Math 124 - Number Theory

Taught by Cliff Taubes
Notes by Dongryul Kim

Fall 2018

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

Contents

1 September 5, 2018

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

1.1 Overview

We are going to denote

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

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

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

$$7x + 10y$$

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

$$6x + 10y.$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Number theory is also used in codes and cyphers.

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

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

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

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

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

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

1.2 Addition and multiplication of integers

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

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

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

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

Then there is a rule about distribution:

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

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

There are also cancellation laws:

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

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

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

1.3 Divisibility and primes

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

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

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

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

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

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

$$xb + yc = xma + yna = (xm + yn)a.$$ □

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

- primes,
- composites,
- 1.

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

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

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

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

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

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

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

This has a nice consequence.

Proposition 1.7. *There are infinitely many primes.*

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

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

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

2 September 10, 2018

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

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

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

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

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

2.1 Davenport's proof of the fundamental theorem of arithmetic

Suppose we have

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

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

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

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

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

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

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

Let us now consider

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

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

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

Now

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

and we can cancel both sides and get

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

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

2.2 Greatest common divisor

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

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

So for instance,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

They are both equal to 2.

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

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

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

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

Then

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

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

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

Example 2.8. We have

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

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

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

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

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

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

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

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

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

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

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

Proof. Consider the Euclidean algorithm

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

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

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

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

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

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

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

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

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

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

2.3 Linear combinations

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

$$ax + by = m$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

We now need to prove this linear algebra proposition.

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

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

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

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

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

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

We will finish this next time. □

3 September 12, 2018

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

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

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

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

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

We were looking at the linear combinations of two integers,

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

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

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

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

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

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

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

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

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

Then we go on with all primes,

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

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

Let us now prove what we wanted to prove.

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

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

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

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

has a solution.

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

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

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

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

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

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

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

3.1 Finding primes

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

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

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

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

2. Let p be the smallest element remaining in X. If $p > \sqrt{n}$, add all of X to P and terminate the program. If $p \leq \sqrt{n}$, add p to P.

3. From X, remove all elements divisible by p.

4. Go to Step 2.

When we pick p in Step 2, it has to be a prime, because in Step 3 we always throw away all the things divisible by smaller primes. So p in Step 2 cannot be

divisible by any smaller prime, which means that it is a prime. But why do we terminate the program when $p > \sqrt{n}$? The reason is this. Let the set X be

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

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

There is another famous theorem of Dirichlet.

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

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

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

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

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

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

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

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

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

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

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

then the theorem states the following asymptotic behavior.

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

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

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

3.2 Groups and rings

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

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

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

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

such that

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

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

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

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

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

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

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

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

such that

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

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

But there are no multiplicative inverses.

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

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

and

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

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

Index