PMATH 340 - Elementary Number Theory

Course Notes, University of Waterloo

Tyrone Ghaswala

Spring 2023

Contents

These notes are an overview of what was covered in each lecture of the course. They will be updated as I go, and are definitely not free of typos and mistakes. If you find any, please let me know about it and I'll fix them as soon as possible.

Lecture 1 - 8th May

1 Divisibility

Divisibility is easy in the real numbers or the rational numbers. Things are a little more interesting when we deal with the integers $\mathbb{Z}$.

Definition. Let $a, b \in \mathbb{Z}$. We say a **divides** b, and write $a \mid b$, if there exists an integer k so that $ak = b$.

If $a \mid b$, we can also say a is a factor of b or b is a multiple of a.

Example.

- $3 \mid 6$ since $3 \cdot 2 = 6$ (and 2 is an integer!).
- $3 \mid -3$ since $3 \cdot (-1) = -3$.
- $27 \mid 0$ since $27 \cdot 0 = 0$.
- $1 \mid a$ for all $a \in \mathbb{Z}$ since $1 \cdot a = a$.

Let's prove something about divisibility.

Theorem 1. *If $d \mid a$ and $a \neq 0$, then $|d| \leq |a|$.*

Proof. Since $d \mid a$, $dk = a$ for some $k \in \mathbb{Z}$. Therefore $|a| = |dk| = |d|\,|k|$. Since $a \neq 0$, $k \neq 0$ so $|k| \geq 1$. Multiplying both sides of this inequality by the positive number $|d|$ gives $|d|\,|k| \geq |d|$. Therefore $|a| \geq |d|$, completing the proof. ■

Notice that the theorem is false if $a = 0$ (for example if $k = 3$ and $a = 0$), so we really do need the assumption $a \neq 0$. Here are some facts about divisibility that we will use, but will be left as an exercise.

Exercise. Prove the following statements.

- If $c \mid a$ and $c \mid b$, then $c \mid av + bu$ for all $u, v \in \mathbb{Z}$.
- If $a \mid b$ and $b \mid c$, then $a \mid c$.
- If $a \mid b$, then $a^2 \mid b^2$.

Lecture 2 - 10th May

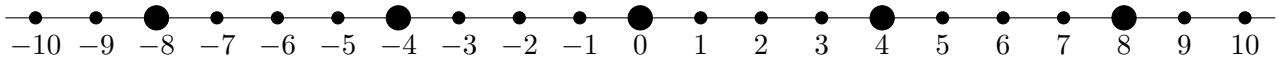
Theorem 2. *Let $a, b \in \mathbb{Z}$. We have $a \mid b$ and $b \mid a$ if and only if $a = \pm b$.*

Proof. If $a = \pm b$, then we have $a(\pm 1) = b$ and $b(\pm 1) = a$, so $a \mid b$ and $b \mid a$. Conversely, suppose $ak = b$ and $bl = a$ for some $k, l \in \mathbb{Z}$. Then $akl = a$. If $a = 0$, then $b = ak = 0$, so $a = \pm b$. Therefore we may assume $a \neq 0$, so $kl = 1$. Then $k = l = \pm 1$ so $a = \pm b$. ■

We could have also proved this theorem by dealing with the case $a = b = 0$ first, and then using Theorem 1 to get $|a| \leq |b|$ and $|b| \leq |a|$. We could then conclude $|a| = |b|$ so $a = \pm b$.

Exercise. Prove or disprove: If $a \mid b$ and $c \mid d$, then $a + c \mid b + d$.

Now, we know not every integer divides every other integer (for example $4 \nmid 5$). However, we can still say something in this case. Let's draw out the number line and emphasise all the multiples of 4.



Notice that although there are a bunch of numbers which aren't multiples of 4, then all either land on a multiple of 4, or either 1, 2, or 3, places to the right of a multiple of 4 (how far to the right is what we would call the remainder when divided by 4). So for example, $4 \nmid 5$ but we do have that 5 is one more than a multiple of 4. In fact, looking at this line, we can see every integer a can be written as $a = q \cdot 4 + r$ where q is some integer and $0 \leq r < 4$. Let's prove this is always the case!

Theorem 3 (The Division Algorithm)**.** *If $a, b \in \mathbb{Z}$ with $b > 0$, then there is a unique pair of integers q, r such that $a = qb + r$ and $0 \leq r < b$.*

Before we embark on the proof, we have to first talk about the well-ordering principle. In this course, the natural numbers are

$$\mathbb{N} = \{0, 1, 2, \ldots\}.$$

The well-ordering principle: Every non-empty subset of $\mathbb{N}$ has a least element.

This is an axiom of the natural numbers (that is, something that is handed to us as a defining feature of $\mathbb{N}$, not something we can prove). Not every set has this property! For example, $\mathbb{Z}$ doesn't have a least element (and $\mathbb{Z}$ is a non-empty subset of, well, $\mathbb{Z}$), so $\mathbb{Z}$ does not satisfy the well-ordering principle.

Exercise. Show that the set $\{x \in \mathbb{Q} \mid x > 0\}$ does not satisfy the well-ordering principle.

Now let's prove the Division Algorithm, and we will rely on the well-ordering principle to do so.

Proof. Let's first show such a q and r exist. Let $S = \{a - nb \mid n \in \mathbb{Z}\}$. If $n = -|a|$ then $a + |a|\, b \geq 0$ so $S \cap \mathbb{N}$ is a non-empty subset of $\mathbb{N}$. Let r be the least element of $S \cap \mathbb{N}$, so $r = a - qb \geq 0$ for some $q \in \mathbb{Z}$. Rearranging gives $a = qb + r$ with $r \geq 0$. We want to show $r < b$. Towards that goal, suppose $r \geq b$. Then $r - b \geq 0$ so $a - (q + 1)b = r - b \geq 0$, which contradicts r being the least element in $S \cap \mathbb{N}$. Therefore $0 \leq r < b$.

For uniqueness, suppose $a = qb + r = qb' + r'$ with $0 \leq r, r' < b$. Then $r - r' = (q' - q)b$. Since $0 \leq r, r' < b$, we have $|r - r'| < |b|$. Therefore $|r - r'| = |q - q'|\,|b|$ implies $|q - q'| < 1$. Since $q, q' \in \mathbb{Z}$ we must have $q = q'$ and thus $r = r'$. ■

The proof was hard, but the theorem can actually do quite a bit of heavy lifting for us!

Lecture 3 - 12th May

Example. Suppose $3 \nmid a$. Then the remainder of a^2 when divided by 3 is 1. Let's investigate this claim. If $3 \nmid a$, then $a = 3q + r$ where $r = 1$ or 2 and $q \in \mathbb{Z}$. If $r = 1$, then

$$a^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1.$$

if $r = 2$ then

$$a^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1.$$

In both cases, the remainder is 1, which justifies the initial claim!

Exercise.

- What are all the remainders of squares of odd numbers when divided by 8?
- Prove that an odd number times an odd number is always odd.

1.1 The Greatest Common Divisor

An extremely useful concept to pay attention to turns out to be the greatest common divisor of two integers. Intuitively, this is how much the two numbers share. You already have experience dealing with this concept when you simplify fractions. For example, you usually wouldn't write $\frac{10}{4}$, but instead you would write $\frac{5}{2}$. In the former case, 2 divides both 10 and 4, and it's the biggest thing that divides both, so you divide the numerator and denominator by 2 to obtain $\frac{5}{2}$. Even better, 5 and 2 don't share any divisors (other than ± 1), so you cannot simplify this fraction any further.

Definition. Let $a, b \in \mathbb{Z}$. A **common divisor** of a and b is an integer c so that $c \mid a$ and $c \mid b$.

Definition. Let $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$. Define the **greatest common divisor** of a and b, denoted $\gcd(a, b)$, to be the integer d such that

- d is a common divisor of a and b, and
- if c is a common divisor of a and b, then $c \leq d$.

We omit the case $a = b = 0$, and leave $\gcd(0, 0)$ to be undefined. After all, every integer divides 0, so there is no candidate for the greatest common divisor!

Example.

- $\gcd(2, 4) = 2$.
- $\gcd(5, 9) = 1$.
- $\gcd(-5, 9) = 1$.
- $\gcd(0, a) = |a|$ for all $a \in \mathbb{Z} \setminus \{0\}$.
- $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$ for all $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$.

Notice that if $c \mid a$ and $c \mid b$, then $-c \mid a$ and $-c \mid b$. Therefore we know $\gcd(a, b) \geq 0$. In the definition of the greatest common divisor we called it "the" greatest common divisor instead of "a" greatest common divisor, suggesting it is unique. Indeed it is!

Theorem 4. *When defined, the greatest common divisor of two integers (not both zero) is unique.*

Proof. Let $a, b \in \mathbb{Z}$, $a \neq 0$ or $b \neq 0$. Suppose d and d' satisfied the properties in the definition of the greatest common divisor of a and b. In particular, both d and d' are common divisors of a and b. Since d is a greatest common divisor of a and b, $d' \leq d$. Similarly since d' is a greatest common divisor, $d \leq d'$. Alas, $d = d'$. ■

Exercise.

1. Compute $\gcd(a, b)$ for the following pairs of integers.
   (a) $a = -1$, $b = 27$.
   (b) $a = 8$, $b = 13$.
   (c) $a = 13$, $b = 21$.
   (d) $a = 21$, $b = 34$.
   (e) $a = 3427$, $b = 20184$.
2. Suppose $\gcd(a, b) = d$. What is $\gcd(a^2, b^2)$?

In Question 1 of the previous exercise, for all but the last pair of integers, it's easy enough to simply write out the divisors of both integers and look for the biggest one. However, this quickly becomes tedious. Thankfully we have the Euclidean Algorithm at our disposal. Let's remind ourselves how it works with an example, and then we'll prove that it does indeed work as advertised.

Example. Let's apply the Euclidean Algorithm to compute $\gcd(203, 77)$. We repeatedly apply the division algorithm as follows:

$$\begin{aligned} 203 &= 2 \cdot 77 + 49 \\ 77 &= 1 \cdot 49 + 28 \\ 49 &= 1 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7 \\ 21 &= 3 \cdot 7 + 0. \end{aligned}$$

The last non-zero remainder gives us that $\gcd(203, 77) = 7$.

Let's write down this algorithm in general.

The Euclidean Algorithm:

Let a and b be positive integers with $a > b$ (if $a = b$ then $\gcd(a, b) = a$, so we don't need to worry about this case).

Set $r_0 = a$, $r_1 = b$, and define r_n for $n \geq 2$ as follows. Suppose r_{n-2} and r_{n-1} are positive integers with $r_{n-2} > r_{n-1}$. By the division algorithm, there exists integers q_{n-1} and r_n, with $0 \leq r_n < r_{n-1}$ so that $r_{n-2} = q_{n-1}r_{n-1} + r_n$. We now have $b > r_2 > r_3 \cdots \geq 0$, so the sequence $r_2, r_3, \ldots$ must become zero (after at most b steps). Let r_m be the last non-zero element in the sequence. The algorithm looks like this:

$$\begin{aligned} a &= q_1 b + r_2 \\ b &= q_2 r_2 + r_3 \\ r_2 &= q_3 r_3 + r_4 \\ &\vdots \\ r_{m-2} &= q_{m-1} r_{m-1} + r_m \\ r_{m-1} &= q_m r_m + 0. \end{aligned}$$

Then $\gcd(a, b) = r_m$.

To prove this works, we first have an important lemma.

Lemma 5. *If $a, q, b, r \in \mathbb{Z}$, $a \neq 0$ or $b \neq 0$, are such that $a = qb + r$, then* $\gcd(a, b) = \gcd(b, r)$.

Proof. If we show that the set of common divisors of a and b is equal to the set of divisors of b and r, then we can conclude they must have the same greatest common divisor. To this end, suppose $c \mid a$ and $c \mid b$. Then $c \mid a - qb = r$, so c is a common divisor of b and r. Conversely, if $c \mid b$ and $c \mid r$, then $c \mid qb + r = a$, so c is a common divisor of a and b. Alas, c is a common divisor of a and b if and only if c is a common divisor of b and r, completing the proof. ■

Applying Lemma 5 to the Euclidean Algorithm we get

$$\gcd(a, b) = \gcd(b, r_2) = \gcd(r_2, r_3) = \gcd(r_3, r_4) = \cdots = \gcd(r_{m-1}, r_m) = \gcd(r_m, 0) = r_m$$

which proves that the Euclidean algorithm works!

Exercise. Find the greatest common divisor of the year you were born and the year one of your parents was born.

1.2 Linear Diophantine equations and Bezout

There will be several serious exploitations of the Euclidean algorithm, here's the first, and it allows us to prove seemingly difficult things about greatest common divisors rather easily. In fact, it will have far reaching consequences throughout the rest of the course.

Bezout's identity is a way to express $\gcd(a, b)$ in terms of a and b. For example, $\gcd(3, 5) = 1$ and we have $3 \cdot 2 - 5 \cdot 1 = 1$. Although this is just one example, this kind of thing happens in general. Even better, the Euclidean algorithm tells us how to write the greatest common divisor of a and b as $ax + by$ for some integers x and y!

Theorem 6 (Bezout's identity)**.** *Let $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$. Then there exist integers x and y such that* $\gcd(a, b) = ax + by$.

Before proving this wonderful fact, let's run through an example with it.

Example (Dilcue)**.** Recall we computed $\gcd(203, 77) = 7$ via the Euclidean algorithm as follows:

$$\begin{aligned} 203 &= 2 \cdot 77 + 49 \\ 77 &= 1 \cdot 49 + 28 \\ 49 &= 1 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7 \\ 21 &= 3 \cdot 7 + 0. \end{aligned}$$

Now we run Dilcue, with is just the above algorithm backwards, starting with the second last line

and substituting our way up the series of equations.

$$\begin{aligned}
7 &= 28 - 1 \cdot 21 \\
&= 28 - 1(49 - 28) \\
&= 2 \cdot 28 - 1 \cdot 49 \\
&= 2 \cdot (77 - 49) - 1 \cdot 49 \\
&= 2 \cdot 77 - 3 \cdot 49 \\
&= 2 \cdot 77 - 3(203 - 2 \cdot 77) \\
&= 8 \cdot 77 - 3 \cdot 203.
\end{aligned}$$

Therefore we have $7 = 77(8) - 203(3)$.

Euclid followed by Dilcue gives us a way to find integers x and y so that $\gcd(a, b) = ax + by$. Let's turn this example into a proof of Bezout's identity.

Proof of Bezout's identity. Suppose $a > b > 0$ (we will deal with all other cases at the end). Perform the Euclidean algorithm, and rearranging the second-last equation gives

$$\gcd(a, b) = r_m = r_{m-2} - q_{m-1} r_{m-1}$$

so r_m is an integer combination of r_{m-1} and r_{m-2}.

Claim. If $\gcd(a, b)$ is written as an integer combination of r_{k-2} and r_{k-1} for some $k \leq m$, then $\gcd(a, b)$ can be written as an integer combination of r_{k-2} and r_{k-3}.

Proof of claim. Suppose $\gcd(a, b) = ur_{k-1} + vr_{k-2}$ for some integers u and v. Then the $(k-2)$nd line of the Euclidean algorithm can be rearranged to give

$$r_{k-1} = r_{k-3} - q_{k-2} r_{k-2}.$$

Substituting gives

$$\gcd(a, b) = u(r_{k-3} - q_{k-2} r_{k-2}) + vr_{k-2} = ur_{k-3} + (v - uq_{k-2}) r_{k-2}$$

completing the proof of the claim. ■

Now, applying the claim repeatedly gives us that $\gcd(a, b)$ can be written as an integer combination of $r_0 = a$ and $r_1 = b$, that is, $\gcd(a, b) = ax + by$ for some integers x, y.

Now, if a or b is negative, we can simply replace a and b by $|a|$ and $|b|$, find a solution to $\gcd(a, b) = |a|\, x + |b|\, y$, and simply change the sign of x or y to get a solution to $\gcd(a, b) = ax + by$. If $a < b$, we can switch the roles of x and y.

If $|a| = |b|$, then the equation we wish to solve takes the form $|a| = a(x \pm y)$ (since $a = \pm b$). This equation can be solved with $x = 1$ and $y = 0$ if a is positive, and $x = -1$ and $y = 0$ if a is negative. ■

An important thing about the proof of Bezout's identity is that although an explicit formula for how to come up with a solution to the equation $\gcd(a, b) = ax + by$, it does give us a recipe for coming up with the solution. And that recipe is exactly to do the Euclidean Algorithm forwards, and then backwards. Such a proof is called a *constructive proof* in mathematics.

Bezout's identity turns out to be super useful! From the definition of the greatest common divisor of a and b, we know that any other divisor c is such that $c \leq \gcd(a, b)$. We can now prove something even stronger.

Proposition 7. *Let $a, b \in \mathbb{Z}$, $a \neq 0$ or $b \neq 0$. We have $c \mid a$ and $c \mid b$ if and only if $c \mid \gcd(a, b)$.*

Proof. Suppose $c \mid \gcd(a, b)$. Notice that $\gcd(a, b) \mid a$, so since $c \mid \gcd(a, b)$ and since divisibility is transitive, $c \mid a$. Similarly $c \mid b$.

Conversely, suppose $c \mid a$ and $c \mid b$. Then by Bezout's identity, there are integers $x, y \in \mathbb{Z}$ so that $ax + by = \gcd(a, b)$. We have $c \mid ax + by$, so $c \mid \gcd(a, b)$. ■

Lecture 5 - 17/05

Bezout's identity gives us a solution to a very specific equation. Such equations are called **linear Diophantine equations**. A Linear Diophantine equation is an equation of the form

$$d = ax + by$$

where $a, b, d \in \mathbb{Z}$.

As an astute reader, you may have recognised $d = ax + by$ as the equation of a line (in fact the line has slope $\frac{-a}{b}$ if $b \neq 0$, and is vertical if $b = 0$). So if we allow x and y to be real numbers, there is always a solution to any linear Diophantine equation (just choose x and y so that (x, y) is a point on the line). However, over the integers, things aren't as simple!

Example. The linear Diophantine equation $4x + 10y = 3$ does not have a solution over $\mathbb{Z}$ since the left hand side is even and the right hand side is odd.

Geometrically, asking for an integer solution to $ax + by = d$ is asking for a point (x, y) on the line with integer coordinates! A point $(x, y) \in \mathbb{R}^2$ where both x and y are integers is called a **lattice point**.

Thanks to Bezout, we are now in a position to work out exactly when a linear Diophantine equation has an integer solution, or equivalently, when a line of the form $ax + by = d$ passes through a lattice point in $\mathbb{R}^2$.

Theorem 8. *Let $a, b \in \mathbb{Z}$, $a \neq 0$ or $b \neq 0$. There exist integers $x, y \in \mathbb{Z}$ such that $ax + by = d$ if and only if $\gcd(a, b) \mid d$.*

Proof. Suppose there are integers x, y so that $ax + by = d$. Since $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, then $\gcd(a, b) \mid ax + by$ so $\gcd(a, b) \mid d$. Conversely, suppose $k \gcd(a, b) = d$ for some $k \in \mathbb{Z}$. Then by Bezout's identity, there exist $x, y \in \mathbb{Z}$ so that $\gcd(a, b) = ax + by$. Then $d = k \gcd(a, b) = a(kx) + b(ky)$, completing the proof. ■

Exercise.

1. Solve the linear Diophantine equation $203x + 77y = 49$ over $\mathbb{Z}$.
2. Find infinitely many integer solutions to the Linear diophantine equation $4x + 10y = 16$. Have you found them all?

1.3 Coprimeness

The case when $\gcd(a, b) = 1$ is special, and worth investigating some more. After all, when you write a fraction $\frac{a}{b}$ in lowest terms, this exactly means $\gcd(a, b) = 1$.

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

Exercise. True or False: If a and b are coprime and b and c are coprime, then a and c are coprime.

When attempting to solve a linear Diophantine equation $ax + by = d$, having that $\gcd(a, b) = 1$ is a dream! Since $1 \mid a$ for all $a \in \mathbb{Z}$, Theorem 8 gives us that $ax + by = d$ always has a solution, regardless of what d is! Let's see what else we can squeeze out of coprimeness.

Theorem 9. *Two integers a and b are coprime if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*

Proof. This is an exercise. ■

As with any if and only if statement in mathematics, we now have that an equivalent definition of a and b being coprimes is that there is an integer solution to $ax + by = 1$. For example, we know $201 - 25(8) = 1$, so we immediately have $\gcd(201, 25) = 1$.

Here are some useful facts about coprime integers.

Proposition 10. *Let a and b be coprime integers.*

1. *If $a \mid c$ and $b \mid c$, then $ab \mid c$.*
2. *If $a \mid bc$ then $a \mid c$.*

Proof.

1. We know there exist $x, y \in \mathbb{Z}$ so that $ax + by = 1$. Since $ak = bl = c$ for some $k, l \in \mathbb{Z}$ we have
$$c = cax + cby = ablx + abky = ab(lx + ky)$$
so $ab \mid c$.
2. As in part 1, there exist $x, y \in \mathbb{Z}$ so that $cax + cby = c$. Since $a \mid a$ and $a \mid bc$ we have $a \mid cax + cby$ so $a \mid c$.

■

Exercise. Find integers a, b, c ($a \neq 0$ or $b \neq 0$) so that:

1. $a \mid c$ and $b \mid c$ but $ab \nmid c$.
2. $a \mid bc$ but $a \nmid c$.

Lecture 6 - 19/05

2 Prime numbers

Prime numbers are the building blocks of the integers. They are fundamental, and mysterious. As you will see, we understand some things about them (like that there are infinitely many primes), but there are some basic questions to which we do not know the answer (such as whether or not there are infinitely many pairs of primes of the form p and $p + 2$).

Definition. An integer $p > 1$ is **prime** if its only positive divisors are 1 and p. An integer is **composite** otherwise.

Appendix A has a list of the first 1000 primes. Please let me know if you find any patterns. Let's begin our investigation into primes.

Observe that $4 \mid 60$ and $60 = 6 \cdot 10$. However, $4 \nmid 6$ and $4 \nmid 10$. This may seem suprising, but what's going on here is that since $2 \mid 6$ and $2 \mid 10$ when we combine them we get $2 \cdot 2 \mid 6 \cdot 10$, so we

have $4 \mid 10$. So, the fact that you can have $4 \mid ab$ but $4 \nmid a$ and $4 \nmid b$ is a consequence of the fact that 4 is composite. So, maybe, we shouldn't expect this kind of thing to happen with primes, and indeed it doesn't!

Here is an important observation: If p is prime, its only positive divisors are 1 and p. Therefore $\gcd(p, a)$ is either 1 or p. So, if $p \nmid a$, then $\gcd(p, a) = 1$.

Proposition 11. *Let p be a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$ then we're done, so suppose $p \nmid a$. Since p is not a factor of a, we must have that p and a are coprime. Therefore $p \mid b$ by Proposition 10. ■

Exercise.

- Prove that if $p \mid a_1 \cdots a_t$ for some $a_1, \ldots, a_t \in \mathbb{Z}$, then $p \mid a_i$ for some i.
- Prove that if p is prime and $p \mid a^k$ for some integer $k \geq 0$, then $p^k \mid a^k$.

2.1 The Fundamental Theorem of Arithmetic

We are now ready to prove a very fundamental theorem about numbers, called, well, the Fundamental Theorem of Arithmetic. It really shows why we consider prime numbers to be the building blocks of the integers.

Theorem 12 (Fundamental Theorem of Arithmetic)**.** *Each integer $n > 1$ has a prime-power factorisation*

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

where $p_1, \ldots, p_k$ are distinct primes and $e_1, \ldots, e_k$ are positive integers. Furthermore, other than permuting the factors, this factorisation is unique.

For example, $100 = 5^2 \cdot 2^2$, which we could also write as $100 = 2^2 \cdot 5^2$ or $100 = 2 \cdot 5^2 \cdot 2$. However, whichever way we write 20 as a product of primes, it must contain two 2s and two 5s.

Lecture 7 - 23/05

Let's prove the fundamental theorem of arithmetic!

Proof. For existence we will proceed by induction on n. The base case $n = 2$ is easy, since $n = 2^1$. Now suppose $n > 2$ and every integer k such that $2 \leq k \leq n - 1$ has a prime factorisation. If n is prime, then $n = n^1$ and we're done. If n is composite, then $n = ab$ for some integers $2 \leq a, b \leq n-1$. Therefore a and b have prime factorisations, so $n = ab$ has a prime factorisation (by multiplying together the prime factorisations of a and b).

For uniqueness, we will again induct on n. The base case $n = 2$ is an exercise for the reader, to show that the only prime factorisation of 2 is indeed 2^1. Now, suppose every integer k such that $2 \leq k \leq n - 1$ has a unique prime factorisation (up to permuting the factors). Suppose $n = p_1^{e_1} \cdots p_s^{e_s} = q_1^{f_1} \cdots q_t^{f_t}$ where the p_i are distinct primes, the q_i are distinct primes and the e_i and f_i are positive integers. Since $p_1 \mid q_1^{f_1} \cdots q_t^{f_t}$, we have $p_1 \mid q_j$ for some j. By permuting the q_i, we have $p_1 \mid q_1$ and since q_1 is prime we have $p_1 = q_1$. Then $\frac{n}{p_1} = p_1^{e_1 - 1} p_2^{e_2} \cdots p_s^{e_s} = q_1^{f_1 - 1} q_2^{f_2} \cdots q_t^{f_t}$. However, $2 \leq \frac{n}{p_1} \leq n - 1$ so these two factorisations of $\frac{n}{p_1}$ are the same after permuting the factors. Therefore the original two factorisations of n are the same after the permuting the factors. ■

Great! The fundamental theorem of arithmetic turns out to be outrageously useful for studying divisibility of integers (among other things). Let's take a look at an example.

Example. Let's look at the prime factorisations of all the positive divisors of $2^3 \cdot 3^2 \cdot 5 = 360$. They are

$$\begin{aligned}
1 &= 2^0 \cdot 3^0 \cdot 5^0 \\
2 &= 2^1 \cdot 3^0 \cdot 5^0 \\
4 &= 2^2 \cdot 3^0 \cdot 5^0 \\
8 &= 2^3 \cdot 3^0 \cdot 5^0 \\
3 &= 2^0 \cdot 3^1 \cdot 5^0 \\
6 &= 2^1 \cdot 3^1 \cdot 5^0 \\
12 &= 2^2 \cdot 3^1 \cdot 5^0 \\
24 &= 2^3 \cdot 3^1 \cdot 5^0 \\
9 &= 2^0 \cdot 3^2 \cdot 5^0 \\
18 &= 2^1 \cdot 3^2 \cdot 5^0 \\
36 &= 2^2 \cdot 3^2 \cdot 5^0 \\
72 &= 2^3 \cdot 3^2 \cdot 5^0 \\
5 &= 2^0 \cdot 3^0 \cdot 5^1 \\
10 &= 2^1 \cdot 3^0 \cdot 5^1 \\
20 &= 2^2 \cdot 3^0 \cdot 5^1 \\
40 &= 2^3 \cdot 3^0 \cdot 5^1 \\
15 &= 2^0 \cdot 3^1 \cdot 5^1 \\
30 &= 2^1 \cdot 3^1 \cdot 5^1 \\
60 &= 2^2 \cdot 3^1 \cdot 5^1 \\
120 &= 2^3 \cdot 3^1 \cdot 5^1 \\
45 &= 2^0 \cdot 3^2 \cdot 5^1 \\
90 &= 2^1 \cdot 3^2 \cdot 5^1 \\
180 &= 2^2 \cdot 3^2 \cdot 5^1 \\
360 &= 2^3 \cdot 3^2 \cdot 5^1
\end{aligned}$$

You may notice something about all the prime factorisations - the exponents of the primes are bounded above by the exponents of the primes in the original factorisation. To state the next proposition slickly, we are going to allow exponents of zero on the prime factorisations. This is just so we can take any two numbers and write them as a product of powers of the same set of primes. For example, $6 = 2^1 \cdot 3^1 \cdot 5^0$ and $15 = 2^0 \cdot 3^1 \cdot 5^1$.

Proposition 13. *Let $n = p_1^{e_1} \cdots p_k^{e_k}$ and $m = p_1^{f_1} \cdots p_k^{f_k}$, where the p_i are distinct primes and $e_i, f_i \geq 0$ for all i. Then $m \mid n$ if and only if $f_i \leq e_i$ for all i.*

Proof. This is an exercise. ■

In fact, we can write down formulas for a whole bunch of things in terms of the prime factorisations.

Proposition 14. *Let $a = p_1^{e_1} \cdots p_k^{e_k}$ and $b = p_1^{f_1} \cdots p_k^{f_k}$, where the p_i are distinct primes and $e_i, f_i \geq 0$ for all i. Then*

$$ab = p_1^{e_1+f_1} \cdots p_k^{e_k+f_k}$$
$$a/b = p_1^{e_1-f_1} \cdots p_k^{e_k-f_k}$$
$$\gcd(a,b) = p_1^{\min\{e_1,f_1\}} \cdots p_k^{\min\{e_k,f_k\}}.$$

Proof. The proof of this proposition is also an exercise. ■

Example. Suppose p,q, and r are distinct primes. Then $\gcd(pq^2, qr^2) = q$.

The formula $\gcd(a,b) = p_1^{\min\{e_1,f_1\}} \cdots p_k^{\min\{e_k,f_k\}}$ certainly seems like an easy way to compute the greatest common divisor of two integers, and it is! Provided you already have the prime factorisations of the integers in which you are interested. An attractive feature of the Euclidean algorithm is that you don't need the prime factorisations of a and b to compute $\gcd(a,b)$. An in general, it's rather difficult to compute the prime factorisation of an integer.

Let's push the fundamental theorem of arithmetic a little further.

Proposition 15. *Let $a = p_1^{e_1} \cdots p_k^{e_k}$ where the p_i are distinct primes and e_i is a positive integer for all i. Then a is a perfect square if and only if e_i is even for all i.*

Proof. Suppose $a = b^2$ and the prime factorisation of b is given by $b = p_1^{f_1} \cdots p_k^{f_k}$. Then $a = b^2 = p_1^{2f_1} \cdots p_k^{2f_k}$. Since the prime factorisation of a is unique up to changing the order of the primes, the exponent of each prime is even. Conversely, suppose the exponent on each prime in the prime factorisation of a is even. Then $a = p_1^{2f_1} \cdots p_k^{2f_k} = (p_1^{f_1} \cdots p_k^{f_k})^2$, completing the proof. ■

Lecture 8 - 24/05

Let's keep going, this time to construct infinitely many irrational numbers.

Proposition 16. *If a positive integer m is not a perfect square, then $\sqrt{m}$ is irrational.*

Proof. Suppose $\sqrt{m} = \frac{a}{b}$ is rational, so a and b are integers. We may choose the positive square root and therefore assume a and b are positive integers. Consider the prime factorisations $a = p_1^{e_1} \cdots p_k^{e_k}$ and $b = p_1^{f_1} \cdots p_k^{f_k}$ where the p_i are distinct primes and the e_i are non-negative integers for all i. Then $m = \frac{a^2}{b^2}$ is an integer so $b^2 \mid a^2$. Therefore $2f_i \leq 2e_i$ for all i and we have $m = p_1^{2(e_i-f_i)} \cdots p_k^{2(e_k-f_k)}$. Since each exponent in the prime factorisation of m is even, m is a perfect square. ■

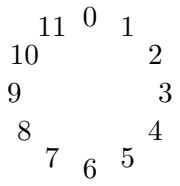
So, for example, $\sqrt{24}$ is irrational!

Exercise. Let a and n be positive integers. When is $a^{\frac{1}{n}}$ rational?

3 Modular Arithmetic

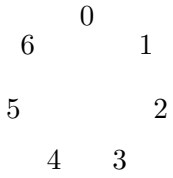
Modular arithmetic, sometimes called clock arithmetic, is a way of doing mathematics while focusing only on remainders. For example, suppose you knew today was Wednesday (which it happens to be as I write this!). What day will it be 22 days from now? The answer is Thursday. A quick way to see this is to note that we only care about what the remainder of 22 is when divided by 7. After 21 days (which is a multiple of 7), it will be Wednesday again, so in 22 days it will be Thursday.

Similarly, we cn do arithmetic on a clock with 12 numbers (just like a regular clock). We will call this clock $\mathbb{Z}_{12}$. It looks like this:



In $\mathbb{Z}_{12}$ we can do addition and multiplication as usual, except we identify some numbers (like 13 is the same as 1, and 12 is the same as 0). For example, $2+3=5$ and $7+8=3$ and $4\cdot 5=8$. We will formalise all of this soon, so take these equations with a grain of salt (the statement $7+8=3$ taken out of context could get me fired!).

Let's do some more examples, this time in $\mathbb{Z}_7$:



Here $2+1=3$, $-2=5$, and $3\cdot 4=12=5$. What's really going on here is that we are associating all numbers that have a remainder of 3 when divided by 7, say, with the number 3 on the clock. Curiously, no harm seems to come to us if we do our arithmetic with different numbers that have the same remainder. For example, $5+4=9=2$, but we know $5=-2$ and $4=-3$. So we could instead have done $(-2)+(-3)=-5=2$. Either way, we get the same answer!

Lecture 9 - 26/05

Let's do one more example, which is maybe a little more familiar to us, that of $\mathbb{Z}_2$. $\mathbb{Z}_2$ as a clock only has two things, 0 and 1. We can think of the 0 as all the numbers which have a remainder of 0 when divided by 2 (ie all the even numbers) and 1 as all the numbers that have a remainder of 1 when divided by 2 (ie all the odd numbers). Since there are only two things in $\mathbb{Z}_2$, it's not too onerous to draw out the addition and multiplication tables. Let's put them alongside tables which summarise what happens when you add and multiply odd and even numbers.

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

$+$	even	odd
even	even	odd
odd	odd	odd

$\times$	even	odd
even	even	even
odd	even	odd

Notice anything? The thing I'm trying to hint at is that the remainder of a and b when divided by 2 is all that matters when figuring out the remainder of $a+b$ and ab when divided by 2. Even better, in the previous sentence, I could have replaced 2 with n and it would still be true. The next section will be all about formalising and proving these ideas.

3.1 Congruences

The first step to formalising is to treat all integers which give the same remainder when divided by n as equal.

Definition. Let n be a positive integer and let a and b be any integers. We say a **is congruent to** b **modulo** n (or simply **mod** n), and write $a \equiv b \pmod{n}$, if $n \mid a-b$. If it is clear from context what n is, we may simply write $a \equiv b$.

You will find many different ways of denoting that a is congruent to b mod n in textbooks and online. Here are some: $a \equiv_n b$, $a \equiv b \mod n$, or $a \equiv b \mod (\mathrm{n})$. Sometimes, instead of saying a is congruent to b mod n, it is said that a is a **residue** of b mod n.

"But wait," I hear you object, "you lead us to believe remainders were important, not this strange n-divides-the-difference business!"

Well, I'm glad you brought that up.

Proposition 17. *Let n be a positive integer and $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n.*

Proof. Suppose $a \equiv b \pmod{n}$ and write $b = qn + r$ as per the division algorithm (so $0 \leq r < n$). Since $n \mid a - b$ we have $a = kn + b$ for some $k \in \mathbb{Z}$. Therefore

$$a = kn + b = kn + qn + r = (k+q)n + r$$

so a has a remainder of r when divided by n, which is the same remainder as b.

Conversely, suppose $a = qn + r$ and $b = tn + r$ for some integers q, t and $0 \leq r < n$. Then $a - b = (q-t)n$ so $a \equiv b \pmod{n}$. ■

As always, whenever we see an if and only if statement, we can now treat either side of the statement as the definition. The next proposition is not terribly difficult to prove, but it is vitally important. It tells us that the relation "congruent mod n" is an equivalence relation. See Appendix B for a crash course on equivalence relations.

Proposition 18. *Let n be a positive integer. Then for all $a, b, c \in \mathbb{Z}$ we have*

- $a \equiv a \pmod{n}$,
- *If* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$, *and*
- *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$.

Proof. The proof is left as an exercse. ■

As explained in Appendix B, the equivalence classes partition the integers into sets. The equivalence classes here are called congruence classes mod n.

Definition. Let n be a positive integer. For $a \in \mathbb{Z}$, define the **congruence class of** a **mod** n as the set

$$[a] = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}.$$

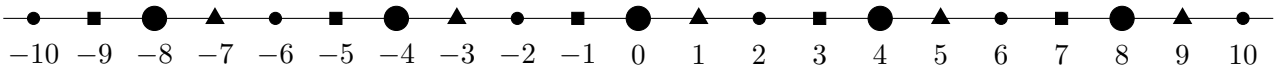
Lecture 10 - 29/05

Unwrapping the definitions we have $[a] = [b]$ if and only if $a \equiv b \pmod{n}$.

Example. When $n = 4$ we have exactly 4 congruence classes. They are

$$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$[2] = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$[3] = \{\ldots, -5, -1, 3, 7, 11, \ldots\}.$$

It turns out that $[4] = [0]$, $[5] = [1]$ and so on (you should check these claims for your self!). Visualising the congruence classes on the number line we have



The ●s give the set [0], the ▲s are [1], the ●s are [2] and the ■s are [3]. Notice that every integer belongs to exactly one congruence class, which is exactly what it means for the congruence classes to partition $\mathbb{Z}$.

3.2 The integers mod n

At the beginning of this section we played around with a clock with 7 things on it, and we called it $\mathbb{Z}_7$. We are now ready to formalise those ideas. It turns out that the set of congruence classes mod 7 are what should go on the clock with 7 things.

Definition. Let n be a positive integer. The set of all congruence classes mod n is called **the integers mod** n and is denoted $\mathbb{Z}_n$.

So, for example, $\mathbb{Z}_3 = \{[0], [1], [2]\}$. We want to do arithmetic on $\mathbb{Z}_n$, in particular, we wish to add and multiply. Addition and multiplication on $\mathbb{Z}$ are operations that eat two elements of $\mathbb{Z}$ and spit out another element of $\mathbb{Z}$. Similarly, we want addition and multiplication on $\mathbb{Z}_n$ to eat two elements of $\mathbb{Z}_n$ (which are subsets of $\mathbb{Z}$) and spit out an element of $\mathbb{Z}_n$ (which is a subset of $\mathbb{Z}$).

Definition. Let n be a positive integer and define addition and multiplication on $\mathbb{Z}_n$ by

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

So, for example, in $\mathbb{Z}_7$ we have $[3] + [5] = [8]$ but remember, $[8] = [1]$. So we could have just written $[3] + [5] = [1]$ which is what we want to do on the clock! Similarly, $[3][5] = [15] = [1]$.

There is something a little dodgy going on with the definition of addition and multiplication, which is that the definition appears to depend on what we call each equivalence class. Let's take $\mathbb{Z}_7$ again as an example. We have $[3] + [5] = [8]$, but what if we decided to write $[-4]$ or $[10]$ instead of $[3]$? Well, let's check: We have $[-4] + [5] = [1]$ and since $[1] = [8]$, all is well in the world and the result of the sum didn't depend on us writing $[3]$ as $[3]$ and not as $[-4]$. Similarly $[10] + [5] = [15] = [8]$. Phew! It would appear that no harm comes to us if we decide to call $[3]$ by any other of its infinitely many names. While a few examples are good, this should be checked!

Proposition 19. *Let n be a positive integer. If $[a] = [a']$ and $[b] = [b']$, then $[a] + [b] = [a'] + [b']$ and $[a][b] = [a'][b']$.*

Proof. If $[a] = [a']$ and $[b] = [b']$ then $n \mid a - a'$ and $n \mid b - b'$. Then $n \mid (a - a') + (b - b')$ so $n \mid (a+b) - (a'+b')$. Alas, $[a+b] = [a'+b']$. For multiplication we have $a = a' + kn$ and $b = b' + tn$ for some $k, t \in \mathbb{Z}$. Then $ab = (a' + kn)(b' + tn) = a'b' + n(kb' + ta' + nkt)$ so $[ab] = [a'b']$. ■

Fantastic! No harm will come to us if in $\mathbb{Z}_9$ we decide to write $[2]$ as $[-7]$ or $[8]$ as $[-1]$.

Although no harm will come to you if you change the name of congruence classes when doing multiplication or addition (and since subtraction is just adding negatives, no harm comes while subtracting either), harm will come to you if you mess around with powers! For example, in $\mathbb{Z}_3$ $[2]^4 = [2][2][2][2] = [16] = [1]$ but $[2]^1 = [2]$. Powers are just an instruction for how many times you should multiply something by itself, which is not something that can be changed!

Exercise. Prove or disprove: Let n be a positive integer. Assume $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, and suppose $b, b' > 0$. Then $a^b \equiv a'^{b'} \pmod{n}$.

Now that we've checked the details to make sure addition and multiplication are well-defined in $\mathbb{Z}_n$, let's bask in our newfound glory.

Example. Let's compute the remainder of $(32)(33)$ when divided by 37. In $\mathbb{Z}_{37}$ we have $[(32)(33)] = [32][33] = [-5][-4] = [20]$. Therefore $(32)(33) \equiv 20 \pmod{37}$ so the remainder is 20.

Example. Let's compute $[3]^8$ in $\mathbb{Z}_{13}$. We have

$$\begin{aligned} &[3]^2 = [9] \\ \Rightarrow &[3]^3 = [3]^2[3] = [9][3] = [27] = [1] \\ \Rightarrow &[3]^6 = ([3]^3)^2 = [1] \\ \Rightarrow &[3]^8 = [3]^6[3]^2 = [1][9] = [9]. \end{aligned}$$

So, in particular, we know that 3^8 leaves a remainder of 9 when divided by 13.

Example. Let's prove that for all $a \in \mathbb{Z}$, $a(a+1)(a+2)$ is divisible by 6. This is equivalent to showing $[a(a+1)(a+2)] = [a]([a]+[1])([a]+[2]) = [0]$ in $\mathbb{Z}_6$. So, we just have to check all the possible values of $[a]$ in $\mathbb{Z}_6$. Let's do it!

If $[a] = [0]$ we have $[0]([0]+[1])([0]+[2]) = [0]$.
If $[a] = [1]$ we have $[1]([1]+[1])([1]+[2]) = [1][2][3] = [6] = [0]$.
If $[a] = [2]$ we have $[2]([2]+[1])([2]+[2]) = [2][3][4] = [0][4] = [0]$.
If $[a] = [3]$ we have $[3]([3]+[1])([3]+[2]) = [3][4][5] = [0]$.
If $[a] = [4]$ we have $[4]([4]+[1])([4]+[2]) = [4][5][0] = [0]$.
Finally, if $[a] = [5] = [-1]$ we have $[-1]([-1]+[1])([-1]+[2]) = [-1][0][1] = [0]$.
Since $[a]([a]+[1])([a]+[2]) = [0]$ for all $[a] \in \mathbb{Z}_6$, $a(a+1)(a+2) \equiv 0 \pmod{6}$ for all $a \in \mathbb{Z}$.

The fantastic thing about the previous example is that it turns checking infinitely many things (namely every integer, which is not possible) into a problem which needs you to check finitely many things! Although sometimes the finite number is large, given enough time and money you can always just do it.

Lecture 11 - 31/05

Exercise. Let $n = p_1^{e_1} \cdots p_k^{e_k}$ where the p_i are distinct primes and $e_i > 0$ for all i. Prove that $a \equiv b \pmod{n}$ if and only if $a \equiv b \pmod{p^{e_i}}$ for all i.

With this exercise in hand, the previous example could have been achieved by simply checking $[a]([a]+[1])([a]+[2])=[0]$ in $\mathbb{Z}_2$ for all $[a]\in\mathbb{Z}_2$ and $[a]([a]+[1])([a]+[2])=[0]$ in $\mathbb{Z}_3$ for all $[a]$ in $\mathbb{Z}_3$.

Example. Let's show there is no integer solution to the equation $x^2=2736483623$, that is we want to show 2736483623 is not a perfect square.

We will approach this problem in $\mathbb{Z}_4$ (it will become clear as we progres as to why we chose 4). If there is an $x\in\mathbb{Z}$ so that $x^2=2736483623$, then it is true that $[x]^2=[2736483623]$ in $\mathbb{Z}_4$ (in fact it's true in $\mathbb{Z}_n$ for any n). Let's take a look at the possible values of $[x]^2$.

If $[x]=[0]$ then $[x]^2=[0]$. If $[x]=[\pm1]$, then $[x]^2=[1]$. If $[x]=[2]$ then $[x]^2]=[0]$. Therefore in $\mathbb{Z}_4$, $[x]^2$ is either $[0]$ or $[1]$.

However, $[2736483623]=[23]+[100][27364836]=[23]=[3]$ and $[3]$ is not one of the possible values of $\mathbb{Z}_4$ obtained by a perfect square. Therefore 2736483623 is not a perfect square.

It is not always clear which $\mathbb{Z}_n$ to investigate. Which one to go for is part of the fun, and you get better at it with experience. Often however, it's just trial and error!. You may often choose an n that's not helpful.

In the previous example, if we had looked at $\mathbb{Z}_{11}$ we would have $[2736483623]=[5]$ but $[4]^2=[5]$. This tells us there is an $[x]\in\mathbb{Z}_{11}$ so that $[x]^2=[2736483623]$, but we cannot conclude anything about whether or not there is an $x\in\mathbb{Z}$ so that $x^2=2736483623$.

The previous example was a special case of showing that a polynomial does not have any integer roots. Since polynomials are just made up of addition and multiplication, they are perfect equations to probe using modular arithmetic.

Proposition 20. *Let $f(x)=a_nx^n+\cdots+a_1x+a_0$ be a polynomial with integer coefficients, and let n be a positive integer. If $[b]=[c]$ in $\mathbb{Z}_n$, then $[a_n][b]^n+\cdots+[a_1][b]+[a_0]=[a_n][c]^n+\cdots+[a_1][c]+[a_0]$ in $\mathbb{Z}_n$.*

Proof. This is an exercise. ■

Exercise. Show that the polynomial x^5-x^2+x-3 has no integer roots.

Exercise. Is it true that if a polynomial with integer coefficients $f(x)$ has a root in $\mathbb{Z}_n$ for all primes n, then $f(x)$ has a root in $\mathbb{Z}$?

Sometimes when solving an equation in $\mathbb{Z}_n$, it's helpful to split it up into a few different equations.

Lemma 21. *Let m and n be positive coprime integers. Then $a\equiv b \pmod{mn}$ if and only if $a\equiv b \pmod{n}$ and $a\equiv b \pmod{m}$.*

Proof. Suppose $a\equiv b \pmod{mn}$. Then $mn\mid a-b$ and since $m\mid mn$ and $n\mid mn$, $m\mid a-b$ and $n\mid a-b$. Conversely, suppose $a\equiv b \pmod{m}$ and $a\equiv b \pmod{n}$, so $mk=a-b$ and $nt=a-b$ for some $k,t\in\mathbb{Z}$. Since $\gcd(n,m)=1$, there exist $u,v\in\mathbb{Z}$ so that $mu+nv=1$. Multiplying both sides by $a-b$ gives

$$\begin{aligned} & (a-b)mu+(a-b)nv=a-b \\ \implies \quad & (nt)mu+(mk)nv=a-b \\ \implies \quad & nm(tu+kv)=a-b \end{aligned}$$

Thereore $a\equiv b \pmod{mn}$, completing the proof. ■

Of course, as is often the case with results that involve coprime integers and their product, there is a generalisation to all pairs of integers, but you have to replace their product with their least common multiple.

Exercise. Prove that for all positive integers m, n, $a \equiv b \pmod{\operatorname{lcm}(m,n)}$ if and only if $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$.

Let's use this to our advantage.

Exercise. Show that for all $a \in \mathbb{Z}$, $2 \mid a(a+1)(a+2)$ and $3 \mid a(a+1)(a+2)$. Conclude that for all $a \in \mathbb{Z}$, $6 \mid a(a+1)(a+2)$.

Lecture 12 - 02/06

4 Inverses and Euler's Totient Function

In the previous section we built up the required machinery to treat $\mathbb{Z}_n$ as an object, like the integers, which comes with its own addition and multiplication. In mathematics, such an object is called a **ring**. We won't give the formal definition here, but a ring is a set endowed with addition and multiplication satisfying certain desirable properties.

A couple of the important properties are the existence of additive and multiplicative identities, which we usually call 0 and 1. The additive identity 0 has the property that $0 + a = a$ for all a in the ring. The multiplicative identity 1 has the property that $1a = a$ for all a in the ring.

Exercise. Let n be a positive integer.

- Which element of $\mathbb{Z}_n$ plays the role of 0 (the additive identity)?
- Which element of $\mathbb{Z}_n$ is $-[a]$? In a ring, $-x$ is the element with the property that $(-x)+x = 0$.
- Which element of $\mathbb{Z}_n$ plays the role of 1 (the multiplicative identity)?
- When element of $\mathbb{Z}_n$ is $[a]^{-1}$? In a ring x^{-1} is the element with the property that $x^{-1}x = 1$.

Let's investigate the last part of this exercise, finding inverses in $\mathbb{Z}_n$.

4.1 Units in $\mathbb{Z}_n$

Consider $\mathbb{Z}_7$. What is the inverse of $[2]$? Now, it's not even clear that one exists. After all, in $\mathbb{Z}$ we know 0 doesn't have an inverse (in fact the only elements with inverses are ± 1). However, if $[2]^{-1}$ does exist, it has the property $[2][2]^{-1} = [1]$. A quick check through the elements of $\mathbb{Z}_7$ gives us $[2]^{-1} = [4]$ since $[2][4] = [1]$. Let's write down all the inverses in $\mathbb{Z}_7$.

x	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
x^{-1}	$*$	$[1]$	$[4]$	$[5]$	$[2]$	$[3]$	$[6]$

So, just like the rational numbers $\mathbb{Q}$, every non-zero element has an inverse! Let's do another one, $\mathbb{Z}_{12}$.

x	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$	$[11]$
x^{-1}	$*$	$[1]$	$*$	$*$	$*$	$[5]$	$*$	$[7]$	$*$	$*$	$*$	$[11]$

Curious! Only some of the elements in $\mathbb{Z}_{12}$ have inverses. From these two examples you may be able to take a guess as to which elements in $\mathbb{Z}_n$ have inverses.

Definition. An element $x \in \mathbb{Z}_n$ is a **unit** if it has a multiplicative inverse. The set of all units in $\mathbb{Z}_n$ is called the **group of units mod** n and is denoted $\mathbb{Z}_n^*$.

So, for example, $\mathbb{Z}_{12}^* = \{[1], [5], [7], [11]\}$.

Theorem 22. *Let n be a positive number. An element $[a] \in \mathbb{Z}_n$ is a unit if and only if* $\gcd(a, n) = 1$.

Proof. If $\gcd(a, n) = 1$ there exist $x, y \in \mathbb{Z}$ so that $ax + ny = 1$, so $ax \equiv 1 \pmod{n}$. Therefore there exists $x \in \mathbb{Z}$ so that $[a][x] = [1]$ in $\mathbb{Z}_n$ and $[a] \in \mathbb{Z}_n^*$. Conversely, suppose $[a][x] = [1]$ in $\mathbb{Z}_n$ for some $x \in \mathbb{Z}$. Then $ax = 1 + ny$ for some $y \in \mathbb{Z}$, which rearranges to $ax - ny = 1$ Therefore $\gcd(a, n) = 1$, completing the proof. ■

From this theorem we get the next quick consequence.

Corollary 23. *Let p be a prime. Then $[x] \in \mathbb{Z}_p^*$ if and only if $[x] \neq [0]$.*

Proof. A fun, for some definition of fun, exercise. ■

This corollary tell us that $\mathbb{Z}_p$ acts a lot like $\mathbb{Q}$ or $\mathbb{R}$ in that every non-zero element is invertible. These are examples of fields.

Definition. We say $\mathbb{Z}_n$ is a **field** if every non-zero element is a unit.

Exercise. Prove that if $\mathbb{Z}_n$ is a field, then n is prime.

"This is all well and good," I hear you start, "but who cares?" Well, let me tell you! The existence of inverses allows us to do division (because division is just multplication by an inverse). In the real numbers $\mathbb{R}$ we were always taught "you can divide by anything except for 0. Dividing by 0 is bad!" The reason we were taught this is that every element of $\mathbb{R}$ has an inverse except for zero. This means we can divide by $a \neq 0$ by simply multiplying by a^{-1}.

Example. Suppose we want to solve the congruence $3x \equiv 4 \pmod{7}$. This is the same as solving $[3][x] = [4]$ in $\mathbb{Z}_7$. We can simply divide both sides by [3], which really means multiplying both sides by $[3]^{-1} = [5]$. This gives $[5][3][x] = [5][4]$ implying $[x] = [20] = [6]$. So the solution to the original congruence is $x \equiv 6 \pmod{7}$.

4.2 Euler's Theorem and a not-big theorem of Fermat

We saw in Section 3.2 that modular arithmetic can help us deal with powers. More specifically, we easily computed that $[3]^8 = [9]$ in $\mathbb{Z}_{13}$.

Let's explore a little more. Suppose we needed to find $[3]^{100}$ in $\mathbb{Z}_{13}$. Let's write out some powers of [3] in $\mathbb{Z}_{13}$.

n	x^n
1	[3]
2	[9]
3	[1]
4	[3]
5	[9]
6	[1]
7	[3]
8	[9]
9	[1]

Let's stop for a moment and stare at this table. It's repeating! Since a [1] appears, we should absolutely expect this to happen. After all if $[3]^k = [1]$, then $[3]^{k+1} = [3]^k[3] = [3]$, taking us back to the start. In this case, we have that if $3 \mid k$, then $[3]^k = [1]$. Therefore

$$[3]^{100} = [3]^{99}[3] = [1][3] = [3]$$

in $\mathbb{Z}_{13}$. Let's see if this kind of repeating patterns happens more generally.

Lecture 13 - 05/06

Here are power tables for the elements of $\mathbb{Z}_5$, $\mathbb{Z}_7$ and $\mathbb{Z}_9$. To make things easier to read, I will simply write $[a]$ as a.

$\mathbb{Z}_5$	0	1	2	3	4
x^1	0	1	2	3	4
x^2	0	1	4	4	1
x^3	0	1	3	2	4
x^4	0	1	1	1	1
x^5	0	1	2	3	4
x^6	0	1	4	4	1

$\mathbb{Z}_7$	0	1	2	3	4	5	6
x^1	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1
x^3	0	1	1	6	1	6	6
x^4	0	1	2	4	4	2	1
x^5	0	1	4	5	2	3	6
x^6	0	1	1	1	1	1	1
x^7	0	1	2	3	4	5	6
x^8	0	1	4	2	2	4	1

$\mathbb{Z}_9$	0	1	2	3	4	5	6	7	8
x^1	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1
x^3	0	1	8	0	1	8	0	1	8
x^4	0	1	7	0	4	4	0	7	1
x^5	0	1	5	0	7	2	0	4	8
x^6	0	1	1	0	1	1	0	1	1
x^7	0	1	2	0	4	5	0	7	8
x^8	0	1	4	0	7	7	0	4	1

There is a myriad of things to discover among these tables, and we will return to them at various points in the course. In fact they're so important I insist you do the following exercise.

Exercise (**Super important!!**)**.** Create power tables for $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$, $\mathbb{Z}_{13}$ and $\mathbb{Z}_{17}$. Stare at them all and look for patterns. Write down anything you notice and try to prove any conjectures you may have. Keep these tables safe and accessible for the rest of the course.

Let's pay attention to the 4th powers in the first power table above, and the 6th powers in the other two. All those rows only consist of 0s and 1s. Even better, the 1s correspond exactly to the units. Let's rewrite these tables, but this time only for the units. Also, we know that once any column gets to a 1, it just repeats, so we'll stop if we see a row of 1s.

$\mathbb{Z}_5^*$	1	2	3	4
x^1	1	2	3	4
x^2	1	4	4	1
x^3	1	3	2	4
x^4	1	1	1	1

$\mathbb{Z}_7^*$	1	2	3	4	5	6
x^1	1	2	3	4	5	6
x^2	1	4	2	2	4	1
x^3	1	1	6	1	6	6
x^4	1	2	4	4	2	1
x^5	1	4	5	2	3	6
x^6	1	1	1	1	1	1

$\mathbb{Z}_9^*$	1	2	4	5	7	8
x^1	1	2	4	5	7	8
x^2	1	4	7	7	4	1
x^3	1	8	1	8	1	8
x^4	1	7	4	4	7	1
x^5	1	5	7	2	4	8
x^6	1	1	1	1	1	1

So, it would appear that if we only look at the units in $\mathbb{Z}_n$, some power of all of the units is 1. Even better, it appears that the special power is equal to the number of units! It would be a cruel cruel joke if this were just a coincidence.

Before we write down this conjecture and try to prove it, we need to introduce the totient function.

Definition. Define **Euler's totient function** (or **Euler's phi function**) to be the function defined by $\varphi(n) = |\mathbb{Z}_n^*|$ for any positive integer n.

Theorem 24 (Euler's Theorem)**.** *Let n be a positive integer, and let $[a] \in \mathbb{Z}_n^*$. Then $[a]^{\varphi(n)} = [1]$ in $\mathbb{Z}_n$.*

Before we embark on the proof, we will need an interesting fact about the group of units. To demonstrate this fact, let's look at the multiplication table for $\mathbb{Z}_5^*$ (again, let's abuse notation and write $[a]$ as a):

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

There are two things worth noticing here. First, every entry in the table is again in $\mathbb{Z}_n^*$.

Exercise. Prove that if $[a], [b] \in \mathbb{Z}_n^*$, then $[a][b] \in \mathbb{Z}_n^*$.

The second thing is that every row and every column contains all the elements of $\mathbb{Z}_5^*$ exactly once! Or, more formally:

Lemma 25. *Let $[a] \in \mathbb{Z}_n^*$. Then the function $\psi : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ given by $\psi([b]) = [a][b]$ is a bijection.*

Proof. Note that since the product of two units is a unit, ψ is well-defined (that is $\psi([b]) \in \mathbb{Z}_n^*$ for every $[b] \in \mathbb{Z}_n^*$).

For injectivity, suppose $\psi([b]) = \psi([c])$, so $[a][b] = [a][c]$. Then since $[a]$ is a unit, multiplying both sides by $[a]^{-1}$ gives $[b] = [c]$ and ψ is injective. For surjectivity, let $[c] \in \mathbb{Z}_n^*$. Since $[a]^{-1}$ and $[c]$ are units, so is $[a]^{-1}[c]$. Then $\psi([a]^{-1}[c]) = [a][a]^{-1}[c] = [c]$, so ψ is surjective, and thus a bijection. ■

We are now ready to prove Euler's theorem.

Proof of Euler's Theorem. Let $\mathbb{Z}_n^* = \{[u_1], \ldots, [u_{\varphi(n)}]\}$. By Lemma 25, for all $[a] \in \mathbb{Z}_n^*$ we have $\mathbb{Z}_n^* = \{[a][u_1], \ldots, [a][u_{\varphi(n)}]\}$.

Consider the product $[u_1][u_2]\cdots[u_{\varphi(n)}]$. Let $[a] \in \mathbb{Z}_n^*$. We have

$$[u_1][u_2]\cdots[u_{\varphi(n)}] = ([a][u_1])([a][u_2])\cdots([a][u_{\varphi(n)}]) = [a]^{\varphi(n)}[u_1][u_2]\cdots[u_{\varphi(n)}].$$

Since each $[u_i]$ is a unit, so is the product $[u_1][u_2]\cdots[u_{\varphi(n)}]$. So we can cancel the product from the equation above to get $[a]^{\varphi(n)} = [1]$. ■

When n is a prime we recover Fermat's Little Theorem.

Corollary 26 (Fermat's Little Theorem)**.** *Let p be a prime and suppose $a \in \mathbb{Z}$ with $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Example. We have $\mathbb{Z}_{15}^* = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$ so $\varphi(15) = 8$. Therefore $15 \mid 7^{8088} - 1$. I'm sure it was keeping you up at night, but now you know that $7^{8088} - 1$ is indeed a multiple of 15.

Exercise. Let p and q be distinct primes, and let $a \in \mathbb{Z}$ be such that $p \nmid a$ and $q \nmid a$.

1. Prove that $a^{p^2-p} \equiv 1 \pmod{p^2}$.
2. Prove that $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

4.3 Euler's Totient Function

As we saw in the previous section, being able to compute the totient function $\varphi(n)$ is useful! Let's investigate this function some more, and we will see that it shares lots of properties with lots of important functions in number theory (called multiplicative functions).

Let's begin with a small example.

Example. Let's work out $\varphi(49)$. So we're looking for all integers n coprime to 49 such that $0 \leq n < 49$. The prime factorisation of 49 is 7^2, so $\gcd(n, 49) = 1$ iff $7 \nmid n$. There are exactly 7 multiples of 7 from 0 to 48, so $\varphi(49) = 49 - 7 = 41$.

This kind of argument works well in general for powers of primes.

Proposition 27. *Let p be a prime and e a positive integer. Then $\varphi(p^e) = p^e - p^{e-1}$.*

Proof. The number of integers in $\{0, \ldots, p^e - 1\}$ coprime to p^e is exactly the number of integers in $\{0, \ldots, p^e - 1\}$ not divisible by p. There are p^{e-1} multiples of p in $\{0, \ldots, p^e - 1\}$ so $\varphi(p^e) = p^e - p^{e-1}$. ■

In general, if we have a function defined on the positive integers and we know how it behaves for prime powers, and for products of coprime integers, then by looking at prime factorisations, we know how the function behaves for all positive integers. With that in mind, let's shift our focus to computing $\varphi(mn)$ where $\gcd(m, n) = 1$.

Let's look at the case $m = 9$ and $n = 5$. We want to count the number of integers in $\{0, \ldots, 44\}$ that are coprime to 45. Let's arrange these integers in an array as follows.

0	**1**	**2**	3	**4**	5	6	**7**	**8**
9	10	**11**	12	**13**	**14**	15	**16**	**17**
18	**19**	20	21	**22**	**23**	24	25	**26**
27	**28**	**29**	30	**31**	**32**	33	**34**	35
36	**37**	**38**	39	40	**41**	42	**43**	**44**

The **boldface blue** entries represent the integers coprime to 45.

There are three things to notice in this array.

- Each column corresponds to a congruence class in $\mathbb{Z}_9$.
- In each column, every congruence class of $\mathbb{Z}_5$ appears exactly once. For example, in the column corresponding to $[1]$ in $\mathbb{Z}_9$, we have $1, 10, 19, 28, 37$. Intriguingly, $\mathbb{Z}_5 = \{[1], [10], [19], [28], [37]\}$.
- The **boldface blue** integers are precisely those that are coprime to both 5 and 9.

With these observations, let's figure out an expression for $\varphi(45)$ in terms of $\varphi(9)$ and $\varphi(5)$. Since the columns correspond to elements of $\mathbb{Z}_9$, our desired integers must appear in columns corresponding to elements of $\mathbb{Z}_9^*$ (since these are precisely the integers coprime to 9). There are $\varphi(9) = 6$ such columns. In each of these columns, since every element of $\mathbb{Z}_5$ is represented precisely once, there are exactly $\varphi(5) = 4$ integers which are coprime to 5. So there are $\varphi(9)$ columns with $\varphi(5)$ integers coprime to both 9 and 5 (and thus 45) in each column, giving $\varphi(45) = \varphi(9)\varphi(5) = 24$.

Lecture 15 - 09/06

Let's prove that this kind of argument works in general.

Lemma 28. *Let $a, m, n \in \mathbb{Z}$. We have* $\gcd(a, m) = 1$ *and* $\gcd(a, n) = 1$ *if and only if* $\gcd(a, mn) = 1$.

Proof. Suppose $\gcd(a, mn) = 1$, so there exist $u, v \in \mathbb{Z}$ such that $au + mnv = 1$. Then $a(u) + m(nv) = 1$ and $a(u) + n(mv) = 1$ so $\gcd(a, m) = \gcd(a, n) = 1$. Conversely, suppose $\gcd(a, m) = \gcd(a, n) = 1$. Therefore there are $w, x, y, z \in \mathbb{Z}$ so that $aw + mx = 1$ and $ay + nz = 1$. Multiplying these equations gives

$$\begin{aligned} (aw + mx)(ay + nz) &= 1 \\ \implies a(awy + wnz + mxy) + mn(xz) &= 1 \end{aligned}$$

and we can conclude $\gcd(a, mn) = 1$. ■

Good! This lemma tells us that to count the integers coprime to mn, we need to count the integers that are coprime to m and n.

Now, suppose we have an $m \times n$ array as above with $\gcd(m, n) = 1$. We need that every column contains every element of $\mathbb{Z}_n$. The next lemma will be prove useful for this.

Lemma 29. *Let m and n be coprime positive integers. Let $c \in \mathbb{Z}$. Then the function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $f([a]) = [a][m] + [c]$ is a bijection.*

Proof. Since $\gcd(m, n) = 1$, $[m]^{-1}$ exists. We will show that the function $g : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $g([a]) = [m]^{-1}([a] - [c])$ satisfies $gf([a]) = fg([a]) = [a]$ for all $[a] \in \mathbb{Z}_n$. We have

$$gf([a]) = g([a][m] + [c]) = [m]^{-1}(([a][m] + [c]) - [c]) = [a] + [m]^{-1}[c] - [m]^{-1}[c] = [a]$$

and

$$fg([a]) = f([m]^{-1}([a] - [c])) = [m]([m]^{-1}([a] - [c])) + [c] = [a] - [c] + [c] = [a].$$

Therefore f is a bijection. ■

Now let's prove that $\varphi(mn) = \varphi(m)\varphi(n)$ if $\gcd(m, n) = 1$.

Proposition 30. *Let m and n be positive coprime integers. Then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. We want to count the number of integers in $\{0, 1, \ldots, mn - 1\}$ that are coprime to both m and n. We will write this set as

$$\{j + mi : 0 \leq j \leq m - 1, 0 \leq i \leq n - 1\}.$$

If we want to think of the array from the previous examples, the entry $j + mi$ is in the ith row and jth column, so the array has n rows and m columns.

Fix t such that $0 \leq t \leq m - 1$ and define the set $C_t = \{t + mi : 1 \leq i \leq n - 1\}$ (this is the column corresponding to the congruence class of $[t] \in \mathbb{Z}_m$).

Since $\gcd(m, j + mi) = \gcd(m, j)$, the integers that are coprime to m are precisely those in the columns C_t where $\gcd(m, t) = 1$. There are exactly $\varphi(m)$ such choices of t.

For a fixed t, we can write

$$C_t = \{t + m(0), t + m(1), t + m(2), \ldots, t + m(n - 1)\}.$$

Since $\gcd(m, n) = 1$, by Lemma 29 there is a bijection $f : \mathbb{Z}_n \to \mathbb{Z}_n$ such that $f([i]) = [t + m(i)]$. Therefore C_t contains exactly one representative of each congruence class in $\mathbb{Z}_n$, or equivalently,

$\{[t+m(0)],[t+m(1)],[t+m(2)],\ldots,[t+m(n-1)]\} = \mathbb{Z}_n$. We can conclude that each set C_t contains $\varphi(n)$ integers coprime to n.

There are $\varphi(m)$ values of t so that $\gcd(k,m)=1$ if and only if $k \in C_t$. Also, each C_t contains exactly $\varphi(n)$ elements coprime to n. Therefore there are $\varphi(n)\varphi(m)$ integers coprime to mn, so $\varphi(n)\varphi(m) = \varphi(nm)$. ■

Propositions 27 and 30 allow us to compute $\varphi(n)$ for any integer n.

Theorem 31. *Suppose a positive integer has prime factorisation $n = p_1^{e_1}\cdots p_k^{e_k}$ where the p_i are distinct prime factors and $e_i > 0$ for all i. Then*

$$\varphi(n) = \prod_{i=1}^{k}\left(p_i^{e_i} - p_i^{e_i-1}\right) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i-1) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).$$

Proof. Note that if p and q are distinct primes, then $\gcd(p^e, q^f) = 1$. With this in mind, the proof is left as an exercise (proceed by induction on k). ■

We may also write

$$\varphi(n) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

which means the product is taken over all primes dividing n.

Lecture 16 - 12/06

Example. We have $120 = 2^3\cdot 3\cdot 5$ so $\varphi(120) = 120(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 120(\frac{1}{2})(\frac{2}{3})(\frac{4}{5}) = 32$.

Exercise. Show there are integers n with $\varphi(n) = 2, 4, 6, 8, 10$, and 12, but not 14.

We finish our study of the totient function with an important property that will rear its head again as the course goes on.

The function $\varphi(n)$ counts the number of integers a in $\{0,\ldots,n-1\}$ that have $\gcd(a,n)=1$. Those of you with a keen eye will notice that in general, 1 is not the only possible value for $\gcd(a,n)$. Why don't we count the others? Great question. Let's count them for $n=12$.

For 12, the possible values of $\gcd(a,12)$ are precisely the positive divisors of 12. That is, $\gcd(a,12) \in \{1,2,3,4,6,12\}$ for all $a \in \mathbb{Z}$. Let's count how many integers a in $\{0,\ldots,11\}$ have each of these greatest common divisors with 12.

$\gcd(a,12)$	a	How many a?
1	1,5,7,11	4
2	2,10	2
3	3,9	2
4	4,8	2
6	6	1
12	0	1

It's not so clear that there's anything interesting to say here, but let's add another column, this time writing down $\frac{a}{\gcd(a,12)}$.

$\gcd(a,12)$	a	How many a?	$\frac{a}{\gcd(a,12)}$
1	1,5,7,11	4	1,5,7,11
2	2,10	2	1,5
3	3,9	2	1,3
4	4,8	2	1,2
6	6	1	1
12	0	1	0

In the last column, the first row is a set of representatives for the elements of $\mathbb{Z}_{12}^*$. The second row is precisely the set of integers in $\{0,\dots,5\}$ that are coprime to 6. The third row is eactly those integers we count to compute $\varphi(4)$. The pattern continues! So, in the column that is counting how many a there are, we have $\varphi(12)$, $\varphi(6)$, $\varphi(4)$, $\varphi(3)$, $\varphi(2)$, and $\varphi(1)$ respectively. Since every number in $\{0,\dots,11\}$ falls into one of these rows, we have

$$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)=12.$$

Coincidence? No way!

Lemma 32. *Let n be a positive integer and d a positive divisor of n. Let*

$$S_d=\left\{a\in\{0,\dots,n-1\}:\gcd(a,n)=\frac{n}{d}\right\}.$$

Then $|S_d|=\varphi(d)$.

Proof. Let $T_d=\{b\in\{0,\dots,d-1\}:\gcd(b,d)=1\}$ and note $\varphi(d)=|T_d|$. So, we want to show that $|S_d|=|T_d|$. Let $f:S_d\to T_d$ be given by $f(a)=\frac{ad}{n}$. It suffices to show f is a bijection.

To see f is well-defined, note that since $\gcd(a,n)=\frac{n}{d}$, $\frac{n}{d}\mid a$ so $\frac{ad}{n}$ is an integer. Furthermore, since $0\le a<n$ and d and n are positive, $0\le f(a)<\frac{nd}{n}=d$. Therefore $f(a)\in\{0,\dots,d-1\}$. Finally, we need to check that $\gcd(f(a),d)=1$. Since $\gcd(a,n)=\frac{n}{d}$, by Bezout's identity there exist $u,v\in\mathbb{Z}$ such that

$$\begin{aligned}au+nv&=\frac{n}{d}\\ \implies \frac{ad}{n}u+\frac{nd}{n}v&=\frac{n}{d}\frac{d}{n}\\ \implies f(a)u+dv&=1\end{aligned}$$

so $\gcd(f(a),d)=1$ and f is a well-defined function.

For injectivity, suppose $f(a)=f(a')$, so $\frac{ad}{n}=\frac{a'd}{n}$. Since $d\neq 0$ and $n\neq 0$, this implies $a=a'$ and f is injective. For surjectivity, let $b\in T_d$, so $\gcd(b,d)=1$. Then by Bezout's identity there exist $u,v\in\mathbb{Z}$ so that

$$\begin{aligned}bu+dv&=1\\ \implies \left(\frac{n}{d}b\right)u+nv&=\frac{n}{d}\end{aligned}$$

so $\gcd(\frac{n}{d}b,n)\mid\frac{n}{d}$. Since $\frac{n}{d}\mid\frac{n}{d}b$ and $\frac{n}{d}\mid n$, we have $\frac{n}{d}\mid\gcd(\frac{n}{d}b,n)$. Since all integers involved here are positive, we can conclude $\gcd(\frac{n}{d}b,n)=\frac{n}{d}$. Therefore $\frac{n}{d}b\in S_d$ and $f(\frac{n}{d}b)=b$ so f is surjective. ∎

Theorem 33. *Let n be a positive integer. Then*

$$\sum_{d\mid n}\varphi(d)=n$$

where $\sum_{d\mid n}$ denotes the sum over all positive divisors d of n.

Proof. The sets $\{S_d : d \mid n\}$ partition the set $\{0, \ldots, n-1\}$ (that is, every element of the set $\{0, \ldots, n-1\}$ belongs to exactly one of the sets S_d). In particular, $a \in S_{\frac{n}{\gcd(a,n)}}$. Let $d_1, \ldots, d_k$ be the positive divisors of n. Then $n = |S_{d_1}| + |S_{d_2}| + \cdots + |S_{d_k}|$ and by Lemma 32 we have $n = \sum_{d|n} \varphi(d)$. ■

5 The group of units

We saw earlier that the power tables lead us to Euler's Theorem and Fermat's Little theorem. Let's squeeze some more juice out of them. Here are some power tables for $\mathbb{Z}_n^*$ from earlier, as well as one for $n = 12$.

$\mathbb{Z}_5^*$	1	2	3	4
x^1	1	2	3	4
x^2	1	4	4	1
x^3	1	3	2	4
x^4	1	1	1	1

$\mathbb{Z}_7^*$	1	2	3	4	5	6
x^1	1	2	3	4	5	6
x^2	1	4	2	2	4	1
x^3	1	1	6	1	6	6
x^4	1	2	4	4	2	1
x^5	1	4	5	2	3	6
x^6	1	1	1	1	1	1

$\mathbb{Z}_9^*$	1	2	4	5	7	8
x^1	1	2	4	5	7	8
x^2	1	4	7	7	4	1
x^3	1	8	1	8	1	8
x^4	1	7	4	4	7	1
x^5	1	5	7	2	4	8
x^6	1	1	1	1	1	1

$\mathbb{Z}_{12}^*$	1	5	7	11
x^1	1	5	7	11
x^2	1	1	1	1
x^3	1	5	7	11
x^4	1	1	1	1

Let's pay even closer attention to where the 1s are. In the first three tables, the first row where all the entries are 1s is in the $x^{\varphi(n)}$ row. However, although the $x^{\varphi(12)}$ row is all 1s, it's not the first place it happens in $\mathbb{Z}_{12}^*$ (it also happens in the x^2 row).

Lecture 17 - 14/06

In fact, there are special columns in the first three tables where the first 1 appears where Euler's theorem tells us there must be a 1, and every other unit appears in that column before then! For example, look at the column [3] in $\mathbb{Z}_7^*$. The first power that is [1] is $[3]^6 = [3]^{\varphi(7)}$, and every unit appears in that column. In other words, every unit is a power of [3] in $\mathbb{Z}_7$. There is no special column like that in $\mathbb{Z}_{12}^*$.

There is another thing worth noticing, which is apparent in the tables for $\mathbb{Z}_7^*$ and $\mathbb{Z}_9^*$. Besides in the first column, the 1s only appear in the rows corresponding to divisors of $\varphi(n)$. In particular, no entry in the x^1 or $x^{\varphi(n)-1}$ rows (besides in the first column) are 1. This phenomenon is perhaps not too surprising: If $[a]^k = 1$ for some positive k, and this is the first positive k where it happens, then all the 1s in the column corresponding to $[a]$ should appear in multiplies of k. If $\varphi(n)$ is not a multiple of k, then $[a]^{\varphi(n)} \neq [1]$, which would contradict Euler's theorem.

But enough handwaving, let's formalise these observations.

Definition. Let n be a positive integer and $[a] \in \mathbb{Z}_n^*$. The **order of** $[a]$ **in** $\mathbb{Z}_n^*$ (sometimes denoted $\text{ord}([a])$ or $|[a]|$) is the smallest positive integer k such that $[a]^k = [1]$ in $\mathbb{Z}_n$.

So, in $\mathbb{Z}_7^*$ for example, $\text{ord}([2]) = 3$, $\text{ord}([3]) = 6$ and $\text{ord}([6]) = 2$. It is always the case that $\text{ord}([1]) = 1$ in $\mathbb{Z}_n^*$.

Exercise. Let n be a positive integer and $[a] \in \mathbb{Z}_n^*$. Prove that if $[a]^p = [1]$ for some prime p, and $[a] \neq [1]$ in $\mathbb{Z}_n$, then $\text{ord}([a]) = p$.

Let's first prove that the order of an element in $\mathbb{Z}_n^*$ must divide $\varphi(n)$.

Proposition 34. *Let $[a] \in \mathbb{Z}_n^*$. If $[a]^k = [1]$ for some integer k, then $\text{ord}([a]) \mid k$.*

Proof. This is left as an exercise (Question 5 on Assignment 2). ■

Exercise. Use Proposition 34 to prove that for $n > 2$, $\varphi(n)$ is even.

5.1 Mersenne Numbers

Let's see a couple of applications of this new point of view. First up, a slick proof that there are infinitely many primes (the first such proof in these notes).

Theorem 35. *There are infinitely many primes.*

Proof. Towards a contradiction, let p be the largest prime and let q be a prime divisor of $2^p - 1$. Then $q \mid 2^p - 1$ so $[2]^p = [1]$ in $\mathbb{Z}_q$. Since q is prime, $[2] \in \mathbb{Z}_q^*$. Since p is prime, $\text{ord}([2]) = p$ and so $p \mid q - 1$ by Proposition 34. Therefore $p \leq q - 1$ so $p < q$, a contradiction. ■

Numbers of the form $2^p - 1$ turn out to be important in the search for primes, and they are called Mersenne numbers. The first few Mersenne numbers are

$$3, 7, 31, 127$$

which are all prime. However, $2^{11} - 1 = 2047 = 23 \cdot 81$ so it's not prime. It is unknown whether or not there are infinitely many Mersenne numbers that are prime (called Mersenne primes), but it is currently the best way we know for finding large primes. In fact, there is a collaborate project called the Great Internet Mersenne Prime Search (GIMPS) which has found the 15 largest primes known. The largest prime currently known is the Mersenne prime

$$2^{82589933} - 1$$

which has 24,862,048 digits. The prime was found in 2018.

While it is unknown whether or not there are infinitely many Mersenne primes, we can prove that any two Mersenne numbers are coprime.

Proposition 36. *Let m and n be positive coprime integers. Then $2^m - 1$ and $2^n - 1$ are coprime.*

Proof. Let $g = \gcd(2^m - 1, 2^n - 1)$, and note that since both $2^m - 1$ and $2^n - 1$ are odd, g is odd. Therefore $[2] \in \mathbb{Z}_g^*$. Since $g \mid 2^m - 1$ we have $[2]^m = [1]$, and similarly $[2]^n = [1]$, in $\mathbb{Z}_g$. Let $x, y \in \mathbb{Z}$ be such that $mx + ny = 1$. Then

$$[2]^1 = [2]^{mx+ny} = ([2]^m)^x([2]^n)^y = [1]$$

in $\mathbb{Z}_g$. Therefore $g \mid (2 - 1)$ so $g = 1$. ■

Lecture 18 - 16/06

5.2 Primitive Roots

As we saw in the power tables above, $\mathbb{Z}_5^*$, $\mathbb{Z}_7^*$, and $\mathbb{Z}_9^*$ all have a special column which contains every unit. This is not the case for $\mathbb{Z}_{12}$. Having this property is desirable. Let's look at $\mathbb{Z}_7^*$ for example. The element $[3]$ gives rise to one of these columns, and we have $\mathbb{Z}_7^* = \{[3]^0, [3]^1, [3]^2, [3]^3, [3]^4, [3]^5\}$. So the powers of $[3]$ generate all of $\mathbb{Z}_7^*$. The existence of such elements will allow us to prove some powerful results.

Definition. An element $[a] \in \mathbb{Z}_n^*$ such that $\text{ord}([a]) = \varphi(n)$ is called a **primitive root** mod n (or a **generator** of $\mathbb{Z}_n^*$).

Example. The primitive roots mod 7 are [3] and [5] (this can be verified by looking at the power table.

The element $[2] \in \mathbb{Z}_{11}^*$ is a generator since $[2]^2 \neq [1]$ and $[2]^5 = [-1] \neq [1]$ in $\mathbb{Z}_{11}$ (why is it enough to just check the second and fifth powers here?).

Exercise. Prove that $[a]$ is a generator in $\mathbb{Z}_n^*$ if and only if $[a]^{\varphi(n)/p} \neq [1]$ in $\mathbb{Z}_n$ for every prime p that divides $\varphi(n)$.

Exercise. Find all (if any) generators of $\mathbb{Z}_{19}^*$. How many are there?

Exercise. Suppose $[a]$ is a generator of $\mathbb{Z}_n^*$. How many generators are there?

You may ask why we use the term "generator" (or "primitive root" for that matter, but let's just focus on "generator" for now). It's because a generator generates every other element of $\mathbb{Z}_n^*$! More precisely:

Exercise. Suppose $[a]$ is a generator of $\mathbb{Z}_n^*$. Prove that for all $[b] \in \mathbb{Z}_n^*$, there exists a positive integer k so that $[a]^k = [b]$.

If a generator for $\mathbb{Z}_n^*$ exists, then we can deduce a lot about how powers of elements behave in $\mathbb{Z}_n^*$.

Example. Let's find all elements $x \in \mathbb{Z}_{19}$ so that $x^3 = [1]$.

First we'll show that [2] is a generator of $\mathbb{Z}_{19}$. We have

$$\begin{aligned}
[2]^2 &= [4] \\
[2]^4 &= [-3] \\
[2]^6 &= [7] \\
[2]^8 &= [9] \\
[2]^9 &= [-1]
\end{aligned}$$

and since $[2]^6 \neq [1]$ and $[2]^9 \neq [1]$, [2] is a generator of $\mathbb{Z}_{19}$.

Now, [0] is not a solution to $x^3 = [1]$, so we only need to consider the units in $\mathbb{Z}_{19}$. Since [2] is a generator of $\mathbb{Z}_{19}^*$, we have $\mathbb{Z}_{19}^* = \{[2]^k : 0 \leq k < 18\}$.

Now, suppose $[2]^k$ satisfies $[1] = ([2]^k)^3 = [2]^{3k}$. Since $\text{ord}([2]) = 18$, we know $18 \mid 3k$. It's a quick exercise to prove that $18 \mid 3k$ if and only if $6 \mid k$, so all the solutions are given by $[2]^0, [2]^6$, and $[2]^{12}$. We can compute these powers to be [1], [7], and [11].

Of course, we could have just checked all 19 possibilities, but this is more fun!

Knowing about primitive roots helps us investigate solutions to polynomials, as in the previous example. Our next goal is to prove that generators exist for $\mathbb{Z}_p^*$ for all primes p. In order to do that, we need to investigate solutions to polynomials in $\mathbb{Z}_p$!

5.3 Polynomials in $\mathbb{Z}_p$

Just about everything we cover in this section works for polynomials over a field $\mathbb{F}$. Recall a **field** is a ring (a set with addition and multiplication) where every non-zero element has an inverse. For the sake of this course, the examples of fields to keep in mind for this section are the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, the rational numbers $\mathbb{Q}$, and of course, $\mathbb{Z}_p$ when p is prime. So whenever you see $\mathbb{F}$, you will be just fine replacing it with $\mathbb{Z}_p$.

We start with an extremely useful fact about fields.

Proposition 37. *For all elements $a, b \in \mathbb{F}$, if $ab = 0$ then $a = 0$ or $b = 0$.*

Proof. Suppose $ab = 0$ and $a \neq 0$. Then a is a unit so $ab = 0$ implies $a^{-1}ab = a^{-1} \cdot 0$ and we conclude $b = 0$. ■

Exercise. Show that the above proposition doesn't hold in $\mathbb{Z}_n$ whenever n is composite. Show that the above proposition does hold in $\mathbb{Z}$. Therefore being a field is sufficient for the proposition to hold, but not necessary!

Now, onto polynomials!

Definition. A **polynomial in the variable x with coefficients in $\mathbb{F}$** is an expression of the form $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where n is a non-negative integer, $a_i \in \mathbb{F}$ for all i, and $a_n \neq 0$. We also say $f(x) = 0$ is a polynomial.

The **degree** of $f(x) = a_n x^n + \cdots + a_0$ is n, denoted $\deg(f(x)) = n$. Define $\deg(0) = 0$.

The set of all polynomials in x over $\mathbb{F}$ is denoted $\mathbb{F}[x]$. When the variable is clear from context, or unimportant, we may denote $f(x)$ simply by f.

Example. $3x^2 - 2x \in \mathbb{R}[x]$ is a degree 2 polynomial with real coeffients. $[3]x^2 - [2]x \in \mathbb{Z}_5[x]$ is a degree 2 polynomial with coefficients in $\mathbb{Z}_5$. We also have $[2] \in \mathbb{Z}_5$, which is a degree 0 polynomial.

The set of polynomials $\mathbb{F}[x]$, comes with multiplication and addition, just like $\mathbb{Z}_n$ is a set with multiplication and addition. This turns $\mathbb{F}[x]$ into a ring. The multiplication and addition works as you're used to, and depends on the addition and multiplication in $\mathbb{F}$.

Example. Let $f, g \in \mathbb{Z}_5[x]$ be $f = x^3 + [2]x - [1]$ and $g = [3]x^2 + [2]x + [1]$. Then

$$f + g = x^3 + [3]x^2 + [4]x$$

and

$$\begin{aligned} fg &= (x^2 + [2]x - [1])([3]x^3 + [2]x + [1]) \\ &= [3]x^6 + [2]x^3 + x^2 + [6]x^4 + [4]x^2 + [2]x + [-1]x^3 + [-2]x + [-1] \\ &= [3]x^6 + [6]x^4 + [1]x^3 + [5]x^2 + [0]x + [0] \\ &= [3]x^6 + x^4 + x^3. \end{aligned}$$

Of course, when we write x^3 we really mean $[1]x^3$, and we simply leave out terms of the form $[0]x^k$.

Exercise. Write down all the units in $\mathbb{Z}_{11}[x]$.

Lecture 19 - 19/06

Up until this point there we haven't seemed to need $\mathbb{F}$ to be a field. In fact, we can define $\mathbb{Z}[x]$ and $\mathbb{Z}_n[x]$ as we have already, and these too are rings. However, for what is about to follow, it's important that $\mathbb{F}$ is a field.

Proposition 38. *Let $f, g \in \mathbb{F}[x]$ with $f \neq 0$ and $g \neq 0$. Then $\deg(fg) = \deg(f) + \deg(g)$.*

Proof. Let $f = a_n x^n + \cdots + a_0$ and $g = b_m x^m + \cdots + b_0$, with $a_n \neq 0$ and $b_m \neq 0$. Then $fg = a_n b_m x^{n+m} + h$ for some $h \in \mathbb{F}[x]$ with $\deg(h) < n + m$. We have $a_n b_m \neq 0$ since $a_n \neq 0$ and $b_m \neq 0$, implying $\deg(fg) = n + m$. ■

Just like in $\mathbb{Z}$, we have a division algorithm in $\mathbb{F}[x]$, which is amazingly useful.

Theorem 39 (Division algorithm for polynomials)**.** *Let $f, g \in \mathbb{F}[x]$ with $g \neq 0$. Then there exist unique polynomials $q, r \in \mathbb{F}[x]$ so that $f = qg + r$ and $\deg(r) < \deg(g)$.*

We won't prove this here.

Exercise. Show that the division algorithm fails in $\mathbb{Z}[x]$. *Hint: consider $g = 2x$.*

Polynomials themselves aren't functions, they are eimply elements of a ring (so things you can add and multiply). However, polynomials in $\mathbb{F}[x]$ do indeed define functions from $\mathbb{F}$ to $\mathbb{F}$.

Definition. Let $f = a_n x^n + \cdots + a_0 \in \mathbb{F}[x]$. Define the function $f : \mathbb{F} \to \mathbb{F}$ by $f(b) = a_n b^n + \cdots + a_1 b + a_0$.

For example, the polynomial $f(x) = x^2 \in \mathbb{R}[x]$ defines a function $f : \mathbb{R} \to \mathbb{R}$, given by $f(a) = a^2$ for all $a \in \mathbb{R}$.

Example. Let $f(x) = x^2 \in \mathbb{Z}_7[x]$. Then

$$\begin{aligned} f([0]) &= [0] \\ f([1]) = f([-1]) &= [1] \\ f([2]) = f([-2]) &= [4] \\ f([3]) = f([-3]) &= [2]. \end{aligned}$$

Example (An important example!)**.** Let p be a prime and let $f(x) = x^p \in \mathbb{Z}_p[x]$. We have $f([0]) = [0]$. For $[a] \neq [0]$, Fermat's little theorem tells us $f([a]) = [a]^p = [a]$.

So, $f(x) = x^p$ and $g(x) = x$ define the same function from $\mathbb{Z}_p \to \mathbb{Z}_p$, but they are not equal as polynomials (indeed, $\deg(f(x)) = p$ and $\deg(g(x)) = 1$).

Definition. Let $f(x) \in \mathbb{F}[x]$. A **root** of $f(x)$ is an element $c \in \mathbb{F}$ so that $f(c) = 0$.

So, as we saw in the last lecture, the roots of $x^3 - [1]$ in $\mathbb{Z}_{19}[x]$ are $[1], [7]$, and $[11]$.

Roots of polynomials turn out to tell us a lot about how the polynomials factor.

Definition. Let $f, g \in \mathbb{F}[x]$. We say f **divides** g, denoted $f \mid g$, if there exists $q \in \mathbb{F}[x]$ so that $fq = g$.

In $\mathbb{Z}_5[x]$, for example, $x^2 + [4] = (x + [4])(x + [1])$, so $x + [4] \mid x^2 + [4]$.

Now, a useful proposition.

Proposition 40. *Let $f(x) \in \mathbb{F}[x]$ and $c \in \mathbb{F}$. Then $f(c) = 0$ if and only if $(x - c) \mid f(x)$.*

Proof. By the division algorithm, there exists a polynomial $g(x) \in \mathbb{F}[x]$ and a constant (a degree 0 polynomial) d so that

$$f(x) = (x - c)g(x) + d.$$

If $f(c) = 0$, then $0 = (c - c)g(x) + d$ so $d = 0$ and $(x - c) \mid f(x)$. Conversely, if $(x - c) \mid f(x)$ then $(x - c)h(x) = f(x)$, and by the uniqueness in the division algorithm, $g(x) = h(x)$ and $d = 0$. Therefore $f(c) = (c - c)g(c) = 0$. ∎

In Assignment 2 you proved that if $x^2 = [a]$ had a solution in $\mathbb{Z}_p$, then there were exactly 2 solutions. However, not every choice of $[a]$ has a solution (for example if $[a] = [2]$ and $p = 5$). So the polynomial $x^2 - [a] \in \mathbb{Z}_p[x]$ has at most 2 roots. In a previous example, we saw that $x^3 - [1] \in \mathbb{Z}_{11}[x]$ has exactly 3 solutions. The fundamental theorem of algebra tells us that a degree d polynomial in $\mathbb{C}[x]$ has exactly d roots (if counted with multiplicity). In $\mathbb{R}[x]$, a degree d polynomial has at most d solutions.

Theorem 41. *Let $f(x) \in \mathbb{F}[x]$ be such that $f(x)$ is not the zero polynomial. Then $f(x)$ has at most $\deg(f(x))$ roots.*

Proof. We will proceed by induction on the degree of f. If $\deg(f) = 0$, then $f = c \neq 0$ for some constant $c \in \mathbb{F}$, so f has no roots.

Assume now that if $\deg(g) = k$, then there are at most k roots of g. Let $f \in \mathbb{F}[x]$ be such that $\deg(f) = k + 1$. If f has no roots, we're done. Suppose f has a root c. Then $f(x) = (x - c)g(x)$ for some $g(x) \in \mathbb{F}[x]$. Since $\deg(f) = 1 + \deg(g)$ we know $\deg(g) = k$. By the inductive hypothesis, g has at most k roots. Now suppose d is a root of f other than c. Then $0 = f(d) = (d - c)(g(d))$. Since $d - c \neq 0$ and since $\mathbb{F}$ is a field, $g(d) = 0$, so d is a root of g. Therefore all roots other than c of f are roots of g and there are at most $k + 1$ roots of f. ■

Exercise. Construct a cubic polynomial in $\mathbb{Z}_7[x]$ with exactly 2 roots.

We now have what we need to return to our study of primitive roots.

Lecture 20 - 21/06

5.4 Back to primitive roots

The goal now is to show that $\mathbb{Z}_p^*$ has a generator when p is prime. In fact, we can prove something stronger. Not only is it the case that there is an element with order $p - 1$, but for every d dividing $p - 1$, there are $\varphi(d)$ elements of order d in $\mathbb{Z}_p^*$.

Let's take $\mathbb{Z}_{11}^*$ as an example. Here is the power table for $\mathbb{Z}_{11}^*$.

$\mathbb{Z}_{11}^*$	1	2	3	4	5	6	7	8	9	10
x^1	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	3	3	5	9	4	1
x^3	1	8	5	9	4	7	2	6	3	10
x^4	1	5	4	3	9	9	3	4	5	1
x^5	1	10	1	1	1	10	10	10	1	10
x^6	1	9	3	4	5	5	4	3	9	1
x^7	1	7	9	5	3	8	6	2	4	10
x^8	1	3	5	9	4	4	9	5	3	1
x^9	1	6	4	3	9	2	8	7	5	10
x^{10}	1	1	1	1	1	1	1	1	1	1

The possible orders of elements in $\mathbb{Z}_{11}^*$ are $1, 2, 5$, and 10, and of course, we can read off the orders straight from the power table. Since we have the power table in front of us, we can even see that $[2]$ is a generator. Let's write out the elements of $\mathbb{Z}_{11}^*$ as powers of $[2]$ and keep track of their orders.

$$\begin{aligned}
\operatorname{ord}([2]^0) &= \operatorname{ord}([1]) = 1 \\
\operatorname{ord}([2]^1) &= \operatorname{ord}([2]) = 10 \\
\operatorname{ord}([2]^2) &= \operatorname{ord}([4]) = 5 \\
\operatorname{ord}([2]^3) &= \operatorname{ord}([8]) = 10 \\
\operatorname{ord}([2]^4) &= \operatorname{ord}([5]) = 5 \\
\operatorname{ord}([2]^5) &= \operatorname{ord}([10]) = 2 \\
\operatorname{ord}([2]^6) &= \operatorname{ord}([9]) = 5 \\
\operatorname{ord}([2]^7) &= \operatorname{ord}([7]) = 10 \\
\operatorname{ord}([2]^8) &= \operatorname{ord}([3]) = 5 \\
\operatorname{ord}([2]^9) &= \operatorname{ord}([6]) = 10
\end{aligned}$$

We know [2] has order 10, and the important thing to notice here, is that the other powers of [2] that have order 10 are precisely those powers $[2]^k$ such that $\gcd(10, k) = 1$. In particular, there are exactly $\varphi(10)$ such elements. If we look at the elements of order 5, these correspond to powers $[2]^k$ such that $\gcd(k, 10) = 2$, and there are exactly $\varphi(5)$ such elements. This should start to feel like the arguments we used in Lemma 32! Similarly, there are $\varphi(2)$ elements of order 2, and $\varphi(1)$ elements of order 1.

Let's try to prove some of these observations in general.

Lemma 42. *Let $[a] \in \mathbb{Z}_n^*$ and suppose $\operatorname{ord}([a]) = t$. Then $\operatorname{ord}([a]^k) = t$ if and only if $\gcd(k, t) = 1$.*

Proof. Let $\gcd(k, t) = d$ and suppose $\operatorname{ord}([a]^k) = t$. We have

$$([a]^k)^{\frac{t}{d}} = ([a]^t)^{\frac{k}{d}} = [1].$$

If $d > 1$, then $\frac{t}{d} < t$, contradicting the assumption that $\operatorname{ord}([a]^k) = 1$. Therefore $\gcd(k, t) = 1$.

Conversely, suppose $\gcd(k, t) = 1$, so there exist $u, v \in \mathbb{Z}$ so that $ku + tv = 1$. Note that $([a]^k)^t = ([a]^t)^k = [1]$ so $\operatorname{ord}([a]^k) \mid t$. Let $s = \operatorname{ord}([a]^k)$, so in particular $[a]^{ks} = [1]$. Then

$$[a]^s = [a]^{(ku+tv)s} = ([a]^{ks})^u([a]^t)^{vs} = 1.$$

Since $\operatorname{ord}([a]) = t$, we have $t \mid s$ so we conclude $t = \operatorname{ord}([a]^k)$. ■

Lecture 21 - 23/06

We can now use this lemma to count exactly now many elements of every possible order there are in $\mathbb{Z}_p^*$. As a consequence we will get that $\mathbb{Z}_p^*$ has a generator for all primes p.

Theorem 43. *Let p be a prime. Then $\mathbb{Z}_p^*$ has $\varphi(d)$ elements of order d for every positive divisor d of $p - 1$.*

Proof. Let $\Omega_d = \{[a] \in \mathbb{Z}_p^* : \operatorname{ord}([a]) = d\}$. Since every element in $\mathbb{Z}_p^*$ has an order dividing $p - 1$ we have

$$\sum_{d|p} |\Omega_d| = p - 1$$

(recall $\sum_{d|p}$ means the sum is taken over all positive divisors d of $p-1$). By Theorem 33 we have

$$\sum_{d|p} \varphi(d) = p - 1.$$

Putting these together we get

$$\sum_{d|p} (\varphi(d) - |\Omega_d|) = 0.$$

If we can show $\varphi(d) \geq |\Omega_d|$ for all d, then we will have a sum of nonnegative integers being equal to 0, and we can conclude that $\varphi(d) = |\Omega_d|$. So let's do that.

If there is no element of order d, then $|\Omega_d| = 0$ and $\varphi(d) \geq |\Omega_d|$. So let's assume $[a] \in \mathbb{Z}_{p^*}$ has order d. Now, $([a]^k)^d = ([a]^d)^k = [1]$, so every power of $[a]$ is a root of $f(x) = x^d - [1] \in \mathbb{Z}_p[x]$. Since $\text{ord}([a]) = d$, the d distinct elements $\{[a]^0, [a]^1, \ldots, [a]^{d-1}\}$ roots of $f(x)$. Since $\deg(f(x)) = d$, this is a complete set of roots of $f(x)$ (by Theorem 41).

Every element of order d in $\mathbb{Z}_p^*$ is a root of $x^d - [1]$, so every element of order d is a power of $[a]$. By Lemma 42, there are exactly $\varphi(d)$ powers of $[a]$ that have order d, so $\varphi(d) = |\Omega_d|$.

We may now conclude $\varphi(d) = |\Omega_d|$ for all positive divisors d of $p-1$. ■

If we take this Theorem and focus on the elements of order $p-1$ we get the following important result.

Corollary 44. *Let p be a prime. There exists a generator of $\mathbb{Z}_p^*$.*

Exercise. Find composite positive integers n and m so that $\mathbb{Z}_n^*$ has a generator and $\mathbb{Z}_m^*$ does not.

Let's exploit this result as best as we can. You may have noticed the curious thing that sometimes -1 has a square root in $\mathbb{Z}_p$. More precisely, for some primes p, there exists an element $[a]$ so that $[a]^2 = [-1]$ in $\mathbb{Z}_p$.

For example, $[2]^2 = [-1]$ in $\mathbb{Z}_5$, but there is no square root of $[-1]$ in $\mathbb{Z}_7$. We are now in a position to completely classify which primes p admit a square root of -1 in $\mathbb{Z}_p$. Another way of phrasing the existence of a square root is to say the polynomial $x^2 + [1]$ has a root in $\mathbb{Z}_p$.

Proposition 45. *let p be an odd prime. The polynomial $x^2 + [1] \in \mathbb{Z}_p[x]$ has a root if and only if $p \equiv 1 \pmod 4$.*

Proof. Suppose $[a]$ is a root of $x^2 + [1]$. Then $[a]^2 = [-1]$ so $[a]^4 = [1]$. Since $[a] \neq [1]$ and $[a]^2 \neq [1]$, $\text{ord}([a]) = 4$. Therefore $4 \mid p - 1$.

Conversely, suppose $p \equiv 1 \pmod 4$, so $4 \mid p - 1$. By Theorem 43, there are $\varphi(4) = 2$ elements of order 4, call them $[b]$ and $[c]$. Then $[b]^4 = [1]$ so $([b]^2)^2 = [1]$. Since $\text{ord}([b]) = 4$, $[b]^2 \neq [1]$ so $\text{ord}([b]^2) = 2$. However, Theorem 43 tells us there is exactly one element of order 2, and that element is $[-1]$. Therefore $[b]^2 = [-1]$. ■

Lecture 22 - (26/06)

Neat! Let's keep pushing.

Proposition 46. *There are infinitely many primes p such that $p \equiv 1 \pmod 4$.*

Proof. Suppose towards a contradiction that $\{p_1, p_2, \ldots, p_k\}$ is the set of primes congruent to 1 (mod 4). Consider $m = (2p_1p_2 \cdots p_k)^2 + 1$, and let q be a prime divisor of m. Note $q \neq p_i$ for all i, and q is an odd prime. Then $(2p_1p_2 \cdots p_k)^2 \equiv -1 \pmod q$, so $q \equiv 1 \pmod 4$, a contradiction. ■

The main result in this section is that $\mathbb{Z}_p^*$ has a generator when p is prime. It turns out that this is not the only time this happens. Indeed, if you go back to your power tables, $\mathbb{Z}_4^*$ and $\mathbb{Z}_9^*$ also have generators, and so does $\mathbb{Z}_{10}^*$. Here is a statement of the theorem classifying which integers n have the property that $\mathbb{Z}_n^*$ has a generator. We will not prove this in these notes.

Theorem 47. *The group of units $\mathbb{Z}_n^*$ has a generator if and only if $n = 1, 2, 4, p^k$, or $2p^k$ where p is an odd prime and k is a positive integer.*

6 Quadratic residues

As we've seen throughout the course, knowing which congruence classes in $\mathbb{Z}_n$ are squares can give us lots of leverage. In this section we'll focus in on this task.

Definition. An element $[a] \in \mathbb{Z}_n^*$ is a **quadratic residue** in $\mathbb{Z}_n^*$ if $[a] = [b]^2$ for some $[b] \in \mathbb{Z}_n^*$. Denote the set of quadratic residues in $\mathbb{Z}_n^*$ by Q_n.

With this language, we have already seen the following:

$$Q_4 = \{[1]\}$$
$$Q_5 = \{[1], [4]\}$$
$$Q_7 = \{[1], [2], [4]\}$$

Note that Q_n is only concerned with units that are squares, not all congruence classes.

Exercise. Let n be a positive integer. Show that

- $[1] \in Q_n$, and
- if $[a], [b] \in Q_n$, then $[a][b] \in Q_n$.

By proving these two properties, you have shown that Q_n is a group, and more precisely, is a subgroup of $\mathbb{Z}_n^*$.

When n is small, it's easy enough to run through the square of every element of $\mathbb{Z}_n^*$ to simply write down the elements of Q_n. But we need something a little more efficient to work out what the quadratic residues are in general.

Enter, once again, primitive roots. When we do have a generator of $\mathbb{Z}_n^*$, we can use it to help us out a little.

Let's see this in action when $n = 11$. We know $[2]$ is a generator of $\mathbb{Z}_{11}^*$. So

$$\mathbb{Z}_{11}^* = \{[2]^0, [2]^1, [2]^2, \ldots, [2]^9\}$$

and therefore

$$Q_{11} = \{[2]^{0\cdot 2}, [2]^{1\cdot 2}, [2]^{2\cdot 2}, [2]^{3\cdot 2}, \ldots, [2]^{8\cdot 2}, [2]^{9\cdot 2}\}.$$

However, we know that by Fermat's little theorem, $[2]^{t\cdot 2} = [2]^{(t+5)\cdot 2}$ and so

$$Q_{11} = \{[2]^0, [2]^2, [2]^4, [2]^6, [2]^8\}.$$

The important thing to notice here is that the quadratic residues are precisely those which are an even power of a generator.

Proposition 48. *Let $n > 2$ and suppose $[g]$ is a generator of $\mathbb{Z}_n^*$. Then $Q_n = \{[g]^k : 2 \mid k\}$.*

Proof. Suppose $k = 2t$ for some integer t. Then $[g]^{2t} = ([g]^t)^2$ so $g^{2t} \in Q_n$. Conversely, suppose $[a] \in Q_n$, so $[a] = [b]^2$ for some $[b] \in \mathbb{Z}_n^*$. Since $[g]$ is a generator, $[b] = [g]^t$ for some $t \in \mathbb{Z}$, and so $[a] = [g]^{2t}$, completing the proof. ■

As a corollary, we get the following result, which is a question on Assignment 3.

Corollary 49. *Let p be an odd prime. Then $[a] \in Q_p$ if and only if $[a]^{\frac{p-1}{2}} = [1]$ in $\mathbb{Z}_p$.*

Proof. This is an exercise (Assignment 3). ■

Notice that although Proposition 48 tells us how to find every element of Q_n, it does rely on us already having a generator. The advantage of the corollary is that we don't need a generator!

Example. In $\mathbb{Z}_{13}$ we have $[4]^2 = [3]$ so $[4]^6 = [3]^3 = [27] = [1]$, so $[4] \in Q_{13}$. It's a little silly to conclude $[4] \in Q_{13}$ because $[4] = [2]^2$, but nevertheless, the computation demonstrates how the Corollary could be used.

Exercise. Let p be an odd prime. Use Corollary 49 to prove that $[-1] \in Q_p$ if and only if $p \equiv 1 \pmod 4$.

Lecture 23 - 28/06

6.1 The Legendre Symbol

Before we push on investigating quadratic residues, we must introduce a surprisingly convenient piece of notation. As we use it throughout this section, we will see it as a shining example of how good notation can be an indispensible aide to a mathematician.

Definition. Let p be an odd prime. For $a \in \mathbb{Z}$, define the **Legendre symbol** as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } [a] = [0] \text{ in } \mathbb{Z}_p \\ 1 & \text{if } [a] \in Q_p \\ -1 & \text{otherwise.} \end{cases}$$

So, for example,

$$\left(\frac{a}{7}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod 7 \\ 1 & \text{if } a \equiv 1, 2, 4 \pmod 7 \\ -1 & \text{if } a \equiv 3, 5, 6 \pmod 7. \end{cases}$$

Rephrasing Proposition 48 we get the following.

Proposition 50. *Let p be an odd prime and $[g]$ a generator of $\mathbb{Z}_p^*$. Then*

$$\left(\frac{g^t}{p}\right) = (-1)^t.$$

We already know that the product of two elements of Q_n is again an element of Q_n. However, we can say something stronger in the case that n is an odd prime.

Proposition 51. *Let p be an odd prime and $a, b \in \mathbb{Z}$. Then*

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

Proof. If $p \mid a$ or $p \mid b$, then both the left and right hand sides are 0. We may therefore assume $[a], [b] \in \mathbb{Z}_p^*$. Let $[g]$ be a generator for $\mathbb{Z}_p^*$, and write $[a] = [g]^t$ and $[b] = [g]^s$ for positive integers t, s. Then $[ab] = [g]^{t+s}$ so

$$\left(\frac{ab}{p}\right) = (-1)^{t+s} = (-1)^t(-1)^s = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

completing the proof. ■

This is a seemingly innocuous statement that gives us a surprising amount of leverage.

Example. Let $p \equiv 1 \pmod 4$ be a prime. Then we know $(\frac{-1}{p}) = 1$. Therefore $[a] \in Q_p$ if and only if $[-a] \in Q_p$. To see this, we have $(\frac{-a}{p}) = (\frac{-1}{p})(\frac{a}{p}) = (\frac{a}{p})$. So, for example, we immediately know $[109] \in Q_{113}$ since $[4] \in Q_{113}$.

Using the Legendre symbol, we can rephrase Corollary 49 as follows. As written, it is often referred to as Euler's criterion.

Theorem 52 (Euler's Criterion)**.** *Let p be an odd prime and $a \in \mathbb{Z}$. Then*

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

Exercise. Find an element of $\mathbb{Z}_{13}^*$ that is not a generator and not an element of Q_{13}.

6.2 Gauss' Lemma

Let's shift our focus to computing $[a]^{\frac{p-1}{2}}$ in $\mathbb{Z}_p$. We will compute $[3]^9$ in $\mathbb{Z}_{19}$ in a very sloppy and questionable manner, yet very suggestive of a more general strategy.

Out of seemingly nowhere, let's consider the following ludicrous way to write 3^9:

$$3^9 = \frac{3}{1} \cdot \frac{6}{2} \cdot \frac{9}{3} \cdot \frac{12}{4} \cdot \frac{15}{5} \cdot \frac{18}{6} \cdot \frac{21}{7} \cdot \frac{24}{8} \cdot \frac{27}{9}.$$

Now let's write it in $\mathbb{Z}_{19}$:

$$[3]^9 = \Big([3][6][9][12][15][18][21][24][27]\Big)\Big([1][2][3][4][5][6][7][8][9]\Big)^{-1}.$$

Here's the trick. We now notice that as subsets of $\mathbb{Z}_{19}$,

$$\{[3], [6], [9], [12], [15], [18], [21], [24], [27]\} = \{[-1], [2], [3], [-4], [5], [6], [-7], [8], [9]\}$$

since $[18] = [-1]$, $[21] = [2]$, $[15] = [-4]$, $[24] = [5]$, $[12] = [-7]$, and $[27] = [8]$. Inserting this observation back into our computation gives

$$\begin{aligned}
[3]^9 &= \Big([-1][2][3][-4][5][6][-7][8][9]\Big)\Big([1][2][3][4][5][6][7][8][9]\Big)^{-1} \\
&= [-1]^3\Big([1][2][3][4][5][6][7][8][9]\Big)\Big([1][2][3][4][5][6][7][8][9]\Big)^{-1} \\
&= [-1]
\end{aligned}$$

and so we can conclude $[3] \notin Q_{19}$.

One incredibly convenient thing happened here. That was that each of the $\frac{p-1}{2} = 9$ elements in the set $\{[3], [6], \ldots, [27]\}$ lie in exactly one of the sets

$$\{[1], [-1]\}, \quad \{[2], [-2]\}, \quad \ldots \quad \{[9, -9]\}$$

and each of the sets contain exactly one of the original $\frac{p-1}{2}$ elements. Said another way, the map

$$f : \{[3], [6], \ldots, [27]\} \to \Big\{\{[1], [-1]\}, \{[2], [-2]\}, \ldots, \{[9], [-9]\}\Big\}$$

defined by $f([a]) = S$ where $[a] \in S$, is a bijection.

Once we have that the map is a bijection, to compute $[3]^9$ we simply had to count how many negatives appeared! Let's show this kind of thing happens in general.

Lecture 24 - 30/06

Lemma 53. *Let p be an odd prime and let $[a] \in \mathbb{Z}_p^*$. The function*

$$f : \left\{[1], [2], \ldots, \left[\frac{p-1}{2}\right]\right\} \to \left\{\{[1], [-1]\}, \{[2], [-2]\}, \ldots, \left\{\left[\frac{p-1}{2}\right], \left[-\frac{p-1}{2}\right]\right\}\right\}$$

given by $f([b]) = S$ where $[ab] \in S$, is a bijection.

Proof. First note that every element of $\mathbb{Z}_p^*$ appears in exactly one of the sets

$$\{[1], [-1]\}, \{[2], [-2]\}, \ldots, \left\{\left[\frac{p-1}{2}\right], \left[-\frac{p-1}{2}\right]\right\}.$$

Furthermore, since the product of two units is a unit, we have that $f([b])$ is in one of the sets for every $[b]$ in $\mathbb{Z}_p^*$. Therefore f is a well-defined function.

Since both the domain and codomain of the function have $\frac{p-1}{2}$ elements, f is an injection if and only if it is a surjection. So it suffices to show f is injective.

Suppose $f([b]) = f([c])$. Then $[ab]$ and $[ac]$ are in the same set of the form $\{[t], [-t]\}$. Therefore $[ab] = [ac]$ or $[ab] = [-ac]$.

Since $[a]$ has an inverse, $[ab] = [-ac]$ implies $[b] = [-c]$. However no two elements in $\{[1], [2], \ldots, [\frac{p-1}{2}]\}$ have this property, so it cannot be the case $[ab] = [-ac]$, and we must have $[ab] = [ac]$. Again, since $[a]$ is a unit we can conclude $[b] = [c]$ and f is an injection. ∎

Great, so we know that for any $[a] \in \mathbb{Z}_p^*$ where p is an odd prime we have

$$\{[a], [2a], [3a], \ldots, [\frac{p-1}{2}a]\} = \{[\epsilon_1 1], [\epsilon_2 2], \ldots, [\epsilon_{\frac{p-1}{2}} \frac{p-1}{2}]\}$$

where $\epsilon_i = \pm 1$ for all i. The content of the next result is that to compute $[a]^{\frac{p-1}{2}}$, we simply need to count how many ϵ_i are -1. To do this, we first need some notation.

Let p be an odd prime. Define the subsets

$$P = \{[1], [2], \ldots, [\frac{p-1}{2}]\} \quad \text{and} \quad N = \{[-1], \ldots, [-\frac{p-1}{2}]\}.$$

We call these P for positive and N for negative. For $[a] \in \mathbb{Z}_p$, define $aP = \{[ab] \in \mathbb{Z}_p : [b] \in P\}$.

Theorem 54 (Gauss' Lemma)**.** *Let p be an odd prime and $[a] \in \mathbb{Z}_p^*$. Then $(\frac{a}{p}) = (-1)^\nu$ where $\nu = |aP \cap N|$.*

Proof. By Euler's criterion, it suffices to show $[a^{\frac{p-1}{2}}] = [(-1)^\nu]$ in $\mathbb{Z}_p$. By Lemma 53 we have

$$\begin{aligned}[a]^{\frac{p-1}{2}}[1][2]\cdots\left[\frac{p-1}{2}\right] &= ([a][1])([a][2])\cdots\left([a]\left[\frac{p-1}{2}\right]\right)\\ &= [\epsilon_1 1][\epsilon_2 2]\cdots\left[\epsilon_{\frac{p-1}{2}}\frac{p-1}{2}\right]\\ &= [(-1)^\nu][1][2]\cdots\left[\frac{p-1}{2}\right]\end{aligned}$$

where $\epsilon_i = \pm 1$ for all i, and ν is the number of ϵ_i that equal -1. The number of ϵ_i that are -1 is precisely the size of the set $aP \cap N$, so $\nu = |aP \cap N|$. If we now cancel the unit $[1][2]\cdots[\frac{p-1}{2}]$ from both sides of the equation above we get

$$[a]^{\frac{p-1}{2}} = [(-1)^\nu]$$

completing the proof. ∎

This is pretty finicky, but let's see it in action.

Example. We will use Gauss' lemma to decide wether or not $[5] \in Q_{29}$. In $\mathbb{Z}_{29}$ we have

$$\begin{aligned}5P &= \{[5],[10],[15],[20],[25],[30],[35],[40],[45],[50],[55],[60],[65],[70]\}\\ &= \{[5],[10],[-14],[-9],[-4],[1],[6],[11],[-13],[-8],[-3],[2],[7],[12]\}.\end{aligned}$$

There are 6 negatives in this set, so $(\frac{5}{29}) = (-1)^6 = 1$ and $[5] \in Q_{29}$.

Example. Let's sketch out when $[2] \in Q_p$ for odd primes p. I say sketch because full details are in the solutions to Assignment 3.

Note that $2P = \left\{[-1],[2],[-3],[4],\ldots,\left[\pm\frac{p-1}{2}\right]\right\}$. So, how many negatives are there?

There are a few cases to consider here. If $\frac{p-1}{2}$ is even (so $p \equiv 1 \pmod 4$), then

$$2P \cap N = \left\{[-1],[-3],\ldots,\left[-\frac{p-3}{2}\right]\right\}$$

so there are $\frac{p-1}{4}$ negatives. We have $\frac{p-1}{4}$ is even if $p \equiv 1 \pmod 8$ and $\frac{p-1}{4}$ is odd if $p \equiv 5 \pmod 8$.

If $\frac{p-1}{2}$ is odd (so $p \equiv 3 \pmod 4$), then

$$2P \cap N = \left\{[-1],[-3],\ldots,\left[-\frac{p-1}{2}\right]\right\}$$

so there are $\frac{p+1}{4}$ negatives. We have $\frac{p+1}{4}$ is even if $p \equiv 7 \pmod 8$ and odd if $p \equiv 3 \pmod 8$.

Putting all of this together, we have $[2] \in Q_p$ if and only if $p \equiv \pm 1 \pmod 8$.

Exercise. When is $[-2] \in Q_p$ for odd primes p?

Lecture 25 - 05/07

6.3 Quadratic Reciprocity

The notation invoked for the Legendre symbol looks an awful lot like a fraction. It clearly doesn't behave like a fraction (for example, we don't have any way to add two legendre symbols and get anything sensible, and Proposition 51 shows us multiplication certainly doesn't immitate multiplication of fractions). However, there is something to be said about "inverses" of Legendre symbols.

This is a great example of the notation suggesting a question: For odd primes p and q how do $(\frac{p}{q})$ and $(\frac{q}{p})$ relate to each other? As always, let's throw some examples at the problem.

$(\frac{p}{q})$	$q=3$	5	7	11	13	17	19
$p=3$	0	−1	1	−1	1	−1	1
5	−1	0	−1	1	−1	−1	1
7	−1	−1	0	1	−1	−1	−1
11	1	1	−1	0	−1	−1	−1
13	1	−1	−1	−1	0	1	−1
17	−1	−1	−1	−1	1	0	1
19	−1	1	1	1	−1	1	0

The table appears to satisfy $(\frac{p}{q}) = (\frac{q}{p})$ most of the time. In fact, let's delete all the cases where this is the case, and see what's left.

$(\frac{p}{q})$	$q=3$	5	7	11	13	17	19
$p=3$			1	−1			1
5							
7	−1			1			−1
11	1		−1				−1
13							
17							
19	−1		1	1			

The cases where $(\frac{p}{q}) = -(\frac{q}{p})$, at least for $p, q < 20$, is exactly when p and q are distinct odd primes, and $p \equiv q \equiv 3 \pmod 4$. This turns out to be true in general, and is known as the law of quadratic reciprocity.

Theorem 55 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = \begin{cases} -(\frac{q}{p}) & \text{if } p \equiv q \equiv 3 \pmod 4 \\ (\frac{q}{p}) & \text{otherwise.} \end{cases}$$

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

The Law of Quadratic Reciprocity was conjectured by Euler in 1783, and Legendre gave several incomplete proofs. In 1795, Gauss (who was 6 years old at the time Euler made the conjecture) discovered and proved the law for himself. We will not prove it in these notes, but let's see it in action!

Example. Let's figure out whether or not $[83] \in Q_{103}$. We have

$$\begin{aligned}\left(\frac{83}{103}\right) &= -\left(\frac{103}{83}\right) \\ &= -\left(\frac{20}{83}\right) \\ &= -\left(\frac{2}{83}\right)^2\left(\frac{5}{83}\right) \\ &= -\left(\frac{5}{83}\right) \\ &= -\left(\frac{83}{5}\right) \\ &= -\left(\frac{3}{5}\right) \\ &= -\left(\frac{5}{3}\right) \\ &= -\left(\frac{2}{3}\right) \\ &= 1\end{aligned}$$

since $[2] \notin Q_3$. Therefore $[83] \in Q_{103}$.

Exercise. Justify each step in the previous example.

Lecture 26 - 07/07

We have seen so far a few characterisations of when congruence classes of certain integers are quadratic residues mod p. For example, we know for odd primes p, $(\frac{-1}{p}) = 1$ if and only if $p \equiv 1 \pmod 4$. We know $(\frac{2}{p}) = 1$ if and only if $p \equiv \pm 1 \pmod 8$. These were hard fought battles, but quadratic reciprocity makes results like these a little easier to come by.

Example. For which primes p is it true that $[3] \in Q_p$? Now, it may be tempting to throw Gauss' lemma at this problem (just like you did for [2] in Assignment 2), but that's hard. Let's use quadratic reciprocity!

We know $[3] \in Q_2$ and $[3] \notin Q_3$, so let's assume $p > 3$. Then there are two cases to consider.

If $p \equiv 1 \pmod 4$, then

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

If $p \equiv 3 \pmod 4$, then

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = \begin{cases} -1 & \text{if } p \equiv 1 \pmod 3 \\ 1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Putting all of this together we have a condition that depends on the congruence class of $p \pmod{12}$: For $p > 3$, $[3] \in Q_p$ if and only if $p \equiv \pm 1 \pmod{12}$.

The fact that this example came out so nicely is a reflection of the power of quadratic reciprocity, and thus an indication of how difficult the proof is (at least if we just rely on Gauss' lemma).

Exercise. Prove that $a \equiv 3 \pmod 4$ and $a \equiv 2 \pmod 3$ if and only if $a \equiv 11 \pmod{12}$.

6.4 Fermat numbers

This is a nice time for a little diversion into an interesting class of numbers named after the French mathematician from the 1600s, Pierre de Fermat. Well a mathematician by night anyway, he was also a lawyer!

Definition. For a nonnegative integer n, define the **Fermat number** as

$$F_n = 2^{2^n} + 1.$$

The first few Fermat numbers are

$$\begin{aligned} F_0 &= 3 \\ F_1 &= 5 \\ F_2 &= 17 \\ F_3 &= 257 \\ F_4 &= 65537 \end{aligned}$$

You can check, that these are prime! In fact, it was conjectured by Pierre de Fermat that all Fermat numbers were prime. Unfortunately, this is False. Leonhard Euler showed in 1732 that

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

Exercise. Prove that if $2^k + 1$ is an odd prime, then k is a power of 2.

Fermat numbers that are prime are called, naturally, **Fermat primes**. To this day there are still only 5 known Fermat primes, and it is known that 318 Fermat numbers are composite. Here are some open questions:

- Is F_n composite for all $n > 4$?
- Are there infinitely many Fermat primes?
- Are there infinitely many composite Fermat numbers?
- Does a Fermat number exist that is not **square free**, that is, the highest power of a prime in its prime factorisation is 1?

How mysterious. So, how does one go about showing that a Fermat number is prime or composite? Well, we have the following primality test, called **Pepin's test**.

Proposition 56 (Pepin's Test)**.** *If $n \geq 1$, then F_n is prime if and only if $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.*

Proof. First note that $2^{2k} \equiv 4 \pmod{12}$, so $F_n \equiv 5 \pmod{12}$. Now, suppose F_n is prime. Then by a result earlier, $[3] \notin Q_p$ so $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$ by Euler's criterion.

Conversely, suppose $[3]^{\frac{F_n-1}{2}} = [-1]$ in $\mathbb{Z}_{F_n}$. Squaring we get $[3]^{F_n-1} = [1]$ in $\mathbb{Z}_{F_n}$. Let p be a prime divisor of F_n. Then $[3]^{F_n-1} = [1]$ in $\mathbb{Z}_p$. Let $m = \text{ord}([3]) \in \mathbb{Z}_p^*$, and we can conclude that $m \mid F_n - 1$. Therefore $m = 2^k$ for some $k \leq 2^n$. Now, since p is odd, we have

$$[3]^{2^{2^n-1}} = [3]^{\frac{F_n-1}{2}} = [-1] \neq [1]$$

in $\mathbb{Z}_p$. Therefore $k = 2^n$ and $m = 2^{2^n} = F_n - 1$. But m divides $p - 1$, so $F_n - 1 \mid p - 1$, implying $F_n \leq p$. Alas, we conclude $F_n = p$. ∎

Exercise. Prove that if F_n is prime, then [3] is a generator of $\mathbb{Z}_{F_n}^*$.

This is another way to show that $F_3 = 257$ is prime, in fact you should try it yourself! Pepin's test has been used to show that several Fermat numbers are composite with the help of computers.

Lecture 27 - 10/07

6.5 Quick diversion: The Chinese Remainder Theorem

Somehow, so far in the course we haven't formally talked about the so called Chinese Remainder theorem. So without further adieu, here it is.

I'm thinking of a number that when I divide it by 5 it leaves a remainder of 2, and when I divide it by 7 it leaves a remainder of 4. What is it?

We could stare at this problem at start listing off all the numbers that leave a remainder of 2 when divided by 5. In fact, let's do that:

$$7, 12, 17, 22, 27, 32, 37, 42, 47, 52, 57, 62, 67, 72, ...$$

Now we stare at this and look for numbers that leave a remainder of 3 when divided by 7. Look, 32 works! And so does 67.

Let's try to approach this with a little more sophistication and class. We are looking for an integer x such that

$$x \equiv 2 \pmod 5 \quad \text{and} \quad x \equiv 4 \pmod 7.$$

So, we have $x = 2 + 5t$ and $x = 4 + 7s$ for some integers t and s. Rearranging this gives the linear diophantine equation

$$5t - 7s = 2.$$

Since $\gcd(5, 7) = 1$, we know there's a solution. The integers $t = -1$ and $s = -1$ work. If we plug that back into our original problem, we get $x = 2 + 5(-1) = -3$. Sure enough, -3 is also a solution, one that we didn't find above!

However, we know there are infinitely many solutions to a linear diophantine equation like this. In fact, for this particular linear diophantine equation, the complete set of solutions is

$$\{(s, t) : s = -1 + 5n, t = -1 + 7n, n \in \mathbb{Z}\}.$$

So in fact, let's plug this back in to the original problem. We have $x = 2+5(-1+7n) = -3+35n$. We could have also done it by substituting the value of s instead of the value of t, which would give $x = 4 + 7(-1 + 5n) = -3 + 35n$. Either way, we get $x \equiv 3 \pmod{35}$.

There are two important things to notice in this example, both which follow from the fact that $\gcd(5, 7)$ are coprime. First, there is always going to be a solution to the linear diophantine equation, which means there will always be a solution to our original problem. Second, the set of solutions to the original problem forms a unique congruence class in $\mathbb{Z}_{35}$, and of course, $35 = 5 \cdot 7$.

Let's prove this in general.

Theorem 57 (The Chinese Remainder Theorem)**.** *Let n and m be coprime positive integers, and let $a, b \in \mathbb{Z}$. The set of integers x satisfying*

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

forms a unique congruence class in $\mathbb{Z}_{nm}$.

Proof. We will first show existence of the desired congruence class in $\mathbb{Z}_{nm}$. Consider the linear diophantine equation

$$sm - tn = a - b.$$

Since $\gcd(m, n) = 1$, there is a solution $s = s_0$ and $t = t_0$. Let $k \in \mathbb{Z}$ and let $x = a + t_0 n + kmn$. Then $x \equiv a \pmod{n}$. Rearranging the linear diophantine equation gives $a + t_0 n = b + s_0 m$ so we also have $x = b + s_0 m + kmn$ and $x \equiv b \pmod{m}$. Therefore any integer congruent to $x \pmod{nm}$ satisfies the desired condition.

For uniqueness, suppose there is an integer y such that $y \equiv a \pmod{n}$ and $y \equiv b \pmod{m}$. Then $y = a + t_1 n = b + s_1 m$ for some $t_1, s_1 \in \mathbb{Z}$. Rearranging gives $s_1 m - t_1 n = a - b$. However we know $s_0 m - t_0 n = a - b$, so putting these together gives

$$(s_1 - s_0)m = (t_1 - t_0)n.$$

Therefore $m \mid (t_1 - t_0)n$, but since $\gcd(n, m) = 1$, we must have $m \mid t_1 - t_0$. So there exists an $l \in \mathbb{Z}$ so that $ml = t_1 - t_0$. Therefore

$$y = a + t_1 n = a + (t_0 + ml)n = a + t_0 n + lmn = x + lmn.$$

Alas, $y \equiv x \pmod{nm}$, completing the proof. ■

Note that although this is an existence proof, it does provide an algorithm to solve problems like this. It comes down to solving some linear diophantine equation, which the Euclidean Algorithm can help us with!

Exercise. Find the set of all integers that are one more than a multiple of 7, 11, and 13.

Example. In the previous section, we found out that if $p \equiv 1 \pmod{4}$ and $p \equiv 2 \pmod{3}$, then $(\frac{3}{p}) = -1$. By the chinese remainder theorem, this is equivalent to the condition that $p \equiv 5 \pmod{12}$. In this case, 3 and 4 are small enough that we can just run through the numbers that are congruent to $1 \pmod{3}$ in between 0 and 11, and once we've found one solution, we've found them all!

Example. Let's find an interesting element of Q_{35}. We know $35 = 5 \cdot 7$, and we know $[4] \in Q_5$ and $[1] \in Q_7$. By the Chinese remainder theorem, there is a unique congruence class $[a] \in \mathbb{Z}_{35}$ so that $[a] \equiv [4]$ in $\mathbb{Z}_5$ and $[a] \equiv [1]$ in $\mathbb{Z}_7$. That class is $[a] = [29]$. Now let's show that $[29] \in Q_{35}$.

We know in $\mathbb{Z}_7$, $[1]^2 = [a]$, and in $\mathbb{Z}_5$, $[2]^2 = [a]$. So if we find the unique class $[b] \in \mathbb{Z}_{35}$ so that $[b] = [2]$ in $\mathbb{Z}_5$ and $[b] = [1]$ in $\mathbb{Z}_7$, this may be a good candidate! That class is $[b] = [22]$. And sure enough, in $\mathbb{Z}_{35}$, $[22]^2 = [484] = [29]$. How about that.

Exercise. Find all the elements $[b] \in \mathbb{Z}_{35}$ so that $[b]^2 = [29]$.

Lecture 28 - 12/07: Guest lecture

Lecture 29 - 14/07

The last example is hinting at something more with the Chinese remainder theorem. Not only does the theorem give us a way to take an element of $\mathbb{Z}_n$ and an element of $\mathbb{Z}_m$, and define a unique element of $\mathbb{Z}_{nm}$, but the way this happens plays nicely with the addition and multiplication in all three of $\mathbb{Z}_n$, $\mathbb{Z}_m$, and $\mathbb{Z}_{nm}$. Let's prove a special case of this phenomenon that we need and we'll leave the general version as an exercise.

Proposition 58. *Let n and m be positive coprime integers. Let $[a] \in Q_n$, $[b] \in Q_m$, and let $[c] \in \mathbb{Z}_{nm}$ be the unique congruence class so that $[a] = [c]$ in $\mathbb{Z}_n$ and $[b] = [c]$ in $\mathbb{Z}_m$. Then $[c] \in Q_{nm}$.*

Proof. First note that by Lemma 28, since $\gcd(c, n) = \gcd(c, m) = 1$, $\gcd(c, nm) = 1$, so $[c] \in \mathbb{Z}_{nm}^*$. Now suppose $[s]^2 = [a]$ in $\mathbb{Z}_n$, and $[t]^2 = [b]$ in $\mathbb{Z}_m$, and let $[z]$ be a congruence class in $\mathbb{Z}_{mn}$ so that $[z] = [s]$ in $\mathbb{Z}_n$ and $[z] = [t]$ in $\mathbb{Z}_m$ (note that such a $[z]$ exists by the Chinese remainder theorem). Then $[z]^2 = [s]^2 = [a]$ in $\mathbb{Z}_n$, and $[z]^2 = [t]^2 = [b]$ in $\mathbb{Z}_m$. By the uniqueness of the Chinese remainder theorem, we must have $[z]^2 = [c]$ in $\mathbb{Z}_{mn}$, so $[c] \in Q_{nm}$. ■

Exercise. Let n and m be positive coprime integers. Let $[a_1], [b_1] \in \mathbb{Z}_n$ and $[a_2], [b_2] \in \mathbb{Z}_m$. Let $[c], [d] \in \mathbb{Z}_{nm}$ be the unique congruence classes so that in $\mathbb{Z}_n$, $[c] = [a_1]$ and $[d] = [b_1]$, and in $\mathbb{Z}_m$, $[c] = [a_2]$ and $[d] = [b_2]$. Prove that in $[c] + [d]$ is the unique congruence class in $\mathbb{Z}_{nm}$ so that $[c]+[d] = [a_1]+[b_1]$ in $\mathbb{Z}_n$ and $[c]+[d] = [a_2]+[b_2]$ in $\mathbb{Z}_m$. Prove that $[c][d]$ is the unique congruence class in $\mathbb{Z}_{nm}$ so that $[c][d] = [a_1][b_1]$ in $\mathbb{Z}_n$ and $[c][d] = [a_2][b_2]$ in $\mathbb{Z}_m$.

Exercise. Let $f(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, and let n and m be positive coprime integers. Prove that $[a_d]x^d + \cdots + [a_1]x + [a_0] \in \mathbb{Z}_{nm}[x]$ has a root if and only if $[a_d]x^d + \cdots + [a_1]x + [a_0] \in \mathbb{Z}_n[x]$ and $[a_d]x^d + \cdots + [a_1]x + [a_0] \in \mathbb{Z}_m[x]$ both have a root.

6.6 Quadratic residues in arbitrary moduli

We will finish the section on quadratic residues with an example of a seriously cool polynomial. One that has a root in $\mathbb{Z}_n$ for every positive integer n, but no roots in $\mathbb{Z}$! To do this, we need to study quadratic residues mod n, where n is not a prime.

Proposition 59. *Let p be an odd prime, e a positive integer. Then $[a] \in Q_p$ if and only if $[a] \in Q_{p^e}$.*

Proof. Suppose $[a] = [b]^2$ in $\mathbb{Z}_{p^e}$. Then since $p \mid p^e$, $[a] = [b]^2$ in $\mathbb{Z}_p$. For the converse, we will rely on the (unproved in these notes) fact that $\mathbb{Z}_{p^e}$ admits a generator. Let $[g]$ be a generator of $\mathbb{Z}_{p^e}^*$. Then there are powers $k_1, \ldots, k_{p-1}$ of $[g]$ so that $[g]^{k_i} = [i]$ in $\mathbb{Z}_{p^e}$. Again, since $p \mid p^e$, this implies $[g]^{k_i} = [i]$ in $\mathbb{Z}_p$ and so $[g]$ is a generator of $\mathbb{Z}_p^*$. Now suppose $[a] \in Q_p$. Then $[g]^k = [a]$ in $\mathbb{Z}_{p^e}$ for some $k \in \mathbb{Z}$. Therefore $[g]^k = [a]$ in $\mathbb{Z}_p$. Then by Proposition 48, k is even. Therefore $[a] \in Q_{p^e}$. ■

In order to get to the promised polynomial, we need to know how squares behave in moduli that are a power of two. We will leave the next proposition unproven, not because it is particularly hard, but because it will take too much time to go through. The proof is left as an exercise.

Proposition 60. *Let e be a positive integer and $[a] \in \mathbb{Z}_{2^e}^*$. Then*

- *$[a] \in Q_2$,*
- *$[a] \in Q_4$ if and only if $[a] = [1]$ in $\mathbb{Z}_4$,*
- *for $e \geq 3$, $[a] \in Q_{2^e}$ if and only if $a \equiv 1 \pmod 8$.*

So, for example,

$$Q_8 = \{[1]\} \quad \text{and} \quad Q_{16} = \{[1], [9]\} \quad \text{and} \quad Q_{32} = \{[1], [9], [17], [25]\}.$$

In particular, any integer that is congruent to 1 (mod 8) is a square in $\mathbb{Z}_{2^e}$ for all positive integers e.

Now for the promised polynomial.

Example. Consider the polynomial $f(x) = (x^2 - 13)(x^2 - 17)(x^2 - 221)$. Since none of $13, 17$, and 221 are perfect squares, $f(x)$ does not have an integer root. We wish to show that $f(x) \in \mathbb{Z}_n[x]$ has a root for every positive integer n.

Fix an positive integer n. It suffices to show at least one of $13, 17$, or 221 is in Q_n. Let $n = p_1^{e_1} \cdots p_k^{e_k}$. By the Chinese remainder theorem and Proposition 59, $[a] \in Q_n$ if and only if $[a] \in Q_{p_i}$ for all i. Therefore, ignoring powers of 2 for the moment, it suffices to show that for every odd prime p, at least one of $[13] \in Q_p$, $[17] \in Q_p$, or $[221] \in Q_p$ is true.

If $p = 2$, then since $17 \equiv 1 \pmod 8$, $[17] \in Q_{2^e}$ for all e. So let p be an odd prime. If $p = 13$, then $[17] = [4]$ in $\mathbb{Z}_{13}$, so $[17] \in Q_{13}$. If $p = 17$, $(\frac{13}{17}) = (\frac{17}{13}) = 1$, so $[13] \in Q_{17}$. Finally, for any other odd prime p we have $(\frac{13}{p})(\frac{17}{p}) = (\frac{221}{p})$ so at least one of $[13]$, $[17]$, or $[221]$ is in Q_p.

Therefore $f(x)$ has a root in $\mathbb{Z}_n$ for all positive integers n, but no root in $\mathbb{Z}$. Amazing.

Lecture 30 - 17/07

7 Multiplicative functions

You may have noticed by now that in number theory, we find ourselves counting things. A lot. For example, $\varphi(n)$ counts the number of congruence classes in $\mathbb{Z}_n^*$. We may wish to know how many generators there are for $\mathbb{Z}_n^*$. Once we have the prime factorisation of a number, we can easily count the number of divisors. Or perhaps, we wish to know how many quadratic residues there are in $\mathbb{Z}_n$.

Before we make a definition, let's see what's interesting about some of these functions. Consider Euler's phi function $\varphi(n) = |\mathbb{Z}_n^*|$. We know that if $\gcd(n, m) = 1$, $\varphi(nm) = \varphi(n)\varphi(m)$. This makes things awfully convenient if we want to compute $\varphi(n)$ in general. This property pops up over and over when counting things to do with the integers.

Here are some examples of multiplicative functions before we give the general definition.

Example. Euler's phi function, $\varphi(n) = |\mathbb{Z}_n^*|$ is an example of a multiplicative function. We know that when $\gcd(n, m) = 1$, $\varphi(nm) = \varphi(n)\varphi(m)$.

Example. The function $\tau(n)$ is defined to be the number of positive divisors of n. So, $\tau(12) = 6$ since the positive divisors of 12 are $1, 2, 3, 4, 6$, and 12.

The function $\sigma(n)$ is defined to be the sum of the positive divisors of n. So, $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$.

Both τ and σ are called **divisor functions**, and we can write them

$$\tau(n) = \sum_{d|n} 1 \quad \text{and} \quad \sigma(n) = \sum_{d|n} d.$$

We will see a little later on that whenever $\gcd(n, m) = 1$, $\tau(nm) = \tau(n)\tau(m)$ and $\sigma(nm) = \sigma(n)\sigma(m)$, although you can prove these properties directly now if you'd like!

Exercise. Prove that if $\gcd(n, m) = 1$, $\tau(nm) = \tau(n)\tau(m)$ and $\sigma(nm) = \sigma(n)\sigma(m)$.

Exercise. Prove that the function $f(n) = |Q_n|$ has the property that whenever $\gcd(n, m) = 1$, $f(nm) = f(n)f(m)$.

All of these functions count something that depends on a positive integer n. So they are functions that eat positive integers, and generally spit out integers, although the following definition allows the functions to take value in the complex numbers.

Definition. An **arithmetic function** is a function $f : \mathbb{Z}_{>0} \to \mathbb{C}$. A **multiplicative function** is an arithmetic function f satisfying $f(nm) = f(n)f(m)$ whenever $\gcd(n, m) = 1$.

For our first result about multiplicative functions, for a positive integer n, let $D_n = \{a \in \mathbb{Z}_{>0} : a \mid n\}$, that is, the set of positive divisors of n.

Lemma 61. *Let n and m be positive coprime integers. Then the function $h : D_n \times D_m \to D_{nm}$ given by $h(a, b) = ab$ is a bijection.*

Proof. This proof is an exercise. ■

We now have a sweet little lemma that helps us easily prove some functions are indeed multiplicative.

Lemma 62. *Let g be a multiplicative function and $f(n) = \sum_{d|n} g(d)$ for all n. Then f is a multiplicative function.*

Proof. Let n and m be positive coprime integers. Then $f(nm) = \sum_{d|nm} g(d)$. However, by the previous lemma,

$$f(nm) = \sum_{a|n} \sum_{b|n} g(ab) = \sum_{a|n} \sum_{b|n} g(a)g(b)$$

since if $a \mid n$ and $b \mid m$, $\gcd(a, b) = 1$. We can rewrite the latest expression as

$$\sum_{a|n} \sum_{b|n} g(a)g(b) = \left(\sum_{a|n} g(a) \right) \left(\sum_{b|n} g(b) \right)$$

so $f(nm) = f(n)f(m)$ as required. ■

To apply this lemma, let's introduct the following multiplicative functions.

Definition. Define multiplicative functions $u(n) = 1$ and $N(n) = n$ for all $n \in \mathbb{Z}_{>0}$. The function u is sometimes referred to as the **unit function**.

Note that both N and u are multiplicative.

Theorem 63. *The divisor functions τ and σ are multiplicative.*

Proof. We have $\tau(n) = \sum_{d|n} 1 = \sum_{d|n} u(d)$ and $\sigma(n) = \sum_{d|n} N(d)$. Therefore τ and σ are multiplicative by Lemma 62. ■

Exercise. Show that for every integer $k \geq 0$, the function $\sigma_k(n) = \sum_{d|n} d^k$ is multiplicative. Note that $\sigma_0 = \tau$ and $\sigma_1 = \sigma$.

Example. Let's write down a formula for $\tau(n)$ and $\sigma(n)$ in terms of the prime factorisation of n.

Let $n = p_1^{e_1} \cdots p_k^{e_k}$. Since τ and σ are multiplicative, we have

$$\tau(n) = \prod_{i=1}^{k} \tau(p_i^{e_i}) \quad \text{and} \quad \sigma(n) = \prod_{i=1}^{k} \sigma(p_i^{e_i}).$$

So, we just need to work out how τ and σ behave on prime powers.

The divisors of p^e are $1, p, p^2, \ldots, p^e$. Therefore $\tau(p^e) = e + 1$ and

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}$$

since $\sigma(p^e)$ is just a geometric series. Therefore

$$\tau(n) = \prod_{i=1}^{k} (e_i + 1) \quad \text{and} \quad \sigma(n) = \prod_{i=1}^{k} \left(\frac{p_i^{e_i+1} - 1}{p_i - 1} \right).$$

Lecture 31 - 19/07

7.1 Möbius inversion

Let's gather up a few similar looking identities from the previous sections.

$$N(n) = \sum_{d|n} \varphi(d)$$
$$\tau(n) = \sum_{d|n} u(d)$$
$$\sigma(n) = \sum_{d|n} N(d).$$

Equations like this, relate one multiplicative function with another. It turns out, there is a neat little way to invert these relations, and it relies on a surprising little function called the Möbius function.

Definition. Let $n = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorisation of n. We say n is **square free** if $e_i = 1$ for all i.

Exercise. Prove that n is square free if and only if the only perfect square dividing n is 1, hence justifying the name.

Definition. Define the **Möbius function** $\mu : \mathbb{Z}_{>0} \to \mathbb{C}$ by

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not square free} \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k, \text{ where } p_i \text{ are distinct primes.} \end{cases}$$

So, for example, $\mu(p) = -1$ for any prime p, and $\mu(15) = \mu(3 \cdot 5) = (-1)^2 = 1$. Essentially, the Möbius function keeps track of whether or not there are an even or odd number of prime factors in a square-free number.

Proposition 64. *The Möbius function is multiplicative.*

Proof. Let m and n be coprime positive integers. If one of them is not square free, then mn is not square free and $\mu(m)\mu(n) = \mu(mn) = 0$. Suppose $m = p_1 p_2 \cdots p_t$ and $n = q_1 q_2 \cdots q_s$ where the p_i are distinct primes and the q_i are distinct primes. Since $\gcd(m, n) = 1$, the set of q_i and p_i are disjoint, so $mn = p_1 \cdots p_t q_1 \cdots q_s$ is square free. Therefore

$$\mu(mn) = (-1)^{s+t} = (-1)^s (-1)^t = \mu(m)\mu(n)$$

as desired. ∎

Lecture 32 - 21/07

Let's see what we can build out of this function. We'll investigate the multiplicative function $I(n) = \sum_{d|n} \mu(d)$.

When $n = 1$ we have $I(1) = \mu(1) = 1$. We know I is multiplicative, so let's figure out what it does to prime powers. We have

$$I(p^e) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^e) = \mu(1) + \mu(p) = 0.$$

Therefore we immediately conclude the following for $n \in \mathbb{Z}_{>0}$:

$$I(n) = \sum_{d|n} \mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

We'll see little later why we call this function I (for identity). The Möbius function seems a little ad-hoc, but it turns out to play a vital role in the study of multiplicative functions.

Theorem 65 (Möbius inversion formula)**.** *Let $f : \mathbb{Z}_{>0} \to \mathbb{C}$ be an arbitrary function, and define $F(n) = \sum_{d|n} f(d)$ for all $n \in \mathbb{Z}_{>0}$. Then*

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Conversely, if for all $n \in \mathbb{Z}_{>0}$, $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$, then $F(n) = \sum_{d|n} f(d)$.

Proof. We have

$$\begin{aligned} \sum_{d|n} \mu(d) F(\frac{n}{d}) &= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') \\ &= \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) \\ &= \sum_{d'|n} f(d') I(\frac{n}{d'}) \\ &= f(n). \end{aligned}$$

Conversely, first note that

$$f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d'|n} \mu(\frac{n}{d'}) F(d').$$

Then

$$\sum_{d|n} f(d) = \sum_{d|n} f(\frac{n}{d}) = \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(\frac{n}{dd'}) F(d') = \sum_{d'|n} F(d') \mu(\frac{n}{d'}) = F(n)$$

completing the proof. ∎

This proof is rather opaque, so it's a good exercise to go through it line by line, justifying each step and trying to build some intuition.

Exercise. Justify each step in the previous proof.

The proof isn't terribly important, but the result does yield some interesting identities.

Example. Let's apply the Möbius inversion formula to the equation $N(n) = \sum_{d|n} \varphi(d)$. We have

$$\varphi(n) = \sum_{d|n} \mu(d) N(\frac{n}{d}) = \sum_{d|n} \frac{n\mu(d)}{d} = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Exercise. Apply the Möbius inversion formula to the following equations. What comes out?

$$I(n) = \sum_{d|n} \mu(d)$$
$$\tau(n) = \sum_{d|n} u(n)$$
$$\sigma(n) = \sum_{d|n} N(n).$$

7.2 The Dirichlet product

We've seen expressions of the forum $F(n) = \sum_{d|n} f(d)$ or even $F(n) = \sum_{d|n} f(d)g(\frac{n}{d})$. The latter is a way to combine two arithmetic functions to get a new arithmetic function, and will provide a surprising amount of structure to the set of all multiplicative functions.

Definition. Let f and g be arithmetic functions. Their **Dirichlet product** or **convolution** is the function defined by

$$f * g(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{de=n} f(d)g(e).$$

So, using this notation, we have the following.

$$N = \varphi * u$$
$$\tau = u * u$$
$$\sigma = N * u$$
$$I = \mu * u.$$

The Möbius inversion formula can now be stated as follows. If $f = g^* u$ then $g = f^* \mu$.

Here are some useful, and familiar, properties of the Dirichlet product.

Proposition 66. *For all arithmetic functions f, g, and h we have*

- $f * g = g * f$,
- $(f * g) * h = f * (g * h)$,
- $f * I = f$.

Proof. The proof of the first two are an exercise. For the last one we have

$$f * I = \sum_{d|n} f(d) I(\frac{n}{d})$$

and since $I(\frac{n}{d}) = 0$ unless $d = n$ when it is 1, we have

$$\sum_{d|n} f(d) I(\frac{n}{d}) = f(n)$$

and so $f * I = f$. ■

So in some sense, the function I is the identity with respect to the operation $*$ on the set of all arithmetic functions. The properties $*$ satisfies should be reminiscent of properties satisfied by addition and multiplication on the integers.

Through this lens, we have already seen that some arithmetic functions have inverses! For example, the equation $\mu * u = I$ means that $\mu^{-1} = u$ (which maybe provides a glimpse as to why μ turns out to be so important). In fact, we can now give a very quick proof of the Möbius inversion formula:

Suppose $f = g * u$. Then $f * \mu = (g * u) * \mu = g * (\mu * u) = g * I = g$. Neat hey?

Exercise. Let f be an arithmetic function with $f(1) \neq 0$. Prove that there exists an arithmetic function g so that $f * g = 1$.

Exercise. Compute $\tau * \mu$ and $\sigma * \mu$.

Exercise. Find the inverse of τ with respect to the Dirichlet product.

Of course, we are mostly interested in multiplicative functions. The next proposition tells us that the Dirichlet product plays very nicely with multiplicative functions.

Proposition 67. *Let f and g be multiplicative functions. Then f^*g is a multiplicative function, and if $f(1) \neq 0$, then f^{-1} is also multiplicative.*

Proof. This proof is also an exercise, but is similar to the proof of Lemma 62. ■

This tells us that the set of multiplicative functions (ignoring the function $f(n) = 0$) forms a group under the Dirichlet product. We are now in a position to prove the following intriguing result.

Lecture 33 - 24/07

Proposition 68. *Let f and g be arithmetic functions, and suppose that $f(n) = \sum_{d|n} g(d)$. Then f is multiplicative if and only if g is multiplicative.*

Proof. We have $f = g * u$. Suppose g is multiplicative. Then since u is multiplicative, f is multiplicative. Conversely, suppose f is multiplicative. Then since $g = f^*\mu$ and since μ is multiplicative, g is multiplicative. ■

This actually gives us a new, although maybe unenlightening, proof that Euler's phi function $\varphi(n)$ is multiplicative. This is because $N(n) = \sum_{d|n} \varphi(d)$, and we know that N is multiplicative!

8 Continued fractions

Let's do something completely different, the Euclidean algorithm. Here is the Euclidean algorithm on the pair of integers 203, 77.

$$\begin{aligned} 203 &= 2 \cdot 77 + 49 \\ 77 &= 1 \cdot 49 + 28 \\ 49 &= 1 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7 \\ 21 &= 3 \cdot 7 + 0. \end{aligned}$$

But, I want to write this slightly differently:

$$\begin{aligned}\frac{203}{77} &= 2 + \frac{49}{77}\\ \frac{77}{49} &= 1 + \frac{28}{49}\\ \frac{49}{28} &= 1 + \frac{21}{28}\\ \frac{28}{21} &= 1 + \frac{7}{21}\\ \frac{21}{7} &= 3 + \frac{0}{7}.\end{aligned}$$

In fact, we can write this whole process in a curious looking form called a continued fraction as follows.

The first equation can be rewritten as

$$\frac{203}{77} = 2 + \frac{1}{\left(\frac{77}{49}\right)}$$

at which point the second equation comes in to the picture and gives

$$\begin{aligned}\frac{203}{77} &= 2 + \frac{1}{1 + \frac{28}{49}}\\ &= 2 + \frac{1}{1 + \frac{1}{\left(\frac{49}{28}\right)}}.\end{aligned}$$

Of course, now the third equation comes in, yielding

$$\frac{203}{77} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{21}{28}}}.$$

Continuing in this fashion through the entire Euclidean algorithm gives us the **continued fraction expansion** of $\frac{203}{77}$

$$\frac{203}{77} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}}}.$$

This is great, but who cares? I mean, it's fun to write down nested fractions like this and all. But at some point, I'm going to be too lazy to write down continued fractions all the way to their completion. Let's see what number comes out if I just decide to stop after some point.

Let's first note that $\frac{203}{77} \approx 2.63636363....$ Here is what comes out of our truncated continued

fractions.

$$\begin{aligned}
2 &= 2 \\
2 + \frac{1}{1} &= 3 \\
2 + \frac{1}{1 + \frac{1}{1}} &= \frac{5}{2} = 2.5 \\
2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} &= \frac{8}{3} = 2.666... \\
2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}}} &= 2.636363636363...
\end{aligned}$$

Cool! Each successive term appears to be a better and better approximation to our original fraction. Let's try something else, and let's run the Euclidean algorithm on π (stay with me here).

Here are the first few steps of what actually goes on forever (becuse π is irrational).

$$\begin{aligned}
\pi &= 3 + r_1 \\
\frac{1}{r_1} &= 7 + r_2 \\
\frac{1}{r_2} &= 15 + r_3 \\
\frac{1}{r_3} &= 1 + r_4 \\
\frac{1}{r_4} &= 292 + r_5 \\
\frac{1}{r_5} &= 1 + r_6.
\end{aligned}$$

And in fact, the integer parts that appear have been well studied, and here are the first few

$$3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2.$$

So, let's play the game we did above, truncating our continued fraction and seeing what comes out. Here are the first few.

$$\begin{aligned}
3 &= 3 \\
3 + \frac{1}{7} &= \frac{22}{7} = 3.142857142857... \\
3 + \frac{1}{7 + \frac{1}{15}} &= \frac{333}{106} = 3.141509433... \\
3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1}}} &= \frac{355}{113} = 3.1415929203... \\
3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{1}{292}}}} &= \frac{103993}{33102} = 3.14159265301...
\end{aligned}$$

These are all very good approximations of π, and in some sense, they are the best possible approximations for fractions with denominators as large as they are.

Before we continue, we will need some notation. To save us writing out the continued fraction in full each time, we have the following short-hand. For integers $a_0, \ldots, a_n$ denote the continued fraction by

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \frac{1}{a_n}}}}} = [a_0, a_1, a_2, \ldots, a_n].$$

So, we have

$$\frac{203}{77} = \frac{29}{11} = [2, 1, 1, 1, 3]$$
$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, ...]$$

and note that since π is irrational, the continued fraction continues (although not in any percievable pattern).

Exercise. Prove that the continued fraction expansion of a real number x is finite if and only if $x \in \mathbb{Q}$.

Exercise. Compute the continued expansion expansion of e.

Lecture 34 - 26/07

Let's compute the continued fraction expansion of $\sqrt{3}$. This time, instead of using a computer to figure out the integer part, we will keep all our computations in exact form, and see how far we can get.

We know $\sqrt{3}$ is between 1 and 2. So the first line in our computation will be $\sqrt{3} = 1 + (\sqrt{3} - 1)$. Then we flip the fraction part, and repeat. By rationalising the denominator we have $\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}$. Since $\sqrt{3} + 1$ is between 2 and 3, we know $\frac{\sqrt{3}+1}{2} = 1 + \frac{\sqrt{3}-1}{2}$. Again, flipping the fractional part and rationalising the denominator gives $\frac{2}{\sqrt{3}-1} = \sqrt{3} + 1$, which we know is between 2 and 3. This gives $\sqrt{3} + 1 = 2 + (\sqrt{3} - 1)$. Hang on, I swear we've been here before! We know what happens when we get to a fractional part of $\sqrt{3} - 1$. Taking this rambling paragraph and organising it gives

$$\begin{aligned}
\sqrt{3} &= 1 + (\sqrt{3} - 1) \\
\frac{1}{\sqrt{3} - 1} &= 1 + \frac{\sqrt{3} - 1}{2} \\
\frac{2}{\sqrt{3} - 1} &= 2 + (\sqrt{3} - 1) \\
\frac{1}{\sqrt{3} - 1} &= 1 + \frac{\sqrt{3} - 1}{2} \\
\frac{2}{\sqrt{3} - 1} &= 2 + (\sqrt{3} - 1) \\
\frac{1}{\sqrt{3} - 1} &= 1 + \frac{\sqrt{3} - 1}{2} \\
\frac{2}{\sqrt{3} - 1} &= 2 + (\sqrt{3} - 1) \\
&\vdots
\end{aligned}$$

Therefore the continued fraction expansion of $\sqrt{3}$ is

$$\sqrt{3} = [1, 1, 2, 1, 2, 1, 2, 1, 2, \ldots] = [1, \overline{1, 2}].$$

Exercise. Compute the continued fraction expansion of $\sqrt{n}$ for $n = 5, 6, 7, 8, 10$.

Exercise. Find an irrational number x with continued fraction expansion $[1, 1, 1, 1, 1, ...]$.

8.1 Convergents and approximating irrationals

As we saw in the introduction to this chapter, the truncated continued fractions for π appear to approximate π very well, and the longer we make our truncated continued fraction, the better the approximation. These truncated continued fractions are called convergents.

Definition. Let x be an irrational number and $x = [a_0, a_1, \ldots]$ its continued fraction expansion. The nth convergent of x is the rational number

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n].$$

So, the 0th, 1st, 2nd, 3rd, and 4th convergents of π, which we computed above, are 3, $\frac{22}{7}$, $\frac{333}{106}$, $\frac{355}{113}$, and $\frac{103993}{33102}$ respectively. Let's compute the first 4 convergents of $\sqrt{3}$. We have

$$\begin{aligned}
\frac{p_0}{q_0} &= 1 \\
\frac{p_1}{q_1} &= 1 + \frac{1}{1} = 2 \\
\frac{p_2}{q_2} &= 1 + \frac{1}{1 + \frac{1}{2}} = \frac{5}{3} \\
\frac{p_3}{q_3} &= 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}} = \frac{7}{4}.
\end{aligned}$$

The decimal expansion for $\sqrt{3}$, up to 10 decimal places, is

$$\sqrt{3} = 1.7320508075...$$

That's pretty close to the 3rd convergent, which is $\frac{7}{4} = 1.75$. This is pretty unimpressive though, since I could have come up with this approximation without the Euclidean algorithm! But, let's look at the 7th convergent:

$$\frac{p_7}{q_7} = \frac{97}{56} = 1.732142857...$$

which is equal to $\sqrt{3}$ when both are rounded to 4 decimal places! This is pretty impressive, because if you asked me to approximate $\sqrt{3}$ to 4 decimal places with a rational number I would have chosen $\frac{17321}{10000}$. My approximation is pretty good, but the denominator has 5 digits. The denominator of the 7th convergent only has 2 digits! In a very precise sense, the convergents give rise to the best approximations of $\sqrt{3}$.

Definition. Let x be a real number. The rational number $\frac{p}{q}$ (written with $\gcd(p, q) = 1$) is a **best rational approximation** to x if

$$\left| x - \frac{p}{q} \right| = \min \left\{ \left| x - \frac{p'}{q'} \right| : q' \leq q \right\}.$$

Here is the main theorem about how much convergents, well, converge.

Theorem 69. *For any real number x, the convergents of x are best approximations of x.*

We won't prove this in these notes, but it is a good thing to think about.

So, for example, if you wanted a better rational approximation of $\sqrt{3}$ than $\frac{97}{56}$, you would need a fraction with denominator at least 57.

Exercise. Let $\phi = \frac{1+\sqrt{5}}{2}$. Find the best rational approximation $\frac{p}{q}$ of ϕ such that $q \leq 377$.

Exercise. Let c_n be the nth convergent of an irrational number x. Prove that $\{c_n\}$ is a Cauchy sequence, and so the limit $\lim_{n\to\infty} c_n$ exists. What is the limit?

So we know convergents give best approximations. What about the other way around? Ordinarily when I ask a question like this, it's because the answer is yes. This time, the answer is no. Mathematics is often beautiful and the theorems are often neat, but just because a statement is beautiful and neat, doesn't mean it's true.

Let's look at the first few convergents of π again.

$$\begin{aligned}
\frac{p_0}{q_0} &= 3 = 3 \\
\frac{p_1}{q_1} &= \frac{22}{7} = 3.142857142857... \\
\frac{p_2}{q_2} &= \frac{333}{106} = 3.141509433... \\
\frac{p_3}{q_3} &= \frac{355}{113} = 3.1415929203... \\
\frac{p_4}{q_4} &= \frac{103993}{33102} = 3.14159265301...
\end{aligned}$$

The third convergent is accurate to 6 decimal places. The denominator in the fourth convergent has 5 digits. It seems unreasonable to think that there are no best approximations with denominator between 113 and 33102. Indeed this is unreasonable and there are lots of best approximations not in the list of convergents. In fact, here are the first few best approximations (listed in order of increasing denominator)

$$\frac{3}{1}, \frac{13}{4}, \frac{16}{5}, \frac{19}{6}, \frac{22}{7}.$$

Only the first and last of these are convergents of π.

This raises the question, if we have a best rational approximation of a number x, can we tell whether or not it's a convergent? Here are a couple of theorems which we won't prove, that partially answer this question.

Theorem 70 (Dirichlet's Approximation Theorem)**.** *Let x be a real number, and $\frac{p}{q}$ a convergent of x. Then $\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$.*

So, if you have a convergent with a 20-digit denominator, then it will be accurate to about 40 digits.

Theorem 71 (Legendre's Theorem)**.** *If $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$, then $\frac{p}{q}$ is a convergent of x.*

For example, in the very first example we did in this part of the course, we saw that $\frac{8}{3}$ is a convergent of $\frac{29}{11}$. Legendre's theorem could have predicted this! Indeed,

$$\frac{8}{3} - \frac{29}{11} = \frac{1}{33} < \frac{1}{3^2}$$

so $\frac{8}{3}$ must be a convergent of $\frac{29}{11}$.

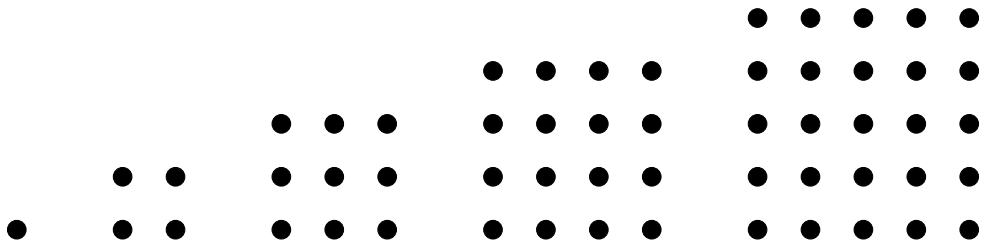
Exercise. Show that the converses of Dirichlet's and Legendre's Theorems are false.

Lecture 35 - 28/07

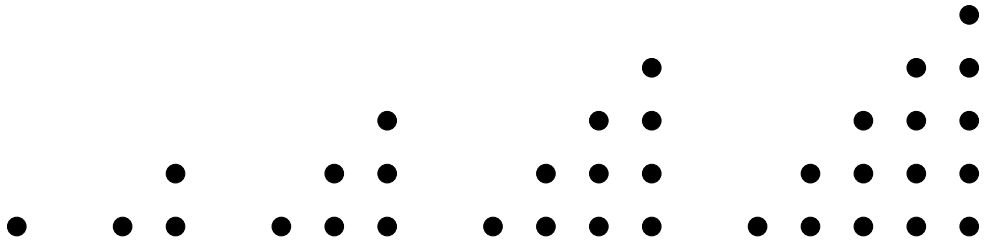
8.2 Pell's equation

One of the motivations for studying the Euclidean algorithm and number theory in general is that it is generally more difficult to solve an equation with integers, than it is with real numbers. We have seen this explicitly when solving linear Diophantine equations.

Let's see another curious example of trying to solve something over the integers. By now we are all familiar with square numbers: $1, 4, 9, 16, 25, ...$ These are called square numbers because, well, they tell us something about the number of things (say coins) you can put in a square.



The nth square number is of course given by n^2. There is the lesser known, but just as pleasant to be around, cousin of the square number, the triangular number. These are the number of things you can arrange into a triangle with base n.



So the first few triangular numbers are $1, 3, 6, 10, 15$ and in fact the nth triangular number is the sum of the first n integers. Thus the nth triangular number is $\frac{n(n+1)}{2}$.

Now, here's a fun question. Can you find a number of dots that can be arranged into both a square, and a triangle? Well, let's list out the first few square numbers and triangular numbers and see if we can find anything.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n^2	1	4	9	16	25	36	49	64	81	100	121	144	169	196	225
$\frac{n(n+1)}{2}$	1	3	6	10	15	21	28	36	45	55	66	78	91	105	120

The blue numbers appear in both lists. The only ones, at least in the first 15 square and triangular numbers, are 1 and 36. Are there others?

Investigating this question further, we want to find integers m and n so that $m^2 = \frac{n(n+1)}{2}$. Rearranging a little gives $(2n+1)^2 = 8m^2 + 1$. If we let $x = 2n+1$ and $y = 2m$ this gives

$$x^2 - 2y^2 = 1.$$

So if we're interested in square triangular numbers (I mean, who isn't?), we're interested in integer solutions to the equation $x^2 - 2y^2 = 1$. Since we are looking at x^2 and y^2, we may as well restrict our attention to $x, y \geq 0$ since we can generate other solutions by just flipping the signs of x and y.

Staring at this equation gives a couple of solutions right off the bat: $(x, y) = (1, 0)$ and $(x, y) = (3, 2)$. The first corresponds to the square-triangular number 0 (which I guess technically works), and the second to the number 1. But this can't be all the solutions, there must be one hiding in the weeds corresponding to the square-triangular number 36. The square number 36 gives $m = 6$ and the triangular number 36 gives $n = 8$. So, it should be the case that $(x, y) = (2n+1, 2m) = (17, 12)$ is another solution. A quick check: $17^2 - 2(12^2) = 289 - 2(288) = 1$. Phew!

So, let's focus on solving the equation $x^2 - 2y^2 = 1$, and those like it, and we'll return to the square triangular numbers later.

Definition. Let $D > 0$ be an integer that is not a perfect square. **Pell's equation** is the equation $x^2 - Dy^2 = 1$.

Let's suppose we did have some solutions to Pell's equation $x^2 - Dy^2 = 1$. The left hand side is curious, and vaguely familiar. If $D = -1$ (which we have explicitly disallowed, but let's continue down the forbidden path anyway), the equation becomes $x^2 + y^2 = 1$, the equation of the unit circle. More importantly, it's the equation satisfied by the complex number $z = x + yi$, if $|z| = 1$. We know in $\mathbb{C}$, that $|z|\,|w| = |zw|$. Therefore, turning solutions to $x^2 + y^2 = 1$ into complex numbers, and multiplying them in $\mathbb{C}$, will yield more solutions! Maybe, if we're lucky, the same kind of thing happens with solutions to $x^2 - Dy^2 = 1$, and solutions correspond to some kinds of numbers with some kind of norm being 1. Let's try this with our couple of solutions to $x^2 - 2y^2 = 1$.

We know $(x_1, y_1) = (3, 2)$ and $(x_2, y_2) = (17, 12)$ are solutions. Let's pretend these are coordinates of numbers that are kind of like the complex numbers, except with D playing the role of -1. Then the corresponding numbers would be $3 + 2\sqrt{2}$ and $17 + 12\sqrt{2}$. Let's multiply these together and see what happens.

$$(3 + 2\sqrt{2})(17 + 12\sqrt{2}) = 51 + (34 + 36)\sqrt{2} + 48 = 99 + 70\sqrt{2}.$$

Now the moment of truth, does $(x_3, y_3) = (99, 70)$ give us a solution to the Pell equation? We have

$$99^2 - 2(70^2) = 9801 - 2(4900) = 1.$$

Amazing! This gives another square triangular number, which is 1225.

Lemma 72. *Suppose (x_1, y_1) and (x_2, y_2) are solutions to Pell's equation $x^2 - Dy^2 = 1$. Then if $x_3 + y_3\sqrt{D} = (x_1 + y_1\sqrt{D})(x_2 + y_2\sqrt{D})$, then (x_3, y_3) is a solution.*

Proof. We have

$$(x_1 + y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = (x_1x_2 + Dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{D}$$

so let $x_3 = x_1x_2 + Dy_1y_2$ and $y_3 = x_1y_2 + x_2y_1$. Then

$$\begin{aligned} x_3^2 - Dy_3^2 &= (x_1x_2 + Dy_1y_2)^2 - D(x_1y_2 + x_2y_1)^2 \\ &= x_1^2x_2^2 + 2Dx_1x_2y_1y_2 + D^2y_1^2y_2^2 - Dx_1^2y_2^2 - 2Dx_1x_2y_1y_2 - Dx_2^2y_1^2 \\ &= (x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) \\ &= 1 \end{aligned}$$

completing the proof. ■

Cool, so if we have a solution to Pell's equation, we can potentially find a bunch more! Let's do this with our solutions that we already have to $x^2 - 2y^2 = 1$. We know $(3, 2)$ is a solution, so let's just take powers of $3 + 2\sqrt{2}$ and see what happens. Here is the result arranged in a helpful table (along with the corresponding square-triangular number).

k	$(3+2\sqrt{2})^k$	solution (x, y)	square-triangular number
1	$3 + 2\sqrt{2}$	$(3, 2)$	1
2	$17 + 12\sqrt{2}$	$(17, 12)$	36
3	$99 + 70\sqrt{2}$	$(99, 70)$	1225
4	$577 + 408\sqrt{2}$	$(577, 408)$	41616
5	$3363 + 2378\sqrt{2}$	$(3363, 2378)$	1413721

We can find infinitely many solutions this way, and thus infinitely many square-triangular numbers!

Exercise. Suppose (x_1, y_1) is a solution to Pell's equation $x^2 - Dy^2 = 1$, with $x_1, y_1 > 0$. Suppose $k, l > 0$. Prove that if $(x_1 + y_1\sqrt{D})^k = (x_1 + y_1\sqrt{D})^l$ then $k = l$. Conclude that if there is one integer solution (x_1, y_1) with $x_1, y_1 > 0$ to the equation $x^2 - Dy^2 = 1$, then there are infinitely many.

Lecture 36 - 31/07

So you have infinitely many of something, the natural question is: Do you have all of them? Well, here's a theorem which we shan't prove because the end of the course is nigh.

Theorem 73. *Let D be a positive integer that is not a perfect square. Then there exists positive integers x_0, y_0 solving Pell's equation $x^2 - Dy^2 = 1$.*

Furthermore, let (x_1, y_1) be the positive solution with the smallest x value (called the **fundamental solution***). Then any other positive solution is of the form (x_k, y_k) where $x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k$ for some positive integer k.*

So, in the case $D = 2$ that we have been playing around with, you can check that there are no solutions with $x = 1$ or $x = 2$, so $(3, 2)$ is the fundamental solution. Therefore all other solutions are of the form (x_k, y_k) where $x_k + y_k\sqrt{2} = (3 + 2\sqrt{2})^k$.

Exercise. Prove that there are no integer solutions to $x^2 - 2y^2 = 1$ with $x = 1$ or $x = 2$.

We are lead, finally, to the last question we shall ask in this course. How do we find the fundamental solution to Pell's equation?

Lemma 74. *Suppose (a, b) is a solution to Pell's equation $x^2 - Dy^2 = 1$. Then $\frac{a}{b}$ is a convergent of $\sqrt{D}$.*

Proof. We have $a^2 - Db^2 = 1$. Implying $(a - b\sqrt{D})(a + b\sqrt{D}) = 1$ and thus

$$a - b\sqrt{D} = \frac{1}{a + b\sqrt{D}} > 0.$$

Therefore $a > b\sqrt{D}$. Now let's see how good an estimate $\frac{a}{b}$ is to $\sqrt{D}$. We have

$$\left|\sqrt{D} - \frac{a}{b}\right| = \frac{a - b\sqrt{D}}{b} = \frac{1}{b(a + b\sqrt{D})} < \frac{1}{b(2b\sqrt{D})} < \frac{1}{2b^2}.$$

Therefore by Legendre's theorem, $\frac{a}{b}$ is a convergent of $\sqrt{D}$. ■

Finally, somewhere to look to find solutions. If we look back at our solutions when $D = 1$ we see each of the solutions do indeed give convergents of $\sqrt{2}$. In fact the 5 solutions listed in the table above are the 1st, 3rd, 5th, 7th, and 9th convergents respectively. That is,

$$\frac{p_1}{q_1} = \frac{3}{2}, \quad \frac{p_3}{q_3} = \frac{17}{12}, \quad \frac{p_5}{q_5} = \frac{99}{70}, \quad \frac{p_7}{q_7} = \frac{577}{408}, \quad \text{and} \quad \frac{p_9}{q_9} = \frac{3363}{2378}.$$

Intriguing.

If Theorem 73 is correct (which it is), we just have to run through the convergents of $\sqrt{D}$ until we find a solution! The first one we find will have the smallest x-value (which is an interesting thing to think about) and therefore it will be our fundamental solution!

Example. Let's find all the solutions to Pell's equation $x^2 - 7y^2 = 1$. To find the fundamental solution, we first compute the continued fraction expansion of $\sqrt{7}$. It turns out to be $[2, \overline{1, 1, 1, 4}]$. Let's compute the first few convergents, and see what they give when plugging them into Pell's equation.

Convergent $\frac{p}{q}$	$p^2 - 7q^2$
$\frac{2}{1}$	-3
$\frac{3}{1}$	2
$\frac{5}{2}$	-3
$\frac{8}{3}$	1

We can stop here since we have found our fundamental solution $(x, y) = (8, 3)$. Then all solutions are of the form (x_k, y_k) where $x_k + y_k\sqrt{7} = (8 + 3\sqrt{7})^k$ for $k > 1$.

Sometimes, the fundamental solution can be quite large and hard to come by. Notably, the fundamental solution to $x^2 - 61y^2 = 1$ is $(x, y) = (1766319049, 226153980)$!

There is a beautiful geometric story to be told regarding the set of all solutions to Pell's equation, but that is a story for another time.

9 That's all folks

We have barely skimmed the surface of the beautiful area of mathematics that is number theory. Hopefully you have gained an appreciation for the richness of the subject. The whole world of number theory, and pure mathematics, is waiting to be rediscovered, or discovered, by you. Your mountain is waiting, so get on your way!

A List of the first 1000 primes

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131
137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263
269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409
419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569
571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719
727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877
881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997 1009 1013 1019 1021 1031
1033 1039 1049 1051 1061 1063 1069 1087 1091 1093 1097 1103 1109 1117 1123 1129 1151 1153
1163 1171 1181 1187 1193 1201 1213 1217 1223 1229 1231 1237 1249 1259 1277 1279 1283 1289
1291 1297 1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399 1409 1423 1427 1429 1433
1439 1447 1451 1453 1459 1471 1481 1483 1487 1489 1493 1499 1511 1523 1531 1543 1549 1553
1559 1567 1571 1579 1583 1597 1601 1607 1609 1613 1619 1621 1627 1637 1657 1663 1667 1669
1693 1697 1699 1709 1721 1723 1733 1741 1747 1753 1759 1777 1783 1787 1789 1801 1811 1823
1831 1847 1861 1867 1871 1873 1877 1879 1889 1901 1907 1913 1931 1933 1949 1951 1973 1979
1987 1993 1997 1999 2003 2011 2017 2027 2029 2039 2053 2063 2069 2081 2083 2087 2089 2099
2111 2113 2129 2131 2137 2141 2143 2153 2161 2179 2203 2207 2213 2221 2237 2239 2243 2251
2267 2269 2273 2281 2287 2293 2297 2309 2311 2333 2339 2341 2347 2351 2357 2371 2377 2381
2383 2389 2393 2399 2411 2417 2423 2437 2441 2447 2459 2467 2473 2477 2503 2521 2531 2539
2543 2549 2551 2557 2579 2591 2593 2609 2617 2621 2633 2647 2657 2659 2663 2671 2677 2683
2687 2689 2693 2699 2707 2711 2713 2719 2729 2731 2741 2749 2753 2767 2777 2789 2791 2797
2801 2803 2819 2833 2837 2843 2851 2857 2861 2879 2887 2897 2903 2909 2917 2927 2939 2953
2957 2963 2969 2971 2999 3001 3011 3019 3023 3037 3041 3049 3061 3067 3079 3083 3089 3109
3119 3121 3137 3163 3167 3169 3181 3187 3191 3203 3209 3217 3221 3229 3251 3253 3257 3259
3271 3299 3301 3307 3313 3319 3323 3329 3331 3343 3347 3359 3361 3371 3373 3389 3391 3407
3413 3433 3449 3457 3461 3463 3467 3469 3491 3499 3511 3517 3527 3529 3533 3539 3541 3547
3557 3559 3571 3581 3583 3593 3607 3613 3617 3623 3631 3637 3643 3659 3671 3673 3677 3691
3697 3701 3709 3719 3727 3733 3739 3761 3767 3769 3779 3793 3797 3803 3821 3823 3833 3847
3851 3853 3863 3877 3881 3889 3907 3911 3917 3919 3923 3929 3931 3943 3947 3967 3989 4001
4003 4007 4013 4019 4021 4027 4049 4051 4057 4073 4079 4091 4093 4099 4111 4127 4129 4133
4139 4153 4157 4159 4177 4201 4211 4217 4219 4229 4231 4241 4243 4253 4259 4261 4271 4273
4283 4289 4297 4327 4337 4339 4349 4357 4363 4373 4391 4397 4409 4421 4423 4441 4447 4451
4457 4463 4481 4483 4493 4507 4513 4517 4519 4523 4547 4549 4561 4567 4583 4591 4597 4603
4621 4637 4639 4643 4649 4651 4657 4663 4673 4679 4691 4703 4721 4723 4729 4733 4751 4759
4783 4787 4789 4793 4799 4801 4813 4817 4831 4861 4871 4877 4889 4903 4909 4919 4931 4933
4937 4943 4951 4957 4967 4969 4973 4987 4993 4999 5003 5009 5011 5021 5023 5039 5051 5059
5077 5081 5087 5099 5101 5107 5113 5119 5147 5153 5167 5171 5179 5189 5197 5209 5227 5231
5233 5237 5261 5273 5279 5281 5297 5303 5309 5323 5333 5347 5351 5381 5387 5393 5399 5407
5413 5417 5419 5431 5437 5441 5443 5449 5471 5477 5479 5483 5501 5503 5507 5519 5521 5527
5531 5557 5563 5569 5573 5581 5591 5623 5639 5641 5647 5651 5653 5657 5659 5669 5683 5689
5693 5701 5711 5717 5737 5741 5743 5749 5779 5783 5791 5801 5807 5813 5821 5827 5839 5843
5849 5851 5857 5861 5867 5869 5879 5881 5897 5903 5923 5927 5939 5953 5981 5987 6007 6011
6029 6037 6043 6047 6053 6067 6073 6079 6089 6091 6101 6113 6121 6131 6133 6143 6151 6163
6173 6197 6199 6203 6211 6217 6221 6229 6247 6257 6263 6269 6271 6277 6287 6299 6301 6311
6317 6323 6329 6337 6343 6353 6359 6361 6367 6373 6379 6389 6397 6421 6427 6449 6451 6469
6473 6481 6491 6521 6529 6547 6551 6553 6563 6569 6571 6577 6581 6599 6607 6619 6637 6653
6659 6661 6673 6679 6689 6691 6701 6703 6709 6719 6733 6737 6761 6763 6779 6781 6791 6793

6803 6823 6827 6829 6833 6841 6857 6863 6869 6871 6883 6899 6907 6911 6917 6947 6949 6959
6961 6967 6971 6977 6983 6991 6997 7001 7013 7019 7027 7039 7043 7057 7069 7079 7103 7109
7121 7127 7129 7151 7159 7177 7187 7193 7207 7211 7213 7219 7229 7237 7243 7247 7253 7283
7297 7307 7309 7321 7331 7333 7349 7351 7369 7393 7411 7417 7433 7451 7457 7459 7477 7481
7487 7489 7499 7507 7517 7523 7529 7537 7541 7547 7549 7559 7561 7573 7577 7583 7589 7591
7603 7607 7621 7639 7643 7649 7669 7673 7681 7687 7691 7699 7703 7717 7723 7727 7741 7753
7757 7759 7789 7793 7817 7823 7829 7841 7853 7867 7873 7877 7879 7883 7901 7907 7919.

B Equivalence Relations and Partitions

Equivalence classes and partitions pop up in just about every area of mathematics, and we will see that both equivalence classes and partitions are two sides of the same coin. It is a common occurrence for us to have a set, and then to consider certain subsets of that set to represent a single element, or to make all the elements in a subset the same.

There are lots of natural examples of equivalence relations.

Example. The rational numbers are the first place you see an equivalence relation, except it's so natural that it's often swept under the rug and we don't even notice! A first attempt at defining the set of rational numbers would be to consider the set

$$\left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \right\}.$$

This looks right, except for the fact that as written, the set thinks that $\frac{2}{4}$ and $\frac{3}{6}$ are different elements. We want them to be the same! To deal with this we say

$$\frac{a}{b} \sim \frac{c}{d} \quad \text{if} \quad ad = bc.$$

Now we can correctly write

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \right\} / \sim$$

which is just fancy notation for "the set $\left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \right\}$ except when $\frac{a}{b} \sim \frac{c}{d}$, we just make them equal". The relation $\sim$ which makes two different things equal is called an **equivalence relation**.

Example. One that you have seen in this course is an equivalence relation on the integers $\mathbb{Z}$. Consider the set of numbers that have the same remainder when divided by 7. Then we can say that two integers $a, b \in \mathbb{Z}$ are equivalent if $7 \mid a - b$. Then this is an equivalence relation (see Proposition 18), and it splits the integers up into 7 disjoint sets, one corresponding to each element of $\mathbb{Z}_7$. In this scenario, we view all the integers which have the same remainder when divided by 7 as the same. Alternatively, we can view this as identifying all of these elements with each other.

Notice that the set of subsets consisting of elements of $\mathbb{Z}$ that are equivalent (which we will soon call equivalence classes) cover all of $\mathbb{Z}$, and no element belongs to two of these subsets. Another way of saying this is that the subsets **partition** $\mathbb{Z}$.

Example. Consider the set $X = \{1, 2, 3, 4, 5, 6\}$ and identify 1 and 2 together, and identify 3, 4, and 6 as the same element. In this case, the equivalence relation identifies each of the subsets $\{1, 2\}, \{3, 4, 6\}, \{5\}$. The idea is that we may as well just consider 1 to be equal to 2, and 3 to be equal to 4 to be equal to 6.

Notice that the subsets that define which elements are equal partition the set X. If we denote equality in this example by $\sim$ we also notice that for all $x, y, z \in X$, $x \sim x$, if $x \sim y$ then $y \sim x$, and if $x \sim y$ and $y \sim z$, then $x \sim z$.

This last example hints at what we would formally want an equivalence relation to be, and we would like it to imitate what we understand "=" to mean. Intuitively in any context, $x = x$ always, if $x = y$ then $y = x$, and if $x = y$ and $y = z$, then $x = z$. Furthermore, if we group equal things together in a set, we should get a partition of that set into subsets consisting of things that are equal!

Let's formalise these ideas. In the next definition, think of a relation as something like $=$ or $\leq$. So something that takes in two elements of a set and gives back that it is either true or false.

Definition. Let X be a set. An **equivalence relation** on X is a relation $\sim$ that satisfies the following properties.

1. $x \sim x$ for all $x \in X$. We say $\sim$ is **reflexive**.
2. If $x \sim y$ then $y \sim x$. We say $\sim$ is **symmetric**.
3. If $x \sim y$ and $y \sim z$, then $x \sim z$. We say $\sim$ is **transitive**.

Definition. Let X be a set and $\sim$ an equivalence relation on X. For $x \in X$, define the **equivalence class of** x by

$$[x] := \{y \in X : y \sim x\}.$$

The set of equivalence classes is denoted by

$$X/\sim := \{[x] : x \in X\}.$$

Definition. Let X be a set. A **partition of** X is a collection of subsets $\{Y_i\}$ such that $Y_i \cap Y_j = \emptyset$ if $i \neq j$, and $\bigcup_i Y_i = X$.

Intuitively a partition is a way to split up your set into a collection of subsets in such a way that every element of X belongs to exactly one of the subsets.

As we have seen above, we can interchange the idea of an equivalence relation on a set with the notion of a partition. Intuitively they come hand in hand, and this is what the next proposition shows.

Proposition 75. *Let X be a set. If $\sim$ is an equivalence relation on X, then the set of equivalence classes of elements in X partition X. Conversely, if we have a partition of X, it arises as the set of equivalnce classes from an equivalence relation on X.*

Proof. Suppose $\sim$ is an equivalence relation on X. Since $x \in [x]$, every element is in an equivalence class. It remains to show that two equivalence classes are disjoint or equal. Suppose $y \in [x_1] \cap [x_2]$, we want to show that $[x_1] = [x_2]$. Let $z \in [x_1]$. Then since $y \in [x_1]$, $z \sim y$ and since $y \in [x_2]$, $y \sim x_2$. By transitivity of $\sim$, $z \sim x_2$ so $z \in [x_2]$. Conversely, if $z \in [x_2]$, $z \sim y$ and $y \sim x_1$ so $z \sim x_1$ and $z \in [x_1]$. Therefore $[x_1] = [x_2]$.

For each equivalence class $\mathcal{T} \in X/\sim$, pick an element $x \in \mathcal{T}$ and define the subset $Y_x \subset X$ by $Y_x = [x]$. Then by the discussion in the previous paragraph, $\bigcup Y_x = X$ and $Y_x \cap Y_y = \emptyset$ if $x \neq y$. Therefore the set of equivalence classes partitions the set X.

Conversely, suppose $\{Y_i\}$ is a partition of X. Then define a relation on X by $x \sim y$ if and only if $x \in Y_i$ and $y \in Y_i$ for the same subset Y_i. Alternatively, the relation is defined by $x \sim y$ if they both belong to the same subset Y_i. Since if $x \in Y_i$, then $x \in Y_i$, we have $x \sim x$. If x and y are both in Y_i for some i, then y and x both belong to the same subset, so $x \sim y$ implies $y \sim x$. Finally, if $x \sim y$ and $y \sim z$ we must have that $x, y \in Y_i$ and $y, z \in Y_j$ for some i, j. Then $y \in Y_i \cap Y_j$, and

since $\{Y_i\}$ is a partition, $Y_i = Y_j$. Therefore $x, z \in Y_i$ and $x \sim z$. This shows $\sim$ is an equivalence relation.

It remains to show the subsets Y_i are exactly the equivalence classes of $\sim$. Let $x \in X$, then $x \in Y_i$ for some i. Then $[x] = \{y \in X : y \sim x\} = \{y \in X : y \in Y_i\} = Y_i$, completing the proof. ■

The important take-home message from this proposition is that we can think of equivalence relations and partitions as two sides of the same coin. This theme occurs lots of times in this course, and it's always useful to have multiple ways of thinking about the same thing.

C Some Set Theory

The goal of this appendix is to go over some facts about functions between sets, and what we can say about sizes of sets by looking at functions between sets. It is often the case that what is coming up is taken for granted. For example, at various points in the notes above we prove that a function is a bijection by finding an inverse. In this appendix we will show that these kinds of techniques actually work!

C.1 Injections, Surjections, and Bijections

Intuitively we know the definitions of an injection, surjection and bijection. An injection from S to T is a function that doesn't send any two elements of S to the same element of T. A surjection from S to T is a function that sends something to everything in T, or a function that hits everything in T. A bijection is a perfect matching, kind of like a dictionary, between elements of S and elements of T. That is, every element of S has an element of T associated to it, and vice versa. This is the same as saying that f is both surjective and injective. Let's make these intuitions formal.

Definition. Let $f : S \to T$ be a function.

- We say f is **injective** (or f is an **injection**) if whenever $f(s_1) = f(s_2)$, we have $s_1 = s_2$.
- We say f is **surjective** (or f is a **surjection**) if for all $t \in T$, there exists an $s \in S$ such that $f(s) = t$.
- We say f is **bijective** (or f is a **bijection**) if f is both injective and surjective.

This definition is all well and good, but there is another way to think about injections, surjections, and bijections. The idea is as follows.

If $f : S \to T$ is an injection, then every element in T that gets hit has a unique preimage (a unique element $s \in S$ such that $f(s) = t$) so we can define a $g : T \to S$ such that if we do f first and then g, we can return every element in S to itself.

If $f : S \to T$ is a surjection, then every $t \in T$ has at least one preimage, so we can define $g : T \to S$ to be a function that sends t to one of its preimages. Since every t has a preimage, this function has the property that if we do g first and then f, every element of t ends up back where it started.

If $f : S \to T$ is a bijection, then we can do what we did for the injections and surjections in a unique way to get a $g : T \to S$ such that $fg(t) = t$ for all $t \in T$ and $gf(s) = s$ for all $s \in S$.

These ideas are formalised in the following proposition. Here is a bit of notation we will use for the proposition and throughout the notes above. Let S be a set and define the identity function $\mathrm{id}_S : S \to S$ by $\mathrm{id}_S(s) = s$ for all $s \in S$.

Proposition 76. *Let $f : S \to T$ be a function between sets.*

- *f is an injection if and only if there exists a function $g : T \to S$ such that $gf = id_S$.*
- *f is a surjection if and only if there exists a function $g : T \to S$ such that $fg = id_T$.*
- *f is a bijection if and only if there exists a function $g : T \to S$ such that $fg = id_T$ and $gf = id_S$. Furthermore, such a g is unique and we denote it $g = f^{-1}$.*

Proof. Suppose f is an injection. Pick an $x \in S$ and for every $t \in f(S)$, let $s_t \in S$ be the unique element of S such that $f(s_t) = t$. Recall $f(S) := \{t \in T : \text{there exists } s \in S \text{ such that } f(s) = t\}$. Define $g : T \to S$ by

$$g(t) = \begin{cases} s_t & \text{if } t \in f(S) \\ x & \text{otherwise.} \end{cases}$$

Since every $s \in S$ is of the form s_t for some $t \in T$, we see $gf(s_t) = g(t) = s_t$ for all $s_t \in S$ so $gf = \mathrm{id}_S$.

Conversely suppose $f(a) = f(b) = t_0$ where $a \neq b$ in S. Suppose $g : T \to S$ is such that $gf = \mathrm{id}_S$. If $g(t_0) \neq a$, then $gf(a) \neq a$, so we must have $g(t_0) = a$. Then we have $gf(b) = a \neq b$, so such a g cannot exist.

Suppose f is a surjection. Define $g : T \to S$ by $g(t) = s_t$ where $f(s_t) = t$. Note that since f is surjective, we can always do this. Then $fg(t) = f(s_t) = t$ for all $t \in T$, so $fg = \mathrm{id}_T$.

Conversely, if f is anot a surjection there is some $t_0 \in T$ such that there is no $s \in S$ such that $f(s) = t_0$. Let $g : T \to S$ be a candidate function such that $fg = \mathrm{id}_T$. Then $fg(t_0) \neq t_0$ since there is no element in S such that $f(s) = t_0$. Therefore there is no function $g : T \to S$ such that $fg = \mathrm{id}_T$.

Finally, if f is a bijection, then define $g : T \to S$ to be $g(t) = s_t$ where $s_t \in S$ is the unique element such that $f(s_t) = t$. Note that every element in S is of the form s_t for some t. Then

$$gf(s_t) = g(t) = s_t \quad \text{and} \quad fg(t) = f(s_t) = t$$

for all $s_t \in S$ and $t \in T$, so $gf = \mathrm{id}_S$ and $fg = \mathrm{id}_T$. Conversely, if f is not injective or surjective, the same arguments above show that there cannot exist a $g : T \to S$ such that $fg = \mathrm{id}_S$ or $gf = \mathrm{id}_T$ respectively.

It remains to show that in the case when f is a bijection, the inverse g is unique. Suppose there is another map $h : T \to S$ such that $fh = \mathrm{id}_S$. Then $f(h(t)) = t = f(g(t))$ fur all $t \in T$. Since f is sinjective, we must have $h(t) = g(t)$ for all $t \in T$, completing the proof. ∎

As is discussed several times in the notes above, whenever you have a sutuation like this, you can use either property as the definition in your head. For example, we can now think of an injection has a map with a left inverse, or as a map which sends different elements to different elements. Whichever definition is easier or more helpful in a particular situation should be the one you use.

It is worth noting here that the above proof relies on the axiom of choice, but that is a discussion for another time and course.

In Lemma 25 we proved that multiplication by a unit induced a bijection on $\mathbb{Z}_n^*$. Let's prove it again here (this time for all of $\mathbb{Z}_n$, not just $\mathbb{Z}_n^*$), this time making use of Proposition 76

Lemma 77. *Let $[a] \in \mathbb{Z}_n^*$. The function $\psi : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $\psi([b]) = [a][b]$ is a bijection.*

Proof. Consider the function $\theta : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $\theta([b]) = [a]^{-1}[b]$. Then $\theta\psi([b]) = \theta([a][b]) = [a]^{-1}[a][b] = [b]$ and $\psi\theta([b]) = \psi([a]^{-1}[b]) = [a][a]^{-1}[b] = [b]$. Therefore $\psi\theta = \mathrm{id}_{\mathbb{Z}_n}$ and $\theta\psi = \mathrm{id}_{\mathbb{Z}_n}$ so ψ is a bijection. ∎

C.2 Comparing the Sizes of Sets

There are lots of times you might want to show that two sets have the same size, or that one is bigger than the other. Here is a formal way to compare the size of two sets. Here, let $|S|$ be the size of a set.

Definition. Let S and T be sets.

- If there exists an injection $f : S \to T$, then $|S| \leq |T|$.
- If there exists a surjection $f : S \to T$, then $|S| \geq |T|$.
- If there exists a bijection $f : S \to T$, then $|S| = |T|$.

Recall that we used this definition in the proof of Lemma 32.

If $|S|$ and $|T|$ are finite, it is easy to see that this agrees with our intuition about what it means for a set to be bigger (or smaller) than another set. The advantage of this definition really becomes apparent when comparing infinite sets, because it gives us a formal way to say whether or not an infinite set is bigger or smaller than another infinite set.

When infinite sets get involved though, there are a few things that we need to check to make sure our notation using $\leq$ and $\geq$ actually makes sense. It turns out that these definitions work because of the following facts, which are far from obvious. They will be stated in terms of the existence of functions, and then in terms of what that means with regards to the relation $\leq$ defined above.

Fact 78. *Let S and T be sets.*

1. *There exists a surjection from S to T or from T to S (or both). Equivalently, $|S| \geq |T|$ or $|T| \geq |S|$ (or both).*
2. *There exists an injection $f : S \to T$ if and only if there exists a surjection $g : T \to S$. Equivalently $|S| \leq |T|$ if and only if $|T| \geq |S|$.*
3. *If there exists an injection $f_1 : S \to T$ and a surjection $f_2 : S \to T$, then there exists a bijection $f : S \to T$. Equivalently, if $|S| \geq |T|$ and $|S| \leq |T|$, then $|S| = |T|$.*

Facts 1 and 2 both rely on the axiom of choice, and Fact 3 is called the Schröder-Bernstein theorem.

With these definitions we can formally prove that $|\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$. However, we have $|\mathbb{Z}| \lneq |\mathbb{R}|$, and we can prove that although there is an injection from $\mathbb{Z}$ to $\mathbb{R}$ (which is the regular inclusion map), we cannot find a bijection. If you're curious about this, look up Cantor's diagonalisation argument. It's one of the neatest lines of reasoning you'll see!

D Groups, rings, and fields

In this course, we have come across groups, rings, and fields, without formally talking about them. Let's do that to add a little algebraic context to our number theory.

D.1 Groups

The word group has popped up a bunch of times in the course, most notably in calling $\mathbb{Z}_n^*$ the group of units. What makes $\mathbb{Z}_n^*$ a group is that it comes with an operation (multiplication) that eats two elements of $\mathbb{Z}_n^*$ and spits out another element of $\mathbb{Z}_n^*$. More than that, there is a special element $[1]$ (the identity with respect to the operation) with the property that $[1][a] = [a]$, and every element in $\mathbb{Z}_n^*$ has an inverse (with respect to the operation). Let's abstract these properties out into the definition of a group, which applies to many more structures in mathematics besides just $\mathbb{Z}_n^*$.

Definition. A **group** is a set G together with an operation $* : G \times G \to G$ such that the following properties are satisfied.

- For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
- There exists an element e, such that for all $a \in G$, $e * a = a * e = a$ for all $a \in G$. We call e the **identity**.
- For every $a \in G$, there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$. We call a^{-1} the **inverse** of a.

If we wish to emphases the operation, we will denote the group G by $(G, *)$.

Exercise. Consider $(\mathbb{Q} \setminus \{0\}, \div)$ where $\mathbb{Q} \setminus \{0\}$ is the set of non-zero rational numbers, and the operation $\div$ is just division, that is $a \div b = \frac{a}{b}$. Show that $(\mathbb{Q} \setminus \{0\}, \div)$ is not a group.

We have already come across a whole bunch of groups, as shown in the next exercise.

Exercise. Show that the following are groups, and verify the identity is indeed the identity.

- $(\mathbb{Z}_n^*, \cdot)$ (where $\cdot$ is multiplication in $\mathbb{Z}_n$), with identity $[1]$.
- $(Q_n, \cdot)$ (where Q_n is the set of quadratic residues in $\mathbb{Z}_n^*$, and $\cdot$ is multiplication in $\mathbb{Z}_n$) with identity $[1]$.
- $(\mathbb{Z}_n, +)$ with identity $[0]$.
- $(\mathbb{Z}, +)$ with identity 0.
- $(\mathbb{R}_{>0}, \cdot)$ (where $\mathbb{R}_{>0}$ is the set of positive real numbers, and $\cdot$ is multiplication) with identity 1.
- $(\mathrm{SL}_2(\mathbb{R}), \cdot)$ (where $\mathrm{SL}_2(\mathbb{R})$ is the set of 2×2 matrices with real entries and determinant 1, and $\cdot$ is matrix multiplication) with identity $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$.

The first four groups in the exercise all have the property that $a * b = b * a$ for all a, b in the group, but the last one does not (for example $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \neq \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$). All the groups we encounter in this course have this nice property, and they are given a special name.

Definition. Let $(G, *)$ be a group. If $a * b = b * a$ for all $a, b \in G$, then we say G is an **abelian group**.

So, $\mathbb{Z}_n^*$ (with multiplication) and $\mathbb{Z}_n$ (with addition) are abelian groups since $[a][b] = [b][a]$ and $[a] + [b] = [b] + [a]$ for all $[a], [b] \in \mathbb{Z}_n$. From here on in, if we write the group $\mathbb{Z}_n^*$, it is understood that the group operation is multiplication, since it's the only reasonable operation that turns $\mathbb{Z}_n^*$ into a group! Similarly for $\mathbb{Z}_n$ and addition. To reinforce this, we have the following exercise.

Exercise. Show that $\mathbb{Z}_n$ with multiplication is not a group. Show that $\mathbb{Z}_n^*$ with addition is not a group.

more to come...