in \mathbb{Z}[\zeta_m]$:

$$\overline{a + b\zeta_m} = a + b\overline{\zeta_m} \qquad \text{and} \qquad \overline{i} = -i \qquad \text{and} \qquad \overline{\zeta_3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i = -1 - \zeta_3.$$

Since $\mathbb{Z}[\zeta_m]$ is a ring, we see that $\beta\overline{\alpha} \in \mathbb{Z}[\zeta_m]$. Since $N(\alpha) \in \mathbb{Z}$, we see that

$$\frac{\beta}{\alpha} = t + s\zeta_m, \qquad \text{for some } t, s \in \mathbb{Q}.$$

Let $a \in \mathbb{Z}$ be an integer that is the closest to t and let $b \in \mathbb{Z}$ be an integer that is the closest to s. (In other words, either the floor or ceiling of t and s.) Hence

$$\frac{\beta}{\alpha} = (a + b\zeta_m) + \big((t - a) + (s - b)\zeta_m\big), \qquad |t - a| \leq \frac{1}{2}, \qquad |s - b| \leq \frac{1}{2}.$$

Then

$$N\big((t - a) + (s - b)\zeta_m\big) \leq |t - a|^2 + |t - a||s - b| + |s - b|^2 \leq \frac{3}{4} < 1.$$

Therefore $q = a + b\zeta_m \in \mathbb{Z}[\zeta_m]$ does the job. □

Remark: When $t = 1/2$ for example, there are two choices for a. Hence the "quotient" and "remainder" are not unique in this division algorithm. The same argument also works for $\mathbb{Z}[\sqrt{2}i]$, $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$. There is a complete classification for which of the $\mathbb{Z}[\zeta_m]$ are Euclidean domains. It turns out that being a Euclidean domain (not necessarily with the norm function) and being a PID is equivalent for $\mathbb{Z}[\zeta_m]$ and it is the case for all $m \leq 40$ except for $m = 23, 29, 31, 37, 39$ and for $m = 44, 45, 48, 60, 84, (42, 50, 54, 66, 70)$. The numbers in paranthesis are of the form $2n$ where n is odd in which case $\mathbb{Z}[\zeta_m] = \mathbb{Z}[\zeta_n]$. For example for $m = 23$, one can prove that

$$(2) = (2, \frac{1 + \sqrt{-23}}{2})(2, \frac{1 - \sqrt{-23}}{2})$$

and that none of the factors are principal in $\mathbb{Z}[\zeta_{23}]$. You will prove in HW 11 P4 that

$$\frac{1 \pm \sqrt{-23}}{2} \in \mathbb{Z}[\zeta_{23}].$$

Proof of Theorems 13.1 and 13.2: Suppose p is a prime congruent to 1 mod m, where $m = 3$ or 4. Then $o_m(p) = 1$ and so $\Phi_m(x)$ splits completely in $\mathbb{F}_p[x]$. Let $n \in \mathbb{Z}$ such that $x - n \in \mathbb{F}_p[x]$ is a factor of $\Phi_m(x)$. Consider the ideal $I_p = (p, \zeta_m - n)$ in $\mathbb{Z}[\zeta_m]$. We apply the third isomorphism theorem to get

$$\mathbb{Z}[\zeta_m]/I_p \cong \mathbb{Z}[x]/(\Phi_m(x), p, x - n) \cong \mathbb{F}_p[x]/(\Phi_m(x), x - n) = \mathbb{F}_p[x]/(x - n) \cong \mathbb{F}_p.$$

As a consequence, we see that I_p is a proper ideal (in fact, a prime ideal). Since $\mathbb{Z}[\zeta_m]$ is a PID, there exists some $\alpha \in \mathbb{Z}[\zeta_m]$ such that $I_p = (\alpha)$. The fact that I_p is a proper ideal implies that α is not a unit. We prove now that $N(\alpha) = p$, so that upon writing $\alpha = a + b\zeta_m$ for $a, b \in \mathbb{Z}$, we have

$$p = a^2 + b^2 \text{ for } m = 4, \qquad \text{and} \qquad p = a^2 - ab + b^2 \text{ for } m = 3.$$

Note that the intrinsic reason for $N(\alpha) = p$ is that

$$p = |\mathbb{Z}[\zeta_m]/I_p| = |\mathbb{Z}[\zeta_m]/(\alpha)| = N(\alpha).$$

Since $p \in I_p = (\alpha)$. We write $p = \alpha\beta$ for some $\beta \in \mathbb{Z}[\zeta_m]$. Since $p \nmid \zeta_m - n$, we see that $I_p \neq (p)$ and so β is also not a unit. Taking norm on $p = \alpha\beta$ gives

$$p^2 = N(p) = N(\alpha)N(\beta).$$

Now for any $\gamma \in \mathbb{Z}[\zeta_m]$, we saw earlier that $\overline{\gamma} \in \mathbb{Z}[\zeta_m]$. Hence if $N(\gamma) = \gamma\overline{\gamma} = 1$, we see that γ is a unit. Since neither α nor β is a unit, we see that $N(\alpha) \neq 1$ and $N(\beta) \neq 1$, but they are positive integers that multiply to p^2. Therefore, they must both be p. □

The converse direction

$$\gamma \in \mathbb{Z}[\zeta_m]^\times \quad \Longrightarrow \quad N(\gamma) = 1$$

is also true. To see this, we note that $\gamma^{-1} \in \mathbb{Z}[\zeta_m]$ and so $N(\gamma)$ and $N(\gamma^{-1})$ are positive integers that multiply to $N(1) = 1$. So they are both 1. Using this characterization of units, we can solve for $a^2 + b^2 = 1$ and $a^2 - ab + b^2 = 1$ to find that

$$\begin{aligned} \mathbb{Z}[i]^\times &= \{1, -1, i, -i\} = \mu_4, \\ \mathbb{Z}[\zeta_3]^\times &= \{1, -1, \zeta_3, -\zeta_3, 1 + \zeta_3, -1 - \zeta_3\} = \mu_6. \end{aligned}$$

Lecture 35.5 Fri 11/29
Tutorial
The ring $\mathbb{Z}[\zeta_{23}]$

The year is 1847. Fermat's Last Theorem had been proved in degrees $3, 4, 5, 7$. The proofs involve a crude factorization of $x^n + y^n$. For example, when $n = 3$, this factors as $(x+y)(x^2-xy+y^2)$. It didn't seem plausible to generalize this to higher degrees. Then on March 1st, Lamé announced a "proof" for general prime degrees p by factoring $x^p + y^p$ completely into linear factors, but using complex numbers:

$$x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y)$$

from the factorization

$$x^p - 1 = \prod_{i=0}^{p-1} (x - \zeta_p^i).$$

If this product is a perfect p-th power z^p, then Lamé concluded that each of the factors $x + \zeta_p^i y$ must then be a p-th power, up to some common factor among the terms. Then some kind of descent argument similar to the known cases can be used to produce a smaller solution, leading eventually to a contradiction. After the presentation, Liouville immediately pointed out the possible lack of unique factorization in the ring $\mathbb{Z}[\zeta_p]$ of cyclotomic integers and he found the whole thing very sus. Lamé agreed but was still optimistic and worked on fixing it. Cauchy also was very enthusiastic and raced to resolve the issue with a series of papers the level of clarity of which is comparable to some of your homework solutions. On May 24, Liouville read a letter from Kummer who had already proved in 1844 that $\mathbb{Z}[\zeta_{23}]$ does not have unique factorization. Lamé felt silent. Cauchy tried some more before moving on to astronomy. Kummer was able to save the "proof" of Fermat's Last Theorem using his new theory of ideals (which he developed in order to prove higher reciprocity laws), but expressed doubts about the case $p = 37$.

For this tutorial and Monday's lecture, we will give Kummer's proof that $\mathbb{Z}[\zeta_{23}]$ doesn't have unique factorization. In what follows, we write $\zeta = \zeta_{23}$.

Theorem 13.4 *The prime number 47 has no prime factorization in $\mathbb{Z}[\zeta]$.*

Recall that $\mathbb{Z}[\zeta]$ consists of elements of form $f(\zeta)$ where $f(x) \in \mathbb{Z}[x]$ and ζ is a root of

$$\Phi_{23}(x) = x^{22} + x^{21} + \cdots + x + 1 = \frac{x^{23}-1}{x-1} = \prod_{j=1}^{22}(x - \zeta^j).$$

Kummer was interested in the factorizations of primes $q \equiv 1 \pmod{23}$ in $\mathbb{Z}[\zeta]$. Similar to the proof of Theorems 13.1 and 13.2, the cyclotomic polynomial $\Phi_{23}(x)$ splits completely in $\mathbb{F}_q[x]$ for these primes. So there is hope that q splits nicely in $\mathbb{Z}[\zeta]$. We define the norm

$$N(f(\zeta)) = \prod_{j=1}^{22} f(\zeta^j).$$

For example, for any integer a,

$$N(a - \zeta) = \prod_{j=1}^{22}(a - \zeta^j) = \Phi_{23}(a).$$

This gives another motivating reason for why primes $\equiv 1 \pmod{23}$ are interesting because they (and 23) are the only possible prime divisors of $\Phi_{23}(a)$.

Lemma 13.5 *For any $f(\zeta) \in \mathbb{Z}[\zeta]$, its norm $N(f(\zeta))$ is a non-negative integer of the form $a^2 - ab + 6b^2$ for some $a, b \in \mathbb{Z}$.*

Proof: We let $g(x) = f(x)f(x^2)\cdots f(x^{22}) \in \mathbb{Z}[x]$. Then $N(f(\zeta)) = g(\zeta)$. Note that for any $n = 1, \ldots, 22$, the elements $\zeta^n, \zeta^{2n}, \ldots, \zeta^{22n}$ are just a permuation of $\zeta, \zeta^2, \ldots, \zeta^{22}$. Hence, we have $g(\zeta) = g(\zeta^n)$. So by HW 11 P4(b), we have $g(\zeta) \in \mathbb{Z}$.

To prove its precise form, we need to use HW 11 P4(c). Recall the notations

$$\begin{aligned} S &= \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} = \langle 4 \rangle \subseteq (\mathbb{Z}/23\mathbb{Z})^\times, \\ T &= \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}. \end{aligned}$$

Then S consists of all the nonzero quadratic residues mod 23 and T consists of all the quadratic non-residues mod 23. Let

$$\theta_1 = \sum_{j\in S} \zeta^j = \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^6 + \zeta^8 + \zeta^9 + \zeta^{12} + \zeta^{13} + \zeta^{16} + \zeta^{18} = \frac{-1 + \sqrt{-23}}{2},$$

$$\theta_2 = \sum_{k\in T} \zeta^k = \zeta^5 + \zeta^7 + \zeta^{10} + \zeta^{11} + \zeta^{14} + \zeta^{15} + \zeta^{17} + \zeta^{19} + \zeta^{20} + \zeta^{21} + \zeta^{22} = \frac{-1 - \sqrt{-23}}{2}.$$

We define

$$G(x) = \prod_{n\in S} f(x^n) = f(x)f(x^2)f(x^3)f(x^4)f(x^6)f(x^8)\cdots f(x^{18}).$$

Since -1 is quadratic non-residue, we see that $n \in S$ if and only if $23 - n \in T$. Moreover since $|\zeta| = 1$, we have

$$\overline{\zeta^n} = \zeta^{-n} = \zeta^{23-n}.$$

This explains why θ_2 is the complex conjugate of θ_1. Moreover,

$$\overline{G(\zeta)} = \prod_{n\in S} f(\zeta^{23-n}) = \prod_{m\in T} f(\zeta^m).$$

Therefore, we have

$$N(f(\zeta)) = G(\zeta)\overline{G(\zeta)}.$$

Since S is a subgroup of $(\mathbb{Z}/23\mathbb{Z})^\times$, we see that for any $n \in S$, the set $\{na\colon a \in S\}$ is just a permutation of S. Hence $G(\zeta) = G(\zeta^n)$ for any $n \in S$. By HW 11 P4(c), we have $G(\zeta) = a + b\theta_1$ for some $a, b \in \mathbb{Z}$. Now

$$G(\zeta)\overline{G(\zeta)} = |(a - \frac{b}{2}) + \frac{\sqrt{23}}{2}bi|^2 = a^2 - ab + 6b^2,$$

as desired. □

Lecture 36 Mon 12/04

$\mathbb{Z}[\zeta_{23}]$ is not a UFD

We prove that 47 does not have a "prime factorization" in $\mathbb{Z}[\zeta_{23}]$.

Corollary 13.6 *There does not exist $\alpha \in \mathbb{Z}[\zeta]$ such that $N(\alpha) = 47$.*

Proof: Suppose $47 = (a - b/2)^2 + (23/4)b^2$ for some integers a, b. Then $|b| = 0, 1, 2$ in order for $(23/4)b^2 \le 47$. However, none of 47, $47 - 23/4 = 165/4$ and $47 - 23 = 24$ are squares of rational numbers. □

Corollary 13.7 *If $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta]$ such that $\alpha = \beta\gamma$, then $N(\alpha) = N(\beta)N(\gamma)$. In particular*

$$\beta \mid \alpha \text{ in } \mathbb{Z}[\zeta] \quad \Longrightarrow \quad N(\beta) \mid N(\alpha) \text{ in } \mathbb{Z}.$$

Now, we have

$$N(4 - \zeta) = \prod_{j=1}^{22}(4 - \zeta^j) = \Phi_{23}(4) = \frac{4^{23} - 1}{4 - 1} = 47 \cdot 178481 \cdot 2796203.$$

The other two prime factors are not important. The important factor is 47, which we know exists because $4^{23} = 2^{46} \equiv 1 \pmod{47}$, and that its $\nu_{47} = 1$ which we can fix by taking $51 - \zeta$ if needed (similar to the proof that $(\mathbb{Z}/p^t\mathbb{Z})^\times$ is cyclic). Suppose now $\mathfrak{p}$ is a prime divisor of 47 in $\mathbb{Z}[\zeta_{23}]$. Then from

$$\mathfrak{p} \mid \prod_{j=1}^{22}(4 - \zeta^j), \qquad \text{we have} \qquad \mathfrak{p} \mid 4 - \zeta^j \text{ for some } j.$$

Then we have

$$N(\mathfrak{p}) \mid N(4 - \zeta^j) = N(4 - \zeta) = 47 \cdot 178481 \cdot 2796203.$$

On the other hand, since $\mathfrak{p} \mid 47$, we have

$$N(\mathfrak{p}) \mid N(47) = 47^{22}.$$

Comparing these, we find that $N(\mathfrak{p}) = 47$, but we proved in Corollary 13.6 that no elements of $\mathbb{Z}[\zeta]$ have norm 47. Therefore, we have proved that 47 doesn't even have a prime divisor, and so it certainly has no prime factorization!

Kummer went a bit deeper than this. He calculated

$$N(1 - \zeta + \zeta^{21}) = 47 \cdot 139.$$

Then from the lack of an element with norm 47, we see that $1 - \zeta + \zeta^{21}$ cannot be factored as a product of two non-units. Elements like this are called irreducible. However, $1 - \zeta + \zeta^{21}$ is not prime because

$$1 - \zeta + \zeta^{21} \mid 47 \cdot 139, \qquad \text{but} \qquad 1 - \zeta + \zeta^{21} \nmid 47 \qquad \text{and} \qquad 1 - \zeta + \zeta^{21} \nmid 139.$$

The two non-divisions follow because the $N(1 - \zeta + \zeta^{21})$ does not divide 47^{22} or 139^{22}.

Kummer resolved this issue of unique factorization using his "ideal numbers". It is worth mentioning that Kummer did not define what the ideal numbers are, but only what it means for them to divide a number or another ideal number. The abstract definition of an ideal was given by Dedekind some 30 years later. Since $\Phi_{23}(x)$ splits completely in $\mathbb{F}_{47}[x]$:

$$\Phi_{23}(x) = (x-2)(x-3)(x-4)(x-6)\cdots(x-36)(x-37)(x-42).$$

There is a very beautiful factorization of the ideal (47):

$$(47) = (47, \zeta - 2)(47, \zeta - 3)(47, \zeta - 4)\cdots(47, \zeta - 36)(47, \zeta - 37)(47, \zeta - 42)$$

and every factor in the right hand side is a prime ideal of $\mathbb{Z}[\zeta]$. Kummer considered the factorization in the cyclotomic integers $\mathbb{Z}[\zeta_p]$ and Dedekind proved in the more general setting of rings of integers of number fields that every ideal can be factored uniquely into a product of prime ideals. It then follows that the failure of unique factorization can be attributed to some prime ideals being non-principal.

One is then lead to the notion of the class number h_p of $\mathbb{Z}[\zeta_p]$, which counts the number of equivalence classes of ideals of $\mathbb{Z}[\zeta_p]$ where two ideals $I \sim J$ if $I \cdot (\alpha) = J \cdot (\beta)$ for some nonzero $\alpha, \beta \in \mathbb{Z}[\zeta_p]$. This set of equivalence class of ideals actually forms a finite abelian group, called the class group. If the ring $\mathbb{Z}[\zeta_p]$ is a PID, then every ideal is principal and so $h_p = 1$. The prime $p = 23$ is the first time $h_p \neq 1$. In fact, $h_{23} = 3$. Kummer proved Fermat's Last Theorem for primes p such that

$$p \nmid h_p.$$

These are called regular primes. There are only three irregular primes less than 100, namely 37, 59, 67:

$$h_{37} = 37, \qquad h_{59} = 3 \cdot 59 \cdot 233, \qquad h_{67} = 67 \cdot 12739.$$

So Kummer was feeling sus about $p = 37$ for a very good reason! It is still open whether there are infinitely many regular primes. It is known that there are infinitely many irregular primes. It is conjectured (by Siegel) that the density of regular primes is $e^{-1/2}$.

We now fast forward to 1954 when Taniyama, and later with the help with Shimura, conjectured that all elliptic curves are modular. This roughly predicts that if $a^p + b^p = c^p$ is an integer solution, then the number of $\mathbb{F}_q$-points on the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ (equivalently, the number of solutions in $\mathbb{F}_q$) as the prime q varies should have some very nice patterns. Ribet proved in 1990 that they actually don't. (Frey introduced this curve and Serre made conjectures which Ribet proved.) It then remains to prove the Taniyama-Shimura conjecture for elliptic curves of this form. Wiles announced a proof of the Taniyama-Shimura conjecture for semistable elliptic curves in 1993. A gap was found and fixed soon by Wiles and Taylor in 1995. The full Taniyama-Shimura conjecture was proved in 2001. We now believe that everything is modular!

So did Fermat have a truly ingenius proof? We may never know. What's more impressive is the amount of mathematics that were developed by the countless mathematicians who worked on it over the last 3 centuries!