Math 124 - Number Theory

Taught by Cliff Taubes
Notes by Dongryul Kim

Fall 2018

¡+instructor+¿ ¡+meetingtimes+¿ ¡+textbook+¿ ¡+enrolled+¿ ¡+grading+¿ ¡+courseassistants+¿

Contents

1 September 5, 2018

There will be two textbooks for the course: *The Higher Arithmetic* by H. Davenport, and *Elementary Number Theory—primes, congruences, and secrets* by W. Stein written in a more modern perspective. There are going to be weekly reading and assignments. The homework is there to make sure you learn number theory, so if you are stuck, email me or the course assistant. You are welcome to collaborate with other students. To hand in your homework late, you need to get my permission. There will be no exams in this course, but instead, there will be midterm and final writing assignments. You will write a lecture on a topic that I did not go over in class.

1.1 Overview

We are going to denote

$$\begin{aligned}
\mathbb{N} &= \{\text{natural numbers}\} = \{1, 2, 3, 4, \dots\}, \\
\mathbb{Z} &= \{\text{integers}\} = \{\dots, -2, -1, 0, 1, 2, \dots\}, \\
\mathbb{Q} &= \{\text{rational numbers}\} = \{\tfrac{p}{q} : p, q \text{ integers with } q \neq 0\}, \\
\mathbb{R} &= \{\text{real numbers}\}, \\
\mathbb{C} &= \{\text{complex numbers}\}.
\end{aligned}$$

Number theory deals with $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$. But what the big deal with $1, 2, 3, \dots$? There are even animals that can count, and one article says that even the Venus fly trap can count.

The integers carry a structure of addition, and also a structure of multiplication. If we look at these structures, some interesting thins happen. Not every number is divisible by 7, and not every number is divisible by 10. But every integer can be written as

$$7x + 10y$$

where x, y are integers. For instance, $15 = 7 \times 5 + 10 \times (-2)$. On the other hand, not every integer can be written as

$$6x + 10y.$$

This is not hard to see, because $6x + 10y$ is always an even number.

So given positive integers n, m, what numbers can be written as $nx + my$? That is, what is the set

$$\{nx + my : x, y \in \mathbb{Z}\}?$$

There is another curious pattern here. If a is an integer not divisible by 3, then $a^2 - 1$ is divisible by 3. For instance, $10^2 - 1 = 99$ and $11^2 - 1 = 120$. This is kind of cool, but why is this? Here is something better. If a is an integer not divisible by 5, then $a^4 - 1$ is divisible by 5. This is called Fermat's little theorem. So is it true that for any positive integer n, is the following true?

> If a is not divisible by n, then $a^{n-1} - 1$ is divisible by n.

This turns out to be false. When $n = 4$ and $a = 2$, we have $a^{n-1} = 2^3 - 1 = 7$ not divisible by $n = 4$. But if we modify the statement a little bit and put $a^{\varphi(n)}$ instead of a^{n-1}, we get a true statement. So there are all these patterns coming from playing with numbers.

Here is another curious pattern. Consider $x^2 + 1$ where x is an integer.

Theorem 1.1. *No number of the form $x^2 + 1$ is divisible by a number of the form $4k + 3$ where $k \geq 0$.*

You can check this all day. Pick any integer $x^2 + 1$ and try dividing it by 7 or 11.

There are also interesting questions about rational numbers. Recall that a rational number is a number of the form p/q where p and q are integers with $q \neq 0$. But are all numbers rational? If you have a square tile of side length 1, the length of a side is $\sqrt{2}$ by Pythagorean's theorem. We can prove that $\sqrt{2}$ is not rational, by proof by contradiction. Suppose that $\sqrt{2}$ is rational, so that we can write

$$\frac{p}{q} = \sqrt{2}.$$

Here we can assume that p and q are not both even, because then we can cancel out the 2 in both p and q. We square both sides and get

$$\frac{p^2}{q^2} = 2, \quad p^2 = 2q^2.$$

But then p has to be an even integer, because p^2 is an even number. So we can write $p = 2k$. Then

$$4k^2 = 2q^2, \quad 2k^2 = q^2.$$

By the same reason, q also has to be an even number, and this contradicts our assumption that p and q are not both even.

Number theory is also used in codes and cyphers.

Definition 1.2. A **prime number** is a positive number not divisible by any smaller number except 1. By convention, 1 is not a prime number.

So the list of prime numbers is $2, 3, 5, 7, 11, 13, 17, 19, \ldots$. RSA encryption is is based on prime numbers. For two big prime numbers p and q, you look at $N = pq$ and make the number N public, but keep p and q hidden. The RSA encryption system is designed so that if you know the number N, you can encrypt any message, but to decrypt it, you need to know the prime numbers p and q. Factoring an integer into primes is a computationally difficult job, so the message is secure.

There is also interesting number theory in geometry. An elliptic curve is the set of solutions of

$$y^2 = x^3 + ax + b$$

in the (x, y)-plane. There is a way of defining addition on elliptic curves, and this satisfies commutativity and associativity.

If there is time, we are also going to talk about how many primes there are.

1.2 Addition and multiplication of integers

Let us look at the set integers $\mathbb{Z}$. There is addition on the set of integer, and they satisfy commutativity and associativity:

$$x + y = y + x, \quad x + (y + z) = (x + y) + z, \quad x + 0 = x, \quad x + (-x) = 0.$$

There is also multiplication, which is just addition. They also satisfy some rules:

$$xy = yx, \quad x(yz) = (xy)z, \quad 1x = x.$$

Then there is a rule about distribution:

$$x(y + z) = xy + xz.$$

Let's assume we all know these rules and not be too pedantic.

There are also cancellation laws:

If $x + y = x + z$ then $y = z$.

You can say that this follows from negative numbers, but in a sense, this law is why we can define negative numbers. There is also cancellation law for multiplication:

If $xy = xz$ and $x \neq 0$, then $y = z$.

1.3 Divisibility and primes

Definition 1.3. We say that a **divides** b if $b = ma$ for some integer a.

If a divides b, then $|a| \leq b$ unless $b = 0$.

Proposition 1.4. *If a divides b and b divides c, then a divides c.*

Proof. If $b = ma$ and $c = nb$ then $c = (mn)a$. □

Proposition 1.5. *If b and c are divisible by a, then $xb + yc$ is also divisible by a.*

Proof. Write $b = ma$ and $c = na$. Then

$$xb + yc = xma + yna = (xm + yn)a. \qquad \square$$

We defined a **prime number** as a number only divisible by n and 1. We say that n is **composite** if n is neither a prime or 1. So every positive integer n falls in exactly one of the following categories:

- primes,
- composites,
- 1.

Prime numbers are important because they form sort of an irreducible basis for multiplication of integers.

Theorem 1.6 (fundamental theorem of arithmetic)**.** *Every number can be written as a product of primes which is unique up to order.*

The factors that appear in the factorization of a are called the **prime factors** of a. The existence part is not hard to prove. Take any natural number n. If $n = 1$ or n is a prime, there is nothing to do. Otherwise, n is composite and we can write

$$n = m \cdot q, \quad 1 < m, q < n.$$

If m and q are both primes, we are done. Otherwise, we factor them further as

$$n = m_1 \cdot m_1 \cdot q \text{ or } n = m \cdot q_1 \cdot q_2.$$

This process should end at a point, so we get a factorization of n into prime numbers.

This has a nice consequence.

Proposition 1.7. *There are infinitely many primes.*

Proof. Again we do proof by contradiction. Suppose there are N prime, and let them be $n_1, \dots, n_N$. Then consider

$$\ell = n_1 n_2 \cdots n_N + 1.$$

This is a number, but it is not divisible by any of $n_1, \dots, n_N$. This contradicts the existence part of the fundamental theorem of arithmetic. □

2 September 10, 2018

We were talking last time about the fundamental theorem of arithmetic.

Theorem 2.1 (fundamental theorem of arithmetic)**.** *Every positive integer n can be written as a product of primes*

$$n = p_1 p_2 \cdots p_k,$$

where p_i are all primes. Moreover, this is unique up to ordering.

By convention, 1 is neither prime or composite, and it is the product of zero primes. If n is prime, we are done. If n is composite, we can write $n = qr$, and then we reduce the problem to smaller cases. So this proves existence of a prime factorization. Uniqueness is harder, and Davenport has a clever proof that is not too enlightening.

2.1 Davenport's proof of the fundamental theorem of arithmetic

Suppose we have

$$n = pq \cdots t = p'q' \cdots t'.$$

Here, write this so that p is the smallest prime in $pq \cdots t$ and p' is the smallest prime in $p'q' \cdots t'$.

Assume that n the smallest case when n has two different representations into products of primes. Then p does not appear in $p'q' \cdots t'$, because otherwise we can cancel out p on both sides and get two different representations of n/p. Similarly, p' does not appear in $pq \cdots t$. Because p is the smallest prime,

$$n = pq \cdots t \geq p \cdot p,$$

and hence $p \leq \sqrt{n}$. Likewise, $p' \leq \sqrt{n}$ and so

$$pp' < \sqrt{n} \cdot \sqrt{n} = n.$$

(Here, we have strict inequality because it cannot be that $p = p' = \sqrt{n}$.)

Let us now consider

$$0 < m = n - pp' = p(q \cdots t - p') = p'(q' \cdots t' - p).$$

Because we assumed that n was the smallest positive integer with non-unique representation, and m is smaller than n, there is a unique prime factorization of m. Therefore p and p' both appear in this representation. So we can write

$$m = n - pp' = pp's \cdots uv.$$

Now

$$n = pp'(1 + s \cdots uv) = pq \cdots t$$

and we can cancel both sides and get

$$\tfrac{n}{p} = q \cdots t = p'(1 + s \cdots uv).$$

But n/p is smaller than n, and so there should be a unique representation. But p' does not appear in $q \cdots t$ but does appear in $p'(1 + s \cdots uv)$. This is a contradiction.

2.2 Greatest common divisor

This was a clever proof, but it doesn't really tell us much. We are now going to develop a new technology that can take us further than that.

Definition 2.2. The **greatest common divisor** $\gcd(a, b)$ of two integers a and b is the largest integer that divides both a and b. (Davenport calls it the highest common factor, but I have never heard it called by that name.)

So for instance,

$$\gcd(12, 15) = 3, \quad \gcd(12, 66) = 6, \gcd(8, 20) = 4.$$

You can compute the greatest common divisor by listing all divisors on both sides, and finding numbers that match. Let p be a prime number. The only divisors of p are 1 and p. So its greatest common divisor with any number is

$$\gcd(p, n) = \begin{cases} 1 & \text{if } p \text{ does not divide } n, \\ p & \text{if } p \text{ divides } n. \end{cases}$$

Definition 2.3. We say that two integers a and b are **relatively prime** if $\gcd(a, b) = 1$.

The greatest common divisor is an important concept, and we will establish some properties.

Lemma 2.4. $\gcd(a, b) = \gcd(b, a) = \gcd(a, -b) = \gcd(-a, -b) = \gcd(-a, b)$.

Proof. This follows from the fact that the list of divisors of n is the same as the list of divisors of $-n$. □

Lemma 2.5. $\gcd(a, b) = \gcd(a, a + b) = \gcd(a, b - a)$.

Proof. If m divides both a and b, then we can write $a = ml$ and $b = mk$. Then $b - a = m(l - k)$, and so m divides $b - a$. That is, m divides a and $b - a$. Conversely, if m' divides both a and $b - a$, then we can write $b - a = m'q$ and $a = m'l$ and $b = m'(l + q)$. That is, m' divides both a and b. This shows that the list of common divisors of a and b is equal to the list of common divisors of a and $b - a$. So when we take the greatest one, we get $\gcd(a, b) = \gcd(a, b - a)$. □

Lemma 2.6. $\gcd(a, b) = \gcd(a, b - na)$ *for any* n.

Proof. We can apply the previous lemma iteratively and get $\gcd(a, b) = \gcd(a, b-a) = \gcd(a, b - 2a) = \cdots$. □

You can find the greatest common divisor by using the Euclidean algorithm. Suppose I have integers a, b as $0 < b < a$. Then there are unique integers q and r such that

$$a = qb + r, \quad 0 \le r < b.$$

So using the lemma above, we get that if $a = qb + r$, then

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

Example 2.7. Take $a = 18$ and $b = 14$. Then

$$\gcd(18, 14) = \gcd(14, 4).$$

They are both equal to 2.

So we have a algorithm here, called the **Euclidean algorithm**. Given $0 < b < a$, we write

$$a = q_1 b + r_1, \quad 0 \le r_1 < b = 0, \quad \gcd(a, b) = \gcd(b, r_1).$$

Then we can do this for r_1 and b, and write

$$b = q_2 r_1 + r_2, \quad 0 \le r_2 < r_1, \quad \gcd(b, r_1) = \gcd(r_1, r_2).$$

Then

$$r_1 = q_3 r_2 + r_3, \quad 0 \le r_3 < r_2, \quad \gcd(r_1, r_2) = \gcd(r_2, r_3),$$

and so on. These r_i decreases, so at some point, we will have $r_n = 0$. Then

$$\gcd(a, b) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_{n-1}, 0) = r_{n-1}.$$

Example 2.8. We have

$$\begin{aligned} 79 &= 66 + 13 \\ 66 &= 5 \times 13 + 1 \\ 13 &= 13 \times 1 + 0. \end{aligned}$$

So $\gcd(79, 66) = 1$.

Lemma 2.9. *Suppose a, b, n are positive integers. Then*

$$\gcd(na, nb) = n \gcd(a, b).$$

Proof. We know that $n \gcd(a, b)$ divides na and nb, because $\gcd(a, b)$ divides both a and b. So

$$\gcd(na, nb) \ge n \gcd(a, b).$$

But it's not obvious how to show the other direction.

So we use the Euclidean algorithm on both sides. If we know the process of the Euclidean algorithm for a and b, we can multiply the entire thing by n and get

$$\begin{aligned} na &= q_1(nb) + nr_1, \quad 0 \leq nr_1 < nb, \\ nb &= q_2(nr_1) + nr_2, \quad 0 \leq nr_2 < nr_1, \\ nr_1 &= \cdots . \end{aligned}$$

This means that $\gcd(na, nb) = nr_{k-1} = n \gcd(a, b)$. □

Lemma 2.10. *Suppose n divides a and b. Then n divides $\gcd(a, b)$ as well.*

Proof. Consider the Euclidean algorithm

$$a = qb + r_1, \quad b = q_1 r_1 + r_2, \quad \dots .$$

If n divides a and b, it divides $r_1 = a - qb$. If n divides r_1 and b, it divides $r_2 = b - q_1 r_1$. You repeat this process until you see that n divides $r_{k-1} = \gcd(a, b)$. □

Theorem 2.11 (Euclid's theorem)**.** *If p is a prime, and if p divides ab, then p divides either a or b.*

Proof. If p divides a, then we are done. So assume that p doesn't divide a so that $\gcd(a, p) = 1$. Then

$$\gcd(ab, pb) = b.$$

Now p divides both ab and pb, so p divides their greatest common divisor, which is b. □

Of course, if we know the fundamental theorem of arithmetic, we can write out and see this. But we are trying to prove the fundamental theorem of arithmetic.

Altenrative proof of the fundamental theorem of arithmetic. Let us write

$$n = pqr \cdots , \quad n = p'q'r' \cdots .$$

By assumption, p divides $n = p'(q'r' \cdots)$, and so p divides either p' or $(q'r' \cdots)$. If p divides p', then $p = p'$, otherwise we can write $q'r' \cdot = q'(r' \cdots)$ and do the same thing over and over. So p appears in $p'q'r' \cdots$ and then we can cancel them out. □

2.3 Linear combinations

Suppose we are given integers a and b. We are interested in what integers we can get by taking integer linear combinations of a and b, i.e., for which m does

$$ax + by = m$$

have a solution $x, y \in \{\dots, -2, -1, 0, 1, 2\}$.

The first thing we observe is that anything that divides both a and b also has to divide m. So we should be able to write

$$m = \gcd(a, b)z, \quad z \in \{\dots, -2, -1, 0, 1, 2\}.$$

But can you get all the multiples of $\gcd(a, b)$?

Proposition 2.12 (Bezout)**.** *The set of linear combinations of two integers is*

$$\{ax + by\}_{x,y \in \{\dots,-1,0,1,\dots\}} = \{k \gcd(a, b)\}_{k \in \{\dots,-1,0,1,\dots\}}.$$

For example, every integer can be written as $3x + 17y$, like $21 = 3 \times (-10) + 17 \times 3$. For now, let us postpone proving this theorem and use it to prove the fundamental theorem of arithmetic.

Another alternative proof of the fundamental theorem of arithmetic. Suppose we have

$$n = pq \cdots r = p'q' \cdots r'.$$

If $p = p'$, we can divide by p and continue. If $p \neq p'$, we can write

$$px + p'y = 1,$$

and so multiplying both sides by $q' \cdots r'$ gives

$$p(xp'q' \cdots r') + p(yq \cdots r) = q' \cdots r'.$$

So p divides $q' \cdots r'$ and we can continue this process. □

We now need to prove this linear algebra proposition.

Proof of Bezout's theorem. Given a and b, then we want find x and y such that $ax + by = \gcd(a, b)$. Then we can write any multiple of $\gcd(a, b)$ as

$$a(kx) + b(ky)k = \gcd(a, b).$$

Write $a' = a/\gcd(a, b)$ and $b' = b/\gcd(a, b)$. Then $\gcd(a', b') = 1$ and it is enough to find x and y such that

$$a'x + b'y = 1.$$

Let m be the smallest positive integer such that we can write

$$a'x + b'y = m.$$

We will finish this next time. □

3 September 12, 2018

We introduced the notion of a greatest common divisor. This is

$$\gcd(a, b) = \text{greatest integer that divides both } a \text{ and } b.$$

Then we proved some interesting things about the greatest common divisor:

- $\gcd(a, b) = \gcd(b, a) = \gcd(\pm a, \pm b)$
- $\gcd(a, b) = \gcd(a, b - na)$
- $\gcd(na, nb) = |n| \gcd(a, b)$
- If n divides a and b, then n divides $\gcd(a, b)$

We also proved that if p is prime and it divides ab, then it divides either a or b.

We were looking at the linear combinations of two integers,

$$\{ax + by\}_{x,y \in \mathbb{Z}},$$

which is the set of k such that $ax + by = k$ has an integer solution.

Proposition 3.1 (Bezout)**.** *The equation $ax + by = k$ can be solved if and only if k is divisible by $\gcd(a, b)$.*

This implies, for instance, that if a and b are relatively prime (i.e., $\gcd(a, b) = 1$) then you can find integers x, y such that $ax + by = 1$. Before we prove this, let me ask a sloppy mathematical question. If you take two integers at random, what is the probability that they are relatively prime? The statement is that the probability is

$$\frac{6}{\pi^2} \approx 0.608.$$

More precisely, you are choosing two integers at random in $\{1, 2, \dots, n\}$, and take n to ∞. Let me give you a heuristic that shows that this somewhat makes sense. The odds of two numbers not being both divisible by 2 is

$$1 - \frac{1}{2^2}.$$

Then the odds of them being not simultaneously divisible by 3 is

$$1 - \frac{1}{3^2}.$$

Then we go on with all primes,

$$\Big(1 - \frac{1}{4}\Big)\Big(1 - \frac{1}{9}\Big)\Big(1 - \frac{1}{25}\Big) \cdots = \prod_p \Big(1 - \frac{1}{p^2}\Big).$$

So the number gets smaller and smaller, but maybe it converges to some one number. Cleverly, Euler realized that this converges to $6/\pi^2$. We might get to these cool statements near the end of the course.

Let us now prove what we wanted to prove.

Proof. We only need to show that $ax + by = k$ can be solved if k is divisible by $\gcd(a, b)$. If we let

$$a' = \frac{a}{\gcd(a,b)}, \quad b' = \frac{b}{\gcd(a,b)},$$

we have $\gcd(a', b') = 1$. So it is enough to show that

$$a'x + b'y = 1$$

has a solution.

Here is how you can prove this, although it doesn't give you the solution. Consider the set

$$\{a'x + b'y\}_{x,y\in\mathbb{Z}}$$

and look at the smallest positive number m that can be written as $a'x+b'y = m$. Suppose that m is not 1. Then m cannot divide both a' and b', because a' and b' are relatively prime. Assume without loss of generality that m does not divide a'. We have $m < a'$, because otherwise $a'(x-1) + b'y = m - a'$ is a smaller positive integer than m. Now write

$$a' = mq + r, \quad 0 < r < m.$$

(We have $0 < r$ because m does not divide a'.) Then we get

$$a' = (a'x + b'y)q + r, \quad a'(1 - qx) + b'(-qy) = r.$$

This contradicts the fact that m is the minimal positive integer, because $r < m$. The only way out of this contradictory loop is when $m = 1$. □

3.1 Finding primes

There is something called the **prime sieve** that lets you to list primes. Suppose we want to compute all primes less than n. There is how you do this.

1. [Initialize] We know that 2 is a prime number. We set

$$X = \{3, 5, 7, \dots \leq n\}, \quad P = \{2\}.$$

   X is the set where we search for primes, and P is the set of primes that we found.

2. Let p be the smallest element remaining in X. If $p > \sqrt{n}$, add all of X to P and terminate the program. If $p \leq \sqrt{n}$, add p to P.
3. From X, remove all elements divisible by p.
4. Go to Step 2.

When we pick p in Step 2, it has to be a prime, because in Step 3 we always throw away all the things divisible by smaller primes. So p in Step 2 cannot be divisible by any smaller prime, which means that it is a prime. But why do we terminate the program when $p > \sqrt{n}$? The reason is this. Let the set X be

$$X = \{p, q, r, \ldots \leq n\}$$

where $p > \sqrt{n}$. Then r cannot be divisible by anything smaller than p. It could be that $r = ab$, but then $ab = r \leq n$ so either $a \leq \sqrt{n} < p$ or $b \leq \sqrt{n} < p$. This means that r has to be eliminated before X reached this state. So r cannot be composite, so it has to be a prime.

There is another famous theorem of Dirichlet.

Theorem 3.2 (Dirichlet)**.** *There are infinitely many primes of the form $ax + b$ (for fixed a and b), if a and b are relatively prime.*

This really requires a lot of technology. But here is one case we can prove. Almost all primes are odd, and they are either of the form $4x - 1$ or $4x + 1$.

Theorem 3.3. *There are infinitely many primes of the form $4x - 1$.*

For instance, $3, 7, 11, 19, 23, 31, \ldots$.

Proof. Let $p_1, p_2, \ldots, p_n$ be primes of the form $4x_n - 1$. Now look at

$$K = 4p_1p_2 \cdots p_n - 1.$$

If this is prime, then it is bigger than any of $p_1, \ldots, p_n$, so we get a new prime. But may be it is composite, and has prime factorization

$$K = (4x_1 + 1)(4x_2 + 1) \cdots (4x_t + 1).$$

This cannot happen, because if you expand the right side, it takes the form of $4X + 1$. So this means that there is a prime of the form $4x_{n+1} - 1$ dividing K, and it cannot be any of $p_1, \ldots, p_n$ because p_i and K are relatively prime. That is, given any n primes we can find a new prime. □

The prime number theorem tells us how rare or common primes are. If we define

$$\pi(x) = \#\text{prime numbers less than or equal to } x,$$

then the theorem states the following asymptotic behavior.

Theorem 3.4 (prime number theorem)**.** *We have*

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

So primes are not too rare, and also not to common.

3.2 Groups and rings

There is applied number theory. There is something called a perfect shuffle of playing cards. When you have 52 cards, you split it into exactly 26 and 26 cards, and you place exactly one between another. This seems like a perfectly randomized shuffle, but the theorem is that if you do the perfect shuffle eight times, you get back to the original position.

We don't have the technology right now, so let me introduce the notion of a group.

Definition 3.5. A **group** is a (finite) set G, with a distinguished element $1 \in G$ and a binary operation

$$G \times G \to G, \quad (a, b) \mapsto ab,$$

such that

- $(ab)c = a(bc)$ for all $a, b, c \in G$,
- $1a = a1 = a$ for all $a \in G$,
- for any $a \in G$ there is b so that $ab = 1$ and $ba = 1$.

Here is an example that might be confusing. If you take $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$ with addition $+$, we have

$$a + 0 = 0 + a = a, \quad a + (-a) = 0, \quad a + (b + c) = (a + b) + c.$$

So this is a group. Here is another example. We can look at the group of pemutations the deck of cards. You can compose permutations, and this is multiplication we use. Every permutation has an inverse, so it becomes a group. This is a bit scary if you think about it. If you do a shuffle, and then do the inverse shuffle, you get the original deck so you can cheat.

Definition 3.6. We say that a group G is an **abelian group** if $ab = ba$ for all $a, b \in G$.

There are groups that are not abelian. Permutation groups are generally not abelian. For instance, take the permutation group on three elements a, b, c. You can actually check this.

Definition 3.7. A **commutative ring** is a set R with two distinguished elements $0, 1 \in R$ with two binary operations

$$+, \cdot : R \times R \to R$$

such that

- $+$ with the identity 0 makes it an abelian group,
- $1 \cdot a = a \cdot 1 = a$ for all $a \in R$,
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$,

- $a \cdot b = b \cdot a$ for all $a, b \in R$,
- $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.

But there are no multiplicative inverses.

So let me give you the simplest possible nontrivial ring. This is $R = \{0, 1\}$, and addition and multiplication are defined as

$$0 + 1 = 1, \quad 0 + 0 = 0, \quad 1 + 1 = 0,$$

and

$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

This is called $\mathbb{Z}/2\mathbb{Z}$, and 1 sort of represents “odd numbers” while 0 represents “even numbers”.

4 September 17, 2018

Last time we introduced the concept of a group. This is a set G with a rule $G \times G \to G$ satisfying

$$a(bc) = (ab)c, \quad 1a = a1 = a,$$

and for every $a \in G$ there exists a b such that $ab = ba = 1$. A group is also called abelian if $ab = ba$. There are groups that are not abelian, for instance, the group of invertible 2×2 real matrices. But in this class, we are mostly look at abelian groups.

Example 4.1. Consider the positive rationals $\mathbb{Q}_{>0} = \{\frac{a}{b} : a, b \text{ positive integers}\}$. This is a group under multiplication, with inverse of $\frac{a}{b}$ being $\frac{b}{a}$. The integers $\mathbb{Z}$ also forms a group under addition, with inverse of a being $-a$.

We also got to the notion of rings. This is a set R with two binary operations $+$ and $\times$. We require that $(R, +, 0)$ is an abelian group, so that we have things like $a + (-a) = 0$. But multiplication is not going to be a group. We are going to require that

$$a \times (b \times c) = (a \times b) \times c, \quad 1 \times a = a \times 1 = a, \quad a \times (b + c) = a \times b + a \times c.$$

Multiplication need not be commutative, but we can further require that multiplication is commutative, in which case the ring is called a commutative ring. The point is that there need not be inverses for multiplication.

Example 4.2. $\mathbb{Z}$ is a commutative ring. We have addition like $3 + (-5) = -2$ and multiplication like $2 \times (-4) = -8$. This satisfies all the condition we listed above.

4.1 The congruence ring $\mathbb{Z}/n\mathbb{Z}$

The definition of a ring won't be very interesting if there is only one ring on earth. Fix a positive integer n. We are going to construct rings $\mathbb{Z}/n\mathbb{Z}$, also called the **congruence modulo n ring**.

Definition 4.3. If a and b are integers such that $a - b$ is divisible by n, then we say that a is **congruent** modulo n and write $a \equiv b \pmod{n}$.

We then define

$$\mathbb{Z}/n\mathbb{Z} = \{\text{equivalence class of integer congruent modulo } n\}.$$

So for $n = 3$, there are three classes

$$[0] = \{\dots, -3, 0, 3, 6, \dots\}, \quad [1] = \{\dots, -5, -2, 1, 4, \dots\}, \quad [2] = \{\dots, -4, -1, 2, 5, \dots\}.$$

In general, $\mathbb{Z}/n\mathbb{Z}$ has n congruence classes,

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \dots, [n-1]\}.$$

We actually do this everyday. The hours are like $\mathbb{Z}/12\mathbb{Z}$. We are only trying to formalize this.

Proposition 4.4. *The set $\mathbb{Z}/n\mathbb{Z}$ with $(+, [0])$ and $(\times, [1])$ forms a ring.*

Let us now analyze the perfect shuffle. We have 26 cards on each side, and if we do the out-shuffle, we get

$$\begin{gathered} 1, 2, 3, 4, \dots, 26, 27, 28, 29, \dots, 52 \\ \downarrow \\ 27, 1, 28, 2, 29, 3, \dots, 51, 25, 52, 26. \end{gathered}$$

So the mth card becomes the $2m$th card, modulo 53 if we suppose that there is a Joker at the end of the deck. So the perfect out-shuffle is just

$$m \mapsto 2m \pmod{53}.$$

If we pick the representatives $\{0, 1, \dots, n-1\}$ of $\mathbb{Z}/n\mathbb{Z}$, then addition is

$$a + b = \begin{cases} a + b & \text{if } a + b \leq n - 1, \\ a + b - n & \text{if } a + b \geq n. \end{cases}$$

We can also define multiplication as doing ordinary multiplication and looking at the remainder when divided by n,

$$a \cdot b = q \cdot n + r, \quad r \in \{0, \dots, n-1\}.$$

Then in $\mathbb{Z}/n\mathbb{Z}$, we have $a \cdot b = r$. The remainder of the product only depends on the remainders of each number, because

$$(a + xn)(b + yn) = ab + n(xb + ya + nxy).$$

Let us do some practice. We can try to compute the multiplication table in $\mathbb{Z}/5\mathbb{Z}$, and the result is in Table 1. Note that in this case, every nonzero element has a multiplicative inverse. If a ring satisfies this property, we call it a **field**. I don't know the etymology of this word. If it is a ring with a nice property, why not call it a bracelet?

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table 1: Multiplication table for $\mathbb{Z}/5\mathbb{Z}$

It is not true that all $\mathbb{Z}/n\mathbb{Z}$ are fields. Let us take $n = 8$ for instance. Then we get Table 2. Here, some numbers like 1, 3, 5, 7 have inverses, but some numbers like 2, 4, 6 don't. So we need to figure out which have inverses and which don't.

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Table 2: Multiplication table for $\mathbb{Z}/8\mathbb{Z}$

Let me do another example. We did the out shuffle, but let's now do the in-shuffle. In this case, it is convenient to renumber the cards to $0, 1, \ldots, 51$ instead of $1, 2, \ldots, 52$. Then the shuffle looks like

$$\begin{gathered} 0, 1, 2, \ldots, 25, 26, \ldots, 51 \\ \downarrow \\ 0, 26, 1, 27, 2, 28, \ldots, 25, 51. \end{gathered}$$

Here, we see that the first and last card never changes, and the rule is that the mth card becomes the $2m$th card modulo 51. That is, the in shuffle is

$$m \mapsto 2m \pmod{51}.$$

Now we can prove that the deck comes back to itself after 8 shuffles. If we iterate the in-shuffle k times, we get

$$m \mapsto 2m \mapsto 4m \mapsto \cdots \mapsto 2^k m \pmod{51}.$$

Here, we note that

$$2^8 = 256 = 5 \times 51 + 1 \equiv 1 \pmod{51}.$$

So if we shuffle it 8 times, the shuffle is $m \mapsto m \pmod{51}$.

If we did this for the out-shuffle, we needed to find when

$$2^k \equiv 1 \pmod{53}.$$

The smallest k happens to be 52. We have

$$2^{52} = 4503\,5996\,2737\,0496 = 8497357784815 \times 53 + 1.$$

(This is like a Visa card number.)

4.2 Linear equations modulo a number

Consider n a number, which we also call the modulus in the following situation. Suppose we want to solve the linear equation

$$ax \equiv b \pmod{n}.$$

If we change $x \mapsto x' = x + qn$, this doesn't change anything. So really we are looking for $x \in \{0, 1, \dots, n-1\}$. Actually, we already know the answer. This equation is equivalent to

$$ax + ny = b.$$

This is solvable for x and y if and only if b is divisible by $\gcd(a, n)$. For instance, if $\gcd(a, n) = 1$ then we can solve the equation for any b.

This is relevant to the question about when you can invert an element.

Lemma 4.5. *If p is prime, then every nonzero element in $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse.*

This means that $\{1, 2, \dots, p-1\}$ is an abelian group under multiplication, so $\mathbb{Z}/p\mathbb{Z}$ is a field. Do you believe this? I don't, so let us check this for $p = 7$. As we see in Table 3, everything can be multiplied by something to give anything else.

×	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Table 3: Multiplication table for $\mathbb{Z}/7\mathbb{Z}$

On the other hand, suppose that n is not a prime. We know that $ax \equiv b \pmod{n}$ can be solved if and only if $\gcd(a, n)$ divides b. This means that if $b = 1$, it can be solve if and only if a and n are relatively prime. So the only elements in $\mathbb{Z}/n\mathbb{Z}$ that has a multiplicative inverse are exactly those that are relatively prime to n. We can see this for $n = 6$.

In general, we can look at

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \text{ that are relatively prime to } n\}.$$

Now this does form a group under multiplication, and this is called the **group of units** in $\mathbb{Z}/n\mathbb{Z}$. You can ask why this set is even closed under multiplication. If a and b are relatively prime to n, then ab is relatively prime to n. You can see this if you apply the fundamental theorem of arithmetic to a, b, n, and compare factors.

Example 4.6. For $n = 8$, we have

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}.$$

In this group, $3 \cdot 5 = 7$, $7 \cdot 3 = 5$, $a \cdot a = 1$ for all $a \in \mathbb{Z}/8\mathbb{Z}$.

4.3 Euler's totient function

Definition 4.7. For a positive integer n, we define

$$\varphi(n) = \text{number of elements in } \{1, \ldots, n\} \text{ that are relatively prime to } n.$$

This is equal to the number of elements in the group $(\mathbb{Z}/n\mathbb{Z})^\times$.

For instance, if p is a prime, then $\varphi(p) = p - 1$. What about $n = pq$, where p and q are distinct primes? We need to count the numbers among

$$1, 2, \ldots, pq$$

that are not divisible by both p and q. First throw away pq. Then numbers divisible by p are

$$p, 2p, 3p, 4p, \ldots, p(q-1),$$

and the numbers divisible by q are

$$q, 2q, 3q, \ldots, (p-1)q.$$

These numbers don't overlap, and so we get

$$\varphi(pq) = pq - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1).$$

5 September 19, 2018

If we look at integers modulo n, we say that $a \sim b$ are equivalent if $a - b$ is divisible by n. So this is modeling things that are cycling, like hours on a clock. If we take

$$\{0, 1, 2, \dots, n-1\},$$

this is a **complete set of residues**. This means that any integer is equivalent to exactly one element in the set modulo n. We can take other sets, for instance,

$$\{n, n+1, n+2, \dots, 2n-1\} \text{ or } \{n, 2n+1, 3n+2, \dots, n^2 + (n-1)\}$$

are complete set of residues, in the sense that no two elements are equivalent modulo n and every integer is equivalent to some element modulo n.

Adding numbers modulo n is something we do all the time. If we try to calculate what day of the week it is, 30 days from today, we are doing addition modulo 7. Multiplication might not be so familiar, but we can do this similarly. If $a \equiv 3 \pmod{12}$ and $b \equiv 5 \pmod{12}$, then we have $ab \equiv 3 \times 5 = 15 \equiv 3 \pmod{12}$. We also showed that a number $a \in \mathbb{Z}/n\mathbb{Z}$ has a (multiplicative) inverse if and only if a is relatively prime to n. Addition in $\mathbb{Z}/52\mathbb{Z}$ also can be thought of as a shuffling. If we break the deck into two sets and exchange them, like

$$\begin{gathered} 0, 1, 2, \dots, a-1, a, a+1, \dots, 51 \\ \downarrow \\ a, a+1, \dots, 51, 0, 1, 2, \dots, a-1, \end{gathered}$$

we are just applying the transformation

$$m \mapsto m - a \pmod{52}.$$

Even if we do this shuffle k times, it is just $m \mapsto m - ka \pmod{52}$. So if ka is a multiple of 52, the deck will come back to itself.

So with all these operations, we can say that $\mathbb{Z}/n\mathbb{Z}$ is a ring. A field was a ring with inverses for every nonzero number, so $\mathbb{Z}/p\mathbb{Z}$ is a field. (Actually, the notion of rings and fields will not be too important in this course. Don't try too hard to remember the precise definition.) The number $a \in \mathbb{Z}/n\mathbb{Z}$ has an inverse if and only if it is relatively prime. We defined

$$(\mathbb{Z}/n\mathbb{Z})^\times = \text{group of units in } \mathbb{Z}/n\mathbb{Z},$$

and we defined $\varphi(n)$ to be the size of this group. We computed

$$\varphi(p) = p - 1, \quad \varphi(pq) = (p-1)(q-1)$$

for distinct prime p, q last time.

Let me do another example. What is $\varphi(p^3)$, for instance? Among the numbers

$$1, 2, 3, \dots, p^3 - 1,$$

the numbers not relatively prime to p^3 are the numbers divisible by p. These are

$$p, 2p, 3p, \dots, p^3 - p = (p^2 - 1)p.$$

If we throw them away, we get

$$\varphi(p^3) = (p^3 - 1) - (p^2 - 1) = p^3 - p^2 = p^2(p - 1).$$

More generally, we will get

$$\varphi(p^k) = (p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1} = p^{k-1}(p - 1).$$

Now we know $\varphi(n)$ for n a power of a prime. There is this theorem, which we will prove later.

Theorem 5.1. *If a and b are relatively prime, then*

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Because any integer is a product of prime powers, relatively prime to each other, this theorem tells us exactly how to calculate $\varphi(n)$ for all n.

5.1 Order of an element

Recall what happened for the perfect shuffle. To find how many times we need to perform a shuffle to get back, we needed to find the k such that

$$2^k \equiv 1 \pmod{51}, \quad 2^k \equiv 1 \pmod{53}.$$

We can do this is greater generality.

Let G be a group, so that there is multiplication $a \cdot b$ satisfying the axioms $a(bc) = (ab)c$ and $1a = a1 = a$ and existence of inverses. (Think of $G = (\mathbb{Z}/n\mathbb{Z})^\times$ if you're confused.) For each element $a \in G$, we can try to look at the smallest positive integer m such that

$$a^m = 1 \in G.$$

This smallest m is called the **order** of a. This number might not exist of the group G is infinite, but if G is finite, the order is always defined and is finite.

Example 5.2. Consider $(\mathbb{Z}/10\mathbb{Z})^\times = \{1, 3, 7, 9\}$. This is a group; everybody has an inverse, because $1 \cdot 1 = 3 \cdot 7 = 7 \cdot 3 = 9 \cdot 9 = 1$. Now we can look for the order of each element. We have

$$3^1 = 3, \quad 3^2 = 9, \quad 3^3 = 9 \cdot 3 = 7, \quad 3^4 = 7 \cdot 3 = 1.$$

This means that the order of $3 \in (\mathbb{Z}/10\mathbb{Z})^\times$ is 4. If we do this for all the elements, we get

$$\operatorname{order}(1) = 1, \quad \operatorname{order}(3) = 4, \quad \operatorname{order}(7) = 4, \quad \operatorname{order}(11) = 2.$$

Example 5.3. What about $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$? Here, we have that

$$\text{order}(1) = 1, \quad \text{order}(5) = 2, \quad \text{order}(7) = 2, \quad \text{order}(11) = 2.$$

So everything sort of cycles around.

Example 5.4. What if we take a prime, like $(\mathbb{Z}/7\mathbb{Z})^\times = \{1, 2, 3, 4, 5, 6\}$? We can calculate

$$\text{order}(1) = 1, \quad \text{order}(2) = 3, \quad \text{order}(3) = 6, \quad \text{order}(4) = 3, \quad \text{order}(5) = 6, \quad \text{order}(6) = 2.$$

Now let me make an argument that every element has a finite order, inside a finite group. Take any element $a \in G$, and look at the sequence

$$1, a, a^2, a^3, a^4, \dots.$$

Because the group is finite, this sequence should visit something that it visited before, at some point. Assume that

$$a^k = a^p$$

for $p < k$. Then we can multiply $(a^{-1})^p$ on both sides, and this gives

$$a^{k-p} = 1.$$

So the order of a must be finite. But there is a theorem of Lagrange gives more than that.

5.2 Lagrange's theorem

Theorem 5.5 (Lagrange)**.** *The order of any element of a finite group divides the size of the group.*

In $(\mathbb{Z}/53\mathbb{Z})^\times$, we had that order(2) = 52. Lagrange's theorem tells us that order(2) has to divide 52, and it just turned out that the order is the maximal possible number. In principle, it could have been order(2) = 4 maybe, but this did not happen. On the other hand, in $(\mathbb{Z}/51\mathbb{Z})^\times$, the order order(2) divides $\varphi(51) = 32$. We actually got order(2) = 8 in this case, and so we were able to conveniently cheat by doing only 8 shuffles.

Proof. Let us write $a \in G$ and $\text{order}(a) = m$. Then we can look at the subset

$$\{1, a, a^2, \dots, a^{m-1}\} \subseteq G.$$

This is this not all of G, we can pick $b_1 \notin \{1, \dots, a^{m-1}\}$ and look at the subset

$$\{b_1, ab_1, a^2b_1, \dots, a^{m-1}b_1\}.$$

These are all distinct, and there is no overlap because if $a^k b_1 = a^p$ then $b_1 = a^{p-k}$ contradicts our assumption. If these two subset exhaust all of G, then we can pick another element $b_2 \in G$ not listed above. Then we again look at

$$\{b_2 ab_2, a^2b_2, \dots, a^{m-1}b_2\},$$

and do this over an over again. Once are done, we see that we divided G into groups of size m. So m divides the size of G. □

Here is another very clever proof, assuming that G is abelian, e.g., for $G = (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Let us write

$$G = \{1 = a_1, a_2, a_3, \dots, a_N\},$$

where N is the size of N. For $x \in G$, I want to look at the product

$$P = (xa_1) \cdot (xa_2) \cdot \dots \cdot (xa_N) = x^N (a_1 a_2 \cdots a_N) \in G.$$

But on the other hand, we have

$$xa_1 = a_k, \quad xa_2 = a_l, \quad xa_3 = a_m, \quad \dots$$

while something like $a_k = a_l$ cannot happen because then $a_1 = x^{-1}a_k = x^{-1}a_l = a_2$. This means that if I multiply them all together, we get

$$P = (xa_1) \cdot (xa_2) \cdot \dots \cdot (xa_N) = a_1 \cdot a_2 \cdot \dots \cdot a_N.$$

Combining the two equations for P, and canceling out $a_1 a_2 \cdots a_N$, we get

$$x^N = 1.$$

This shows that order(m) divides N, because otherwise we can write $N = mq + r$ and get $x^r = x^N (x^m)^{-q} = 1$. □

If we apply this to $(\mathbb{Z}/n\mathbb{Z})^\times$, we get the following fact. If x is relatively prime to n, then

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

If n is prime, we get the following theorem.

Theorem 5.6 (Fermat's little theorem)**.** *If p is prime and x does not divide p, then*

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

6 September 24, 2018

We can think of $(\mathbb{Z}/n\mathbb{Z})^\times$ as the numbers that are relatively prime to n. If $n = p$ is prime, this is just

$$\{1, 2, \dots, p-1\},$$

which is an interesting case. If $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, we call the smallest m with $a^m \equiv 1 \pmod{n}$ the order of a. We showed that

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

which implies that the order of every a divides $\varphi(n)$. If n is a prime, we get Fermat's little theorem, that

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

if p is a prime that does not divide a. So for instance, $10^6 - 1 = 999\,999$ is divisible by 7.

Corollary 6.1. *We have*

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

for all $a \in \{1, 2, \dots, p-1\}$ if and only if p is prime.

Proof. We know this for p a prime. Suppose p is composite, so that $p = rs$ with $1 < r, s < p$. Is it possible that $r^{p-1} - 1 = qp$? No, because both r^{p-1} and qp are divisible by r. □

This is important in coding. There is a Rabin–Miller algorithm that takes a number and tells you whether it is probably a prime.

6.1 Wilson's theorem

There is another theorem about primes.

Theorem 6.2 (Wilson)**.** *For $p > 2$ an integer*

$$(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1) \equiv (-1) \pmod{p}$$

if and only if p is a prime.

Actually this does not give an efficient algorithm for primality testing, because to compute $(p-1)!$, you need to actually perform $p-2$ multiplications.

Proof. Suppose p is prime. Then for every element $a \in \{2, 3, \dots, p-2\}$, there is an inverse. So these things pair up with the inverse. Here, note that none of them are their own inverses, because $x \equiv x^{-1} \pmod{p}$ means $x^2 - 1 \equiv 0 \pmod{p}$, and $x^2 - 1 = (x+1)(x-1)$ implies that this is possible only for $x \equiv \pm 1 \pmod{p}$. Then when we pair up, they vanish, so

$$(p-2)! \equiv 1 \cdot (p-1) \cdot (1 \cdot \dots \cdot 1) \equiv -1 \pmod{p}.$$

On the other hand, if p is not a prime, so that $p = rs$, then r divides $(p-1)!$ because r is going to be one factor. It cannot be that r divides p and p divides $(p-1)! + 1$, because r divides $(p-1)!$. □

We can check this:

$$\begin{aligned} 4! = 24 &\equiv -1 \pmod 5, & 5! = 120 &\equiv 0 \pmod 6, \\ 6! = 720 &\equiv -1 \pmod 7, & 7! = 5040 &\equiv 0 \pmod 8. \end{aligned}$$

So you can impress people at the party using this.

6.2 Rabin–Miller and Euclidean algorithms

Here is how you run the **Rabin–Miller algorithm**, which tests if p is prime.

1. Look at the number p, and write it as $p-1 = 2^k \cdot m$, where m is odd. (Assume that p is odd, because that is when primality testing is interesting. Then $k \geq 1$.)
2. Pick an integer $1 \leq a \leq p-1$ at random.
3. Compute $b = a^m \pmod p$. If $b \equiv \pm 1 \pmod p$, then output "probably prime" and stop.
4. Compute b^{2^r} for $r = 1, 2, \dots, k-1$. If $b^{2^r} \equiv -1 \pmod p$ for some r, then output "probably prime" and stop.
5. Otherwise, output "not prime".

All steps seems to take at most $\log_2 p$ computations, except for computing $b = a^m \pmod p$. This seems to take m steps, but is there a more efficient way? We first write m in the base 2 expansion,

$$m = 2^k + \epsilon_{k-1} 2^{k-1} + \cdots + \epsilon_1 2^2 + \epsilon_0$$

with $\epsilon_j \in \{0, 1\}$. (Then k is around $\log_2 m$.) To compute a^m, we first compute the powers

$$a^1, a^2, a^4, a^8, \dots, a^{2^k} \pmod p$$

by iterative squaring. This can be done using not much memory, because we can take the remainder modulo p after each squaring. So this only requires something like $k \sim \log_2 m$ multiplications. Then we take

$$a^m = (a^{2^k}) \cdot (a^{2^{k-1}})^{\epsilon_{k-1}} \cdot \cdots \cdot (a^2)^{\epsilon_1} \cdot (a)^{\epsilon_0}.$$

This takes at most $k \sim \log_2 m$ additional multiplications. So the entire process takes at most $C \log_2 p$ time, where C is some constant not depending on p. This is pretty fast. This whole subject of unbreakable codes is based on calculation of primes.

Here is another algorithm that was in the book. Recall that we proved that there exist integers x and y such that

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

Stein's book gives a proof by finding an algorithm for doing this. This is based on the Euclidean algorithm. Given $a < b$, we look at

$$\begin{aligned} a &= qb + r_1, \\ b &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

Now we can read this as r_1 is a linear combination of a and b, and then r_2 is a linear combination of b and r_1 so it is also a linear combination of a and b. We can use this to inductively go down the equations and see that $r_n = \gcd(a, b)$ is a linear combination of a and b.

This algorithm is really efficient. To see this, note that $r_1 \leq \frac{1}{2}a$, because $r_1 \leq a - b$ and $r_1 \leq b$. (Adding these give $2r_1 \leq a$.) Now we can do this for each equation, and we get

$$r_1 \leq \frac{1}{2}a, \quad r_2 \leq \frac{1}{2}b, \quad r_3 \leq \frac{1}{2}r_1, \quad \cdots.$$

So there are at most $2 \log_2 a$ steps in the Euclidean algorithm. This means that it is pretty fast.

6.3 Sunzi's remainder theorem

Now I am going to introduce a theorem about relatively prime numbers. It is also called the **Chinese remainder theorem**, because it is unclear if Sunzi first discovered it or just wrote down common knowledge.

Theorem 6.3 (Sunzi's remainder theorem)**.** *Let a and b be integers, and n and m be positive integers with $\gcd(n, m) = 1$. Then there is an integer x such that*

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}.$$

Moreover x is unique modulo mn (up to adding multiples of mn).

So you can solve double congruence equations.

Proof. For the first congruence, we can just write $x = a + mq$. Now the question is, can we choose q so that the second congruence is satisfied? The second equation can be written as

$$a + mq + sn = b.$$

Then because m and n are relatively prime, we can find q and s such that $mq + sn = b - a$. Moreover, the solution is unique up to $q \to q + cn$ and $s \to s - cm$. This shows that $x = a + mq$ is unique up to adding multiples of mn. □

What this means is that if I look at

$$\mathbb{Z}/21\mathbb{Z} = \{0, 1, 2, \ldots, 20\},$$

then specifying an element of $\mathbb{Z}/21\mathbb{Z}$ is the same as specifying an element of $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$ and specifying an element of $\mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$. We can make a table out of this:

	0	1	2	3	4	5	6
0	0	15	9	3	18	12	6
1	7	1	16	10	4	19	13
2	14	8	2	17	11	5	20

Table 4: Chinese remainder theorem for $\mathbb{Z}/21\mathbb{Z} \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$

It is saying in general, in terms of rings, there is a one-to-one map

$$\mathbb{Z}/nm\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}); \quad x \mapsto (a, b) = ([x]_{\text{ mod } m}, [x]_{\text{ mod } n}).$$

This is even a homomorphism of rings, i.e., they carry around the ring structure. So we also get

$$(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$$

as groups. If we count the number of elements on both sides, we learn a new thing. If n and m are relatively prime, then

$$\varphi(mn) = \varphi(m)\varphi(n).$$

So if we write any integer n as

$$n = p_1^{k_1} p_2^{k_2} \cdots ,$$

then we can compute

$$\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots = p_1^{k_1 - 1}(p_1 - 1) p_2^{k_2 - 1}(p_2 - 1) \cdots .$$

7 September 26, 2018

We looked at Sunzi's theorem, which characterizes $\mathbb{Z}/ab\mathbb{Z}$ for a and b relatively prime. We showed that as a ring, this is isomorphic to

$$\mathbb{Z}/ab\mathbb{Z} \cong (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}).$$

This means that given integers y and z, there is a unique $x \pmod{ab}$ such that

$$x \equiv y \pmod{a}, \quad x \equiv z \pmod{z}.$$

This even implies that

$$(\mathbb{Z}/ab\mathbb{Z})^\times \cong (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times; \quad x \mapsto ([x]_a, [x]_b)$$

is an isomorphism. If we count elements, we get $\varphi(ab) = \varphi(a)\varphi(b)$.

7.1 Primitive roots

We know that $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \dots, p-1\}$ for p a prime, but we don't know a lot about the multiplicative group structure.

Theorem 7.1. *If p is a prime, there are $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ that generate $(\mathbb{Z}/p\mathbb{Z})^\times$, that is,*

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, a, a^2, \dots, a^{p-2}\}.$$

In such a case, a is called a **primitive root**. This also can be stated as that there is an element of $(\mathbb{Z}/p\mathbb{Z})^\times$ with order equal to $p-1$. (Recall that it always divides $p-1$.) So this group is really simple, given that we can find this element a. Let us look at examples.

- Take $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$. That works.
- What about $(\mathbb{Z}/3\mathbb{Z})^\times = \{1, 2\}$? We have $2^2 = 1$ so $a = 2$ satisfies this.
- For $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$, we have $2^2 = 4, 2^3 = 3$ so we have everybody for $a = 2$. We find that $a = 3$ also works.
- For $(\mathbb{Z}/7\mathbb{Z})^\times = \{1, 2, 3, 4, 5, 6\}$, we have $2^2 = 4, 2^3 = 1$, so it fails. We have $3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5$ and so $a = 3$ works.

The algorithm is basically, try 2, then try 3, and so on.

The proof is based on that $\mathbb{Z}/p\mathbb{Z}$ is a field. Basically if $ab = 0$ then $a = 0$ or $b = 0$.

Theorem 7.2. *Suppose k is a field. Consider solving the polynomial equation*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

for $x \in k$, where $a_i \in k$ and $a_n \neq 0$. Then there are at most n solutions.

This works because k is a field. For instance, $x^2 - 1 = 0$ has 4 solutions in $\mathbb{Z}/8\mathbb{Z}$, which is not a field.

Proof. We do induction on $n = \deg f$. If $n = 1$, we have $a_1x + a_0 = 0$, so we have $x = a_1^{-1}a_0$. (Recall that $a_1 \neq 0$ by assumption and any nonzero element of k has an inverse.)

Let's now look at $a_nx^n + \cdots + a_1x + a_0 = 0$. If there are no solutions, we are done. Otherwise, let α be one solution to this equation. Then $f(x) = 0$ is equivalent to

$$a_n(x^n - \alpha^n) + a_{n-1}(x^{n-1} - \alpha^{n-1}) + \cdots + a_1(x - \alpha) = 0.$$

But then we can factor $x^q - y^q = (x - y)(x^{q-1} + \cdots + y^{q-1})$. Then we can write equation as

$$(x - \alpha)\big[a_n(x^{n-1} + \alpha x^{n-2} + \cdots) + a_{n-1}(x^{n-2} + \cdots) + \cdots + a_1\big] = 0.$$

Here, the thing in the bracket is a polynomial in x of degree $n - 1$. By the induction hypothesis, that polynomial has at most $n - 1$ solutions.

If x is a solution to $f(x) = 0$, then either $x - \alpha = 0$ or $[\cdots] = 0$ because k is a field. That is, either $x = \alpha$ or x is one of the roots of $[\cdots] = 0$. This shows that $f(x)$ has at most $1 + (n - 1) = n$ solutions. □

By the way, there are all kinds of interesting fields number theorists introduce. For instance

$$\{a + bi \in \mathbb{C} : a, b \in \mathbb{Q}\} \text{ or } \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

are fields. We have

$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + bb') + (ab' + a'b)\sqrt{2}.$$

Now we have this algebraic fact. We know that $x^{p-1} - 1 = 0$ has exactly $p - 1$ solutions in $\mathbb{Z}/p\mathbb{Z}$.

Lemma 7.3. *If p is a prime and d divides $p - 1$, then*

$$x^d - 1 = 0$$

has exactly d solutions in $\mathbb{Z}/p\mathbb{Z}$.

Proof. There is some e such that $d \cdot e = p - 1$. So we write $x^{p-1} - 1$ as

$$0 = x^{p-1} - 1 = (x^d)^e - 1 = (x^d - 1)((x^d)^{e-1} + (x^d)^{e-2} + \cdots + 1).$$

Here, $x^d - 1$ has at most d solutions, $(\cdots)$ has at most $d(e - 1)$ solutions, but are exact $p - 1$ solutions to $x^{p-1} - 1$. This shows that $x^d - 1$ has to have exactly d solutions and $(\cdots)$ has to have exactly $d(e - 1)$ solutions. □

So let's see how we can prove something. Let's assume that $p - 1 = 2q$ where q is an odd prime, for instance. The solutions to the equation $x^2 - 1 = 0$ are ± 1, so there are two. There are going to be q solutions to $x^q - 1 = 0$, and 1 is a common solutions. So there are going to be $q + 2 - 1 = q + 1$ numbers that are solutions to either $x^2 - 1$ or $x^q - 1$. This leaves out $q - 1$ numbers, whose order must be $2q = p - 1$.

Example 7.4. If we look at $p = 7$ and $q = 3$. Then the solutions of $x^2 - 1 = 0$ are $\{1, 6\}$, and the solutions of $x^3 - 1 = 0$ are $\{1, 2, 4\}$. So 5, which is left out, should be a primitive root of 7.

In the general case, let us write $p - 1 = q_1^{k_1} \cdots q_l^{k_l}$. Then the equation

$$x^{q^k} - 1 = 0$$

has q^k solutions, and $x^{q^{k-1}} - 1 = 0$ has q^{k-1} solution. So there are $q^{k-1}(q - 1)$ many x such that $x^{q^k} - 1 = 0$ but $x^{q^{k-1}} - 1 \neq 0$. That is, there are elements $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that the order of a is $q_i^{k_i}$.

Lemma 7.5. *In an abelian group, if a has order m and b has order n and m and n are relatively prime, then ab has order mn.*

Proof. Note that

$$(ab)^{mn} = (a^m)^n (b^n)^m = 1^n 1^m = 1,$$

so the order divides mn. So we can write the order as rs, where r divides m and s divides n. Write $m = rr'$ and $n = ss'$. Then

$$1 = 1^{r'} = ((ab)^{rs})^{r'} = a^{ms} b^{ms} = b^{ms}.$$

Because b has order n, this implies that n divides ms, and so n divides s. This shows that $n = s$. Similarly, we get $m = r$. Therefore the order of ab is mn. □

We showed above that we can find elements

$$a_1, a_2, \dots, a_l \in (\mathbb{Z}/p\mathbb{Z})^\times$$

such that a_i has order $q_i^{k_i}$. So then the order of their product

$$a = a_1 a_2 \cdots a_l$$

is $q_1^{k_1} \cdots q_l^{k_l} = p - 1$, by the above lemma. This shows that a is a primitive root. In fact, you can show that there are exactly $\varphi(p - 1)$ primitive roots, if you are careful with counting.

So what is the probability that a random number in $(\mathbb{Z}/p\mathbb{Z})^\times$ will be a primitive root? We can calculate this by

$$\begin{aligned}\frac{\varphi(p-1)}{p-1} &= \frac{q_1^{k_1-1}(q_1 - 1) q_2^{k_2-1}(q_2 - 1) \cdots q_l^{k_l-1}(q_l - 1)}{q_1^{k_1} q_2^{k_2} \cdots q_l^{k_l}} \\ &= \frac{q_1 - 1}{q_1} \cdots \frac{q_l - 1}{q_l} = \Big(1 - \frac{1}{q_1}\Big)\Big(1 - \frac{1}{q_2}\Big) \cdots \Big(1 - \frac{1}{q_l}\Big).\end{aligned}$$

This is going to be pretty big, so you will probably find a primitive root pretty soon.

Theorem 7.6. *For an odd prime p, the group $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is a cyclic group as well, that is, there is primitive root for p^k.*

Proof. I'm not going to prove it. □

Now we're going to move to an applied topic. There is a cryptography called the RSA, and it uses the fact that if p and q are primes, then

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

for any $a \in (\mathbb{Z}/pq\mathbb{Z})^\times$.

8 October 1, 2018

Let p be a prime. A primitive root is, we defined, an element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ that has order $p-1$, so that

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, a, a^2, \dots, a^{p-2}\}.$$

There is a famous conjecture called Artin's conjecture.

Artin's conjecture. *For every integer $a \neq -1$ that is not a perfect square, there are infinitely many primes p such that a is a primitive root for p.*

Even if you can prove this for $a = 2$, you will become famous. The reason we are excluding -1 is because $(-1)^2 = 1$, and the reason we are excluding $a = x^2$ is because $a^{(p-1)/2} = x^{p-1} \equiv 1 \pmod{p}$.

8.1 Secret key exchange

Suppose my son wants to use my Amazon account, and I want to send him my password. But someone might be reading my emails. So here is what I do. First choose a prime number $p \approx 100^{600}$ of 600 digits, and a small number g, and share them over email.

- Now I choose a number m and my son (H) chooses n.
- I send H the number $g^m \pmod{p}$.
- H sends me the number $g^n \pmod{p}$.
- I compute the number $g^{mn} = (g^n)^m \pmod{p}$.
- H computes the number $g^{mn} = (g^m)^n \pmod{p}$.

So at the end, we share the number $g^{mn} \pmod{p}$. What the eavesdropper know is

$$p, \quad g, \quad g^n, \quad g^m.$$

But it is hard to compute n from g^n. This is called the **discrete logarithm problem**. Given $g \in G$ and $b = g^n \in G$, we can't efficiently calculate the number n. One thing you can try is enumerate the power of g,

$$g, g^2, g^3, \dots, g^n = b$$

until b appears, but it will take n time, where n is of the order 10^{600}. On the other hand, taking the nth power has an efficient algorithm. This is because we can do binary expansion and compute $g^1, g^2, \dots, g^{2^k}$.

In calculus, we have $g^{x+\Delta x} \sim g^x + O(\Delta x)$. But in the discrete logarithm problem, the number $g^{x+\Delta x}$ changes drastically for a small Δx. For instance, if $p = 17$ and $g = 3$, we get the sequence

$$3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6.$$

So it just bouncing around, almost randomly.

Now suppose there are three people, let's say me and H and A. Again, choose a prime p of 600 digits and a number $g \in \{1, 2, \ldots, p-1\}$, and then share them over email with everyone.

- I pick m, H picks n, and A picks k.
- I send H the number g^m, then H sends A the number $(g^m)^n = g^{mn}$, and then A calculates the number $(g^{mn})^k = g^{mnk}$.
- H sends A the number g^n, then A sends me the number g^{nk}, then I compute $(g^{nk})^m = g^{mnk}$.
- A sends me the number g^k, then I send H the number g^{mk}, and then H computes $(g^{mk})^n = g^{mnk}$.

At the end, we all share the number $s = g^{mnk}$. That's pretty clever.

But here is what the eavesdropper (E) can do, if E can intercept the message rather than just eavesdropping.

- E picks a number t.
- I think I am sending H the number g^m, but actually E receives the number.
- E gets the number g^m, and sends g^t instead to H, so that H thinks g^t came from me.
- H thinks that the secret key is g^{tm}.
- Similarly, E intercepts H's message and sends g^t instead to me.
- I think that the secret key is g^{tn}.

$$\begin{tikzcd} C \arrow[r, shift left, "g^m"] & E \arrow[l, shift left, "g^t"] \arrow[r, shift left, "g^t"] & H \arrow[l, shift left, "g^n"] \end{tikzcd}$$

But at this point, E knows both the number g^{tm} and g^{tn}. So when we try to encode messages using the secret key s, what E can do is to intercept all messages, decode with respect to one key and encode with respect to another key.

8.2 RSA cryptography

This is based on the fact that it is really hard to factorize integers. Pick two primes p and q of the order 10^{600}, and compute the public key $N = pq$. This number N is displayed in public, although p and q are kept secret. I also pick a number c that is relatively prime to $(p-1)(q-1)$, and make c public as well.

Now we consider

$$(\mathbb{Z}/pq\mathbb{Z})^\times = \{\text{relatively prime to } N \text{ between 1 and } pq-1\}.$$

If a is relatively prime to N, we have

$$a^{(p-1)(q-1)} \equiv 1 \pmod{N}$$

by Euler's theorem. Because c is chosen to be relatively prime to $(p-1)(q-1)$, I can solve

$$cd + (p-1)(q-1)y = 1$$

using the Euclidean algorithm, so I can compute the inverse $cd \equiv 1 \pmod{(p-1)(q-1)}$ relatively efficiently. This d is kept secret, and people can't do the same computation efficiently because $(p-1)(q-1)$ is kept secret (although $N = pq$ is public).

If A wants to encode some message and send this to me, A can first change the message to a number a smaller than 10^{600} (just to ensure that it is relatively prime to N), and then send

$$a^c \pmod{N}$$

to me. This is the encoded message. To decode it, I can receive the number $a^c \pmod{N}$ and then raise it to the power of d, which gives

$$(a^c)^d \equiv a^1 = a \pmod{N}.$$

So here is how this works in entirety, if A wants to send C some message.

- C picks large primes p and q.
- C picks a number c that is relatively prime to $(p-1)(q-1)$.
- C sends A the number $N = pq$ and c.
- A chops the message into pieces and turns them into numbers smaller than N (or maybe $\min(p, q)$).
- A computes the numbers $a^c \pmod{pq}$, and then sends C these numbers.
- C computes the integer d such that $cd \equiv 1 \pmod{(p-1)(q-1)}$.
- Then C computes $(a^c)^d \equiv a \pmod{pq}$. This process recovers the original message a.

If the eavesdropper figures out what p and q are, then E can do the decoding as fast as I can. Or if E can compute the order of b in $(\mathbb{Z}/pq\mathbb{Z})^\times$ then E can decode the message.

Here is how we could encode the message (in English) in $(\mathbb{Z}/pq\mathbb{Z})^\times$. First attach to each alphabet a number,

$$\text{space} = 0, \quad A = 1, \quad B = 2, \quad \dots, \quad Z = 26.$$

Then we can look at any text and write it in base 27, like

$$a_k 27^k + a_{k-1} 27^{k-1} + \cdots + a_0$$

where the original message was $a_0 a_1 \cdots a_k$. As long as $27^{k+1} < N$, this number fits in $(\mathbb{Z}/pq\mathbb{Z})^\times$. If this is not relatively prime, just add a number of spaces at the end, and this will be relatively prime with very high probability.

If you can get either p or q, you can decode the message. This is equivalent to knowing $\varphi(N) = (p-1)(q-1)$, because $p+q = pq - \varphi(N) + 1$. As we will see on Wednesday, if b is an encoded message and I know some r such that $b^r \equiv 1 \pmod{pq}$, (not necessarily the smallest!) then I can decode the message easily.

9 October 3, 2018

Let us recall the idea of RSA. We pick two primes p, q, and make their product $N = pq$ public. Also, we pick c a number relatively prime to $(p-1)(q-1)$, and make that public as well. The message is encoded by raising to the power of c. The decoding is done by finding a d such that $cd \equiv 1 \pmod{(p-1)(q-1)}$ and then raising to the power of d.

Suppose that the message is b, and suppose we know the order r of the message b, so that $b^r \equiv 1 \pmod{N}$. What can we do with that? Then r is an order of a as well, because

$$a^r \equiv (b^d)^r = (b^r)^d \equiv 1^d = 1 \pmod{N}.$$

Because r is an order, it divides $(p-1)(q-1)$ and so c is relatively prime to r. Then we can find a d' such that

$$d'c \equiv 1 \pmod{r}, \quad d'c = 1 + mr.$$

Then

$$b^{d'} \equiv (a^c)^{d'} = a^{cd'} = a \cdot a^{mr} = a \cdot 1^m = a \pmod{N}.$$

That is, we can decode the message by raising to the power of d'. This shows that if we know the order of the message b, then we can decode the message pretty fast. But again, finding the order of an element is not an easy task.

If you know the order, it is also pretty easy to factorize the integer. Suppose that we have

$$h^m \equiv 1 \pmod{N}.$$

Keep dividing m by 2, until we have something like

$$h^m \equiv 1 \pmod{N}, \quad h^{m/2} \not\equiv \pm 1 \pmod{N}.$$

Then $h^{m/2}$ is not 1, but its square is 1. We saw that

$$\mathbb{Z}/pq\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z}),$$

so there are four numbers squaring to 1, namely $(1, 1)$ and $(1, -1)$ and $(-1, 1)$ and $(-1, -1)$. Because we are assuming that it is not $(1, 1)$ or $(-1, -1)$, it is either $(1, -1)$ or $(-1, 1)$. Then

$$\gcd(h^{m/2} - 1, N)$$

will give one prime factor of N.

9.1 Equations with powers

Previously, we looked at how to solve the equation

$$ax \equiv b \pmod{p}.$$

Now let's try to solve equations that look like

$$ax^k \equiv b \pmod{p}.$$

Because we can find a d such that $ad \equiv 1 \pmod{p}$, we can multiply d on both sides and write the equation equivalently as

$$x^k \equiv bd = c \pmod{p}.$$

where we define $c = bd$.

We know that, because $\mathbb{Z}/p\mathbb{Z}$ is a field, the equation $x^k \equiv c \pmod{p}$ has at most k solutions.

Definition 9.1. The number c is called a kth **power residue** if $x^k \equiv c$ has a solution. It is called a **quadratic residue** if $x^2 \equiv c$ has a solution, and a **quadratic non-residue** if there is not.

Let's try to solve $x^k \equiv c \pmod{p}$ in general. Pick a primitive root g, and then we can write

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, g, g^2, \dots, g^{p-2}\}.$$

Then we can write $c = g^m$ for some m and $x = g^z$ for some z. This z is what we are looking for. Then our equation can be written as

$$g^{kz} \equiv g^m \pmod{p},$$

which is equivalent to

$$kz \equiv m \pmod{p-1},$$

because g is a primitive root. So this reduces to a linear equation, not mod p but mod $p - 1$.

If k is relatively relatively prime to $p - 1$, then there exists a k' such that $kk' \equiv 1 \pmod{p-1}$. then we have

$$z \equiv k'm \pmod{p-1}.$$

Corollary 9.2. *If k is relatively prime to $p-1$, then every nonzero element in $\mathbb{Z}/p\mathbb{Z}$ is a kth power residue.*

Example 9.3. Take $\mathbb{Z}/17\mathbb{Z}$. Then 3 turns out to be a primitive root, and so we can write $(\mathbb{Z}/17\mathbb{Z})^\times$ as

$$(\mathbb{Z}/17\mathbb{Z})^\times = \{1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6\}.$$

Now suppose that we want to solve $x^3 = c$. Everything is going to be a cube. If we list $(3^k)^3$, we will get

$$1, 10, 15, 14, 4, 6, 9, 5, 16, 7, 2, 3, 13, 11, 8, 12.$$

This is a complete list.

But for quadratic residues, it is not true. If we try to solve

$$g^{2z} = g^m$$

for instance, we get

$$2z \equiv m \pmod{p-1}.$$

Because $p-1$ is an even number, this will have a solution if and only if m is even.

Example 9.4. In $(\mathbb{Z}/17\mathbb{Z})^\times$, the quadratic residues are

$$1, 9, 13, 15, 16, 8, 4, 12, 6$$

if we list $(3^k)^2$.

In fact, this list is not going to depend on the choice of our primitive root g. You can see this from the definition of a power residue, which does not depend on any primitive root. Or you can see that if g and h are primitive roots, then $h = g^l$ for some l relatively prime to $p-1$, and so

$$kz \equiv m \pmod{p-1}$$

has a solution if and only if

$$kz \equiv ml \pmod{p-1}.$$

9.2 Linear equations in an abelian group

Here is a different way to look at the equation $x^k = c$. Consider the abelian group

$$G = (\mathbb{Z}/p\mathbb{Z})^\times.$$

We can now define a map

$$\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times; \quad x \mapsto x^k.$$

You can check that this map preserves products and inverses, i.e., $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ and $\varphi(g_1^{-1}) = \varphi(g_1)^{-1}$.

Now we look at the kernel of this map,

$$\begin{aligned} \ker(\varphi) &= \{g \in G : \varphi(g) = 1\} \\ &= \{x \in (\mathbb{Z}/p\mathbb{Z})^\times : x^k = 1\}. \end{aligned}$$

So this is just the set of solutions for $x^k = 1$. So far, we know that

- there is exactly one solution if k is relatively prime to $p-1$,
- if k is a divisor of $p-1$ then it has k solutions.

We are going to try and prove the following theorem.

Theorem 9.5. *The equation*

$$x^k \equiv c \pmod{p}$$

has a unique solution if k is relatively prime to $p-1$. If k is a divisor of $p-1$, then there is exactly 0 *of k solutions.*

We already know this, but we are going to do this using group theory only. Recall that we defined

$$\varphi : G \to H, \quad K = \ker(\varphi) = \{g \in G : \varphi(g) = 1\},$$

and this is going to be a group inside G. This is because if $g_1 \in \ker(\varphi)$ and $g_2 \in \ker(\varphi)$ then

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = 1 \cdot 1 = 1$$

so $g_1 g_2 \in \ker(\varphi)$. Similarly, you can check that inverses of things in $\ker(\varphi)$ are also in $\ker(\varphi)$.

We also can think of the subset

$$K_c = \{g \in G : \varphi(g) = c\} \subseteq G.$$

This is closely related to K, because if if pick any element $g \in K_c$, then for any $h \in K$ we have

$$\varphi(gh) = \varphi(g)\varphi(h) = c \cdot 1 = c$$

so $g' = gh \in K_c$. Conversely, if we have any two $g, g' \in K_c$, we can divide $h = g^{-1}g'$ and we get $h \in K$. This means that if K_c is nonempty, then there is a one-to-one correspondence between

$$K_c = \{g : \varphi(g) = c\} \quad \longleftrightarrow \quad K = \{g : \varphi(g) = 1\}.$$

Proposition 9.6. *If $x^k = c$ has a solution, then the number of solutions is same as the number of solutions to $x^k = 1$.*

The last thing we can do with this is to count how many c we can solve the equation. Each c accounts for k solutions in $(\mathbb{Z}/p\mathbb{Z})^\times$. So in the case where k divides $p-1$, the number of kth power residues is

$$\frac{\#(\mathbb{Z}/p\mathbb{Z})^\times}{k} = \frac{p-1}{k}.$$

This is the number of c such that $x^k = c$ has a solution. For instance, there are $\frac{p-1}{2}$ number of c such that $x^2 = c$ has a solution.

10 October 10, 2018

We were looking at equations of the form

$$x^k \equiv a \pmod{p}.$$

Here, if we write $x = g^z$ and $a = g^m$, this equation just becomes

$$g^{kz} \equiv g^m \pmod{p},$$

which is equivalent to the linear equation

$$kz \equiv m \pmod{p-1}.$$

If k divides $p-1$, there are either 0 or $\frac{p-1}{k}$ solutions to this equations. (If m is divisible by k then there are $\frac{p-1}{k}$ solutions, if not, there are no solutions.) So there are exactly $\frac{p-1}{k}$ elements $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ for which the equation

$$x^k - c \equiv 0$$

is solvable, in which case there are exactly k solutions.

10.1 Quadratic residues

We are mostly interested in the case $k = 2$. Assume that p is odd. We know that there are $\frac{p-1}{2}$ elements $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $x^2 - c$ is solvable, and $\frac{p-1}{2}$ elements c such that $x^2 - c$ is not solvable.

Definition 10.1. Fix p an (odd) prime. We call an element $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ a **quadratic residue** if the equation

$$x^2 \equiv c \pmod{p}$$

is solvable. If $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ is not a quadratic residue, we call it a **quadratic non-residue**.

There are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues. But which number is a quadratic residue and which number is a quadratic non-residue? For instance, we can ask when -1 is a quadratic residue, that is,

$$x^2 + 1 \equiv 0 \pmod{p}$$

has a solution.

Lemma 10.2. *Let p be an odd prime. A number $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a quadratic residue if and only if*

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

Proof. If a is a quadratic residue, then $a \equiv x^2$ for some x. Then

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

by Fermat's little theorem.

Now we can count numbers of quadratic residues and solutions of the equation. There are exactly $\frac{p-1}{2}$ solutions to the equation $a^{\frac{p-1}{2}} \equiv 1$, and there are exactly $\frac{p-1}{2}$ quadratic residues. Because all quadratic residues are solutions, it must be the case that the set of quadratic residues is equal to the set of solutions. Therefore we get if and only if. □

This answers the question of when -1 is a quadratic residue. By this lemma, -1 is a quadratic residue if and only if

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Corollary 10.3. *For an odd prime p, the number -1 is a quadratic residue if and only if $p = 4k + 1$.*

Now we can ask the question of, after fixing an odd prime p, whether a given number is a quadratic residue or a quadratic non-residue. We have seen that a is a quadratic residue if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. But it is always true that $(a^{(p-1)/2})^2 \equiv 1 \pmod{p}$, so we always have $a^{(p-1)/2} \equiv \pm 1$. That is,

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 & a \text{ is a quadratic residue} \\ -1 & a \text{ is a quadratic non-residue} \end{cases} \pmod{p}.$$

This implies the following properties:

- If a and b are quadratic residues, then ab is also a quadratic residue. (You can see this by $a \equiv x^2$ and $b \equiv y^2$ implying $ab \equiv (xy)^2$.)
- If a is a quadratic residue and b is a quadratic non-residue, then ab is a quadratic non-residue. (If $a^{(p-1)/2} \equiv 1$ and $b^{(p-1)/2} \equiv -1$ then $(ab)^{(p-1)/2} \equiv -1$.)
- If a and b are quadratic non-residues, then ab is a quadratic residue. (If $a^{(p-1)/2} \equiv -1$ and $b^{(p-1)/2} \equiv -1$ then $(ab)^{(p-1)/2} \equiv -$.)

This means that there is a group homomorphism

$$(\mathbb{Z}/p\mathbb{Z})^\times \to \{1, -1\}$$

that sends quadratic residues to 1 and quadratic non-residues to -1.

Definition 10.4. We define the **Legendre symbol** as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue} \\ -1 & a \text{ is a quadratic non-residue.} \end{cases}$$

This is the homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ we described above.

So we immediately have

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

For instance, if we have a prime factorization $a = q_1^{r_1} q_2^{r_2} \cdots$ then we have

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)^{r_1}\left(\frac{q_2}{p}\right)^{r_2} \cdots .$$

10.2 Statement of quadratic reciprocity

There is this celebrated theorem of Gauss, which is one of the early major achievements of number theory. The proof is really complicated, maybe the hardest proof we will do in this semester. But I spent my Columbus day trying to understand the proof, so I will give you a distilled version.

Theorem 10.5 (Gauss, quadratic reciprocity 1)**.** *If p and q are odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

What is this thing on the right hand side saying? If we write $p = 2k+1$ and $q = 2l+1$, then

$$(-1)^{\frac{(p-1)(q-1)}{4}} = (-1)^{kl}.$$

So it is -1 if both k and l are odd, and 1 if at least one of k or l is even. We then see that

$$(-1)^{\frac{(p-1)(q-1)}{4}} = \begin{cases} 1 & \text{at least one of } p \text{ or } q \text{ is of the form } 4k+1, \\ 1 & \text{both } p \text{ and } q \text{ are of the form } 4k+3. \end{cases}$$

This theorem doesn't say anything about the prime 2. So there is a part for this as well.

Theorem 10.6 (Gauss, quadratic reciprocity 2)**.** *For p an odd prime,*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \textit{ is of the form } 8k \pm 1, \\ -1 & p \textit{ is of the form } 8k \pm 3. \end{cases}$$

This theorem is really useful in computing the Legendre symbols.

Example 10.7. Suppose we want to compute

$$\left(\frac{3}{389}\right).$$

One ways is to just compute $3^{194} \pmod{389}$, because $194 = \frac{389-1}{2}$. This is doable, but it is a pain to try and do this. If we use Gauss's theorem, we can just do

$$\left(\frac{3}{389}\right)\left(\frac{389}{3}\right) = 1, \quad \left(\frac{389}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

So we see that 3 is a quadratic non-residue of 389.

Example 10.8. Let's try another example. Is 29 a square modulo 23? First, we can reduce

$$\left(\frac{29}{23}\right) = \left(\frac{6}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{3}{23}\right).$$

Here, $(\frac{2}{23}) = 1$ because $23 = 8 \times 3 - 1$, and

$$\left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = 1.$$

So 29 is a quadratic residue of 23.

10.3 First proof: counting points

The first idea is this. Take any number a relatively prime to p. We look at the numbers

$$S = \{a, 2a, 3a, \ldots, (\tfrac{p-1}{2})a\}$$

If we multiply them, we will get

$$1 \cdot 2 \cdot \cdots \cdot (\tfrac{p-1}{2}) \cdot a^{\frac{p-1}{2}}.$$

On the other hand, we can take all the number in S and make them lie in the range

$$-(\tfrac{p-1}{2}), \ldots, -1, 0, 1, \ldots, (\tfrac{p-1}{2})$$

modulo p. Here, different elements of S become different numbers in this range, because $-(\frac{p-1}{2}), \ldots, \frac{p-1}{2}$ forms a complete set of residues. Moreover, there can't be something landing in x and something landing in $-x$, because that will mean that

$$ka \equiv -x, \quad la \equiv x \pmod{p}$$

and adding them gives $(k+l)a \equiv 0 \pmod{p}$, which is impossible because $2 \leq k + l \leq p - 1$ and a is relatively prime to p.

$$\begin{tikzcd} a, 2a, 3a, \ldots, \frac{p-1}{2}a \arrow[d, rightsquigarrow, "\text{mod}p"] \\ \epsilon_1, 2\epsilon_2, \ldots, \frac{p-1}{2}\epsilon_{\frac{p-1}{2}} \end{tikzcd}$$

Figure 1: First proof of quadratic reciprocity: reducing numbers modulo p

In the above picture, each ϵ_i is either $+1$ or -1. So when we multiply everything, we get

$$\left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)! \cdot (\epsilon_1 \cdots \epsilon_{\frac{p-1}{2}}) \pmod{p}.$$

So to compute $a^{\frac{p-1}{2}}$, we only need to count how many ϵ_j are -1. More precisely,

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{an even number of } \epsilon_j \text{ are } -1, \\ -1 & \text{an odd number of } \epsilon_j \text{ are } -1. \end{cases}$$

Graphically, here is what we are doing. We draw a real line, and color the intervals $[kp, (k+\frac{1}{2})p]$ red and color the intervals $[(k+\frac{1}{2})p, (k+1)p]$ blue. Then we take a ruler with markings at $a, 2a, \ldots, (\frac{p-1}{2})a$, and count how many points lie in the blue part of the real line. We will try to do this next class.

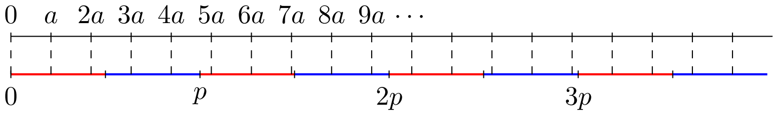

Figure 2: First proof of quadratic reciprocity: geometric interpretation

Index