1. Greatest common divisor

In the previous lecture we should that any subgroup of \((\mathbb{Z}, +)\) is of the form \(d\mathbb{Z}\) for some non-negative integer \(d\). We see how this can help us to get a better understanding of the greatest common divisor of two integers and reprove a result that you have seen in math109.

The main result of this section is the following theorem.

**Theorem 1.** Suppose \(a\) and \(b\) are two non-zero integers. Then

\[
a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z};
\]

alternatively we can say that for an integer \(c\) the equation

\[
ax + by = c
\]

has an integer solution if and only if \(\gcd(a, b)|c\).

We prove Theorem 1 in several steps.

**Lemma 2.** For integers \(a\) and \(b\),

\[
 a\mathbb{Z} + b\mathbb{Z} := \{ak + bl | k, l \in \mathbb{Z}\}
\]

is a subgroup of \((\mathbb{Z}, +)\).

**Proof.** Since + is associative, to show \(a\mathbb{Z} + b\mathbb{Z}\) is a subgroup it is enough to prove the following:

1. \(0 \in a\mathbb{Z} + b\mathbb{Z},\)
2. If \(c_1, c_2 \in a\mathbb{Z} + b\mathbb{Z},\) then \(c_1 + c_2 \in a\mathbb{Z} + b\mathbb{Z}.\)
3. If \(c \in a\mathbb{Z} + b\mathbb{Z},\) then \(-c \in a\mathbb{Z} + b\mathbb{Z}.\)

Notice that \(0 = (a)(0) + (b)(0) \in a\mathbb{Z} + b\mathbb{Z}.\)
If $c_1, c_2 \in a\mathbb{Z} + b\mathbb{Z}$, then $c_1 = ak_1 + bl_1$ and $c_2 = ak_2 + bl_2$ for some integers $k_1, k_2, l_1, l_2$. Hence

$$c_1 + c_2 = (ak_1 + bl_1) + (ak_2 + bl_2) = a(k_1 + k_2) + b(l_1 + l_2).$$

Since $k_1 + k_2$ and $l_1 + l_2$ are integers, we deduce that $c_1 + c_2 \in a\mathbb{Z} + b\mathbb{Z}$.

If $c \in a\mathbb{Z} + b\mathbb{Z}$, $c = ak + bl$ for some integers $k, l$. Hence

$$-c = (a)(-k) + (b)(-l),$$

which implies that $-c \in a\mathbb{Z} + b\mathbb{Z}$; and claim follows. $\square$

**Corollary 3.** For two non-zero integers $a$ and $b$, there is a positive integer $d$ such that

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$  

**Proof.** By Lemma 2, $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Hence by a result that we proved in the previous lecture there is an integer $d$ such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Since $a = (a)(1) + (b)(0) \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ and $a \neq 0$, we deduce that $d \neq 0$.

We also notice that $d\mathbb{Z} = (-d)\mathbb{Z}$. Since $d$ is not zero, either $d$ or $-d$ is positive; and claim follows. $\square$

**Proof of Theorem 1.** By Corollary 3, there is a positive integer $d$ such that

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$  

We will prove that $d = \gcd(a, b)$. We do this by proving that $d \leq \gcd(a, b)$ and $\gcd(a, b) \leq d$. **Step 1.** $d \leq \gcd(a, b)$.

**Proof of Step 1.** Notice that

$$a = (a)(1) + (b)(0) \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z},$$

which means

(1) $d | a$.

Similarly

$$b = (a)(0) + (b)(1) \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z},$$

which means

(2) $d | b$.

By (1) and (2), we have that $d$ is a common divisor of $a$ and $b$. Thus $d$ is at most the greatest common divisor of $a$ and $b$; that means $d \leq \gcd(a, b)$. 


Step 2. \( \gcd(a, b) \leq d \).

Proof of Step 2. Notice that \( d = (d)(1) \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \); and so

\[
d = ar + bs \text{ for some integers } r, s.
\]

(3)

Let \( d' := \gcd(a, b) \). Hence \( d'|a \) and \( d'|b \), which imply that \( d'|ar \) and \( d'|bs \). Therefore

\[
d' \mid ar + bs = d.
\]

(4)

Since \( d' \) and \( d \) are positive, by (4) we deduce that

\[
d' \leq d,
\]

which means \( \gcd(a, b) \leq d \); and claim follows.

By Steps 1 and 2, we get

\[
a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}.
\]

This means an integer combination of \( a \) and \( b \) is a multiple of \( \gcd(a, b) \) and vice versa an integer multiple of the \( \gcd(a, b) \) is an integer combination of \( a \) and \( b \). Alternatively we can say the equation

\[
ax + by = c
\]

has an integer solution for \( x \) and \( y \) if and only if \( \gcd(a, b) \mid c \). \( \square \)

2. Relatively prime and Euclid’s lemma

We say two integers \( a \) and \( b \) are relatively prime if \( \gcd(a, b) = 1 \). An immediate corollary of Theorem 1 is the following.

**Theorem 4.** Suppose \( a \) and \( b \) are two non-zero integers. Then \( a \) and \( b \) are relatively prime if and only if \( ar + bs = 1 \) for some integers \( r \) and \( s \).

**Proof.** \( \Rightarrow \) If \( a \) and \( b \) are relatively prime, then \( \gcd(a, b) = 1 \). Hence by Theorem 1 the equation \( ax + by = 1 \) has an integer solution as \( \gcd(a, b) = 1 \) divides 1. This means for some integers \( r \) and \( s \) we have \( ar + bs = 1 \).

\( \Leftarrow \) Suppose \( ar + bs = 1 \) for some integers \( r \) and \( s \); then by Theorem 1 we have

\[
1 = ar + bs \in a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}.
\]

Hence 1 is a multiple of \( \gcd(a, b) \), which implies that \( \gcd(a, b) = 1 \), and claim follows. \( \square \)
The following is an important corollary of Theorem 4. It is called Euclid’s lemma.

**Lemma 5** (Euclid’s lemma). Suppose $a, b, c$ are non-zero integers, and $a$ and $b$ are relatively prime. Then $a | bc$ implies $a | c$.

In mathematical language

$$(\gcd(a, b) = 1 \& a | bc) \implies a | c.$$  

**Proof.** Since $\gcd(a, b) = 1$, by Theorem 4, for some integers $r$ and $s$ we have

$$ar + bs = 1. \tag{5}$$

Multiplying both sides of (5) by $c$ we get

$$acr + bcs = c. \tag{6}$$

Notice that $a | (a)(cr)$ and $a | (bc)(s)$; and so by (6)

$$a | acr + bcs,$$

which implies $a | c$; and claim follows. □

3. **Prime numbers**

3.1. **Definition and Euler’s lemma for primes.** Let us recall that we say an integer $p \geq 2$ is prime if it has exactly two positive divisors 1 and $p$.

**Lemma 6.** Suppose $p$ is prime. Then for any positive integer $n$ we have that either $p | n$ or $\gcd(p, n) = 1$.

**Proof.** Since $\gcd(p, n)$ is a positive divisor of $p$, it is either $p$ or 1. If $\gcd(p, n) = p$, then $p | n$. Otherwise, $\gcd(p, n) = 1$. □

The following is an important corollary of Euclid’s lemma (Lemma 5) for primes.

**Proposition 7.** Suppose $p$ is prime, and $a, b \in \mathbb{Z} \setminus \{0\}$. If $p | ab$, then either $p | a$ or $p | b$.

**Proof.** It is enough to show that

$$(p | ab \text{ and } p \nmid a) \implies p | b.$$
By Lemma 6, \( p \nmid a \) implies that \( \gcd(p, n) = 1 \). Hence by Euclid’s lemma we get
\[
(p|ab \text{ and } p \nmid a) \implies (p|ab \text{ and } \gcd(p, a) = 1) \implies p|b;
\]
and claim follows.

By induction on \( n \) we can show the following.

**Proposition 8.** Suppose \( p \) is prime and \( a_1, \ldots, a_n \) are non-zero integers. Then
\[
p|a_1 \cdots a_n \implies p|a_i \text{ for some } i.
\]

**Proof.** We proceed by induction on \( n \). By Proposition 7 we get the base of induction. So now we focus on the induction step. Suppose \( p|a_1 \cdot a_2 \cdot \cdots \cdot a_{n+1} \); so \( p \) divides the product of \( n \) non-zero integers
\[
a_1, a_2, \ldots, a_{n-1}, \text{ and } (a_n a_{n+1}).
\]
Hence by the induction hypothesis either for some \( i \leq n - 1 \), we have \( p|a_i \), or \( p|(a_n a_{n+1}) \). In the former case we are done. In the latter case by Proposition 7 we have that \( p|a_n \text{ or } p|a_{n+1} \); and claim follows.

---

### 3.2. Sieve of Eratosthenes

The sequence of prime numbers is a fascinating sequence. They are at one hand very structured and at the same time behave like random numbers (We will see more about this in the next lecture). Because of this there is no direct way of finding the \( n \)-th prime number. Our fastest way of finding all the numbers less than \( x \) is using sieve of Eratosthenes. This method works because of the following observation:

**Lemma 9.** Suppose \( n \in \mathbb{Z}^+ \) is a composite number. Then \( n \) has a divisor \( d \) which is more than 1 and is at most \( \sqrt{n} \).

**Proof.** Since \( n \) is composite, there are positive numbers \( a \) and \( b \) such that \( n = ab \) and \( 1 < a, b < n \). Without loss of generality less let us assume that \( a \leq b \). Then \( a^2 \leq ab \leq n \). Hence \( 1 < a \leq \sqrt{n} \); and claim follows.
than 100, we need to cross our all the multiples of numbers less than $\sqrt{100}$, which means multiples of 2, 3, 5, and 7. So the set of primes less than 100 is

$$\{2, 3, 5, 7\} \cup \{n \in \mathbb{Z}^+ | 2 \leq p \leq 100, 2 \nmid n, 3 \nmid n, 5 \nmid n, 7 \nmid n\}.$$ 

4. FUNDAMENTAL THEOREM OF ARITHMETIC.

Primes are the atoms of integers in the multiplicative sense:

**Theorem 10.** Any integer more than 1 can be written as a product of primes in a unique way.

\[\text{\footnotesize \cite{1}}\text{I have used a code that is provided in https://tex.stackexchange.com/questions/44673/sieve-of-eratosthenes-in-tikz}\]
Proof. **The existence part.** Suppose to the contrary that there is a positive integer that cannot be written as a product of primes. Then
\[ \{ n \in \mathbb{Z}^{\geq 2} | n \text{ cannot be written as a product of primes} \} \]
is a non-empty set. Hence by the well-ordering principle, there is a minimum integer \( n \) (more than 1) that cannot be written as a product of prime. Since \( n \) cannot be written as a product of prime, \( n \) is not prime. Therefore \( n = ab \) for some integers \( 1 < a, b < n \). Since \( n \) is the minimum integer more than 1 that cannot be written as a product of primes and \( 1 < a, b < n \), we deduce that \( a \) and \( b \) can be written as products of primes. So there are primes \( p_1, \ldots, p_n \) and \( q_1, \ldots, q_m \) such that
\[
a = p_1 \cdots p_n \quad \text{and} \quad b = q_1 \cdots q_m.\]
Hence \( n = ab = p_1 \cdots p_n \cdot q_1 \cdots q_m \); this implies that \( n \) can be written as a product of primes as well, which is a contradiction.

**The uniqueness part.** We proceed by contradiction again. Suppose to the contrary that
\[ \{ n \in \mathbb{Z}^{\geq 2} | n \text{ can be written as a product of primes at least in 2 ways} \} \]
is not empty. Hence by the well-ordering principle, there is a minimum integer \( n_0 \) in this set; that means
\[
(1) \quad n_0 = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r} \quad \text{for some distinct primes} \ p_i \text{'s and non-negative integers} \ k_i, l_i \text{ such that at least for one index} \ i_0 \text{ we have} \ k_{i_0} \neq l_{i_0}.\]

(2) Any integer \( 2 \leq m < n_0 \) can be written as a product of primes in a unique way.

Since \( k_{i_0} \neq l_{i_0} \) and these are non-negative integers, at least one of them is not zero. Without loss of generality we can and will assume that \( k_{i_0} \neq 0 \); that means \( p_{i_0} | n_0 \). Therefore \( p_{i_0} | p_1^{l_1} \cdots p_r^{l_r} \). By Proposition 7, \( p_{i_0} \) should divide \( p_j^{l_j} \) for some \( j \). If \( p_{i_0} | p_j \), then again by Proposition 7 \( p_{i_0} | p_j \). Since \( p_j \) is prime, we deduce that \( p_{i_0} = p_j \); and so \( i_0 = j \). Hence \( l_{i_0} \) is positive. Hence we have
\[ k_{i_0} > 0 \text{ and } l_{i_0}, \]
which means we can cancel out one \( p_{i_0} \) from both sides and get
\[ m_0 := p_1^{k_1} \cdots p_{i_0}^{k_{i_0} - 1} \cdots p_r^{k_r} = p_1^{l_1} \cdots p_{i_0}^{l_{i_0} - 1} \cdots p_r^{l_r}. \]
Since $m_0$ is strictly smaller that $n_0$, by the item (2) of the mentioned properties of $n_0$ we have that $m_0$ can be written as a product of primes in a unique way. Thus by (7) we have that

$$k_{i_0} - 1 = l_{i_0} - 1,$$

which implies $k_{i_0} = l_{i_0}$; and this is a contradiction.