

Introduction to Topology

Elementary Number Theory, Lecture 3,4

Haoming Wang

23 June 2019

THIS IS THE LECTURE NOTE FOR THE *Introduction to Topology*. The course covers the following topics: Naive Set Theory, Elementary Number Theory, Group Theory, Topological Spaces and Continuous Maps, Introduction to Algebraic Topology.

Fundamental Theorem of Arithmetic

Proposition 1 (Division). $\forall a \in \mathbb{Z}, b \in \mathbb{N}, \exists! q \in \mathbb{Z}, r \in \mathbb{N}_0$, s.t. $a = bq + r \wedge 0 \leq r < b$.

You can divide the number axis as a family of intervals with open left and closed right $[kb, (k+1)b)$, just like right figure.

So any integer a would fall into a specific interval of the axis, denote as $[qb, qb + b)$, and it can only be represented as $a = qb + r$ with $0 \leq r < b$, which implies the existence and uniqueness of the q and r .

Exercise 1. Show that if $a \in \mathbb{Z}, b \in \mathbb{N}$, then $b|a \Leftrightarrow \exists q \in \mathbb{Z}, r \in \mathbb{N}_0$ s.t. $a = bq + r \wedge r = 0$.

Proof. \Rightarrow : Trivial, \Leftarrow : if $b|a$ then $\exists \mu \in \mathbb{Z}$, s.t. $a = \mu b = \mu b + 0$. Since the existence and uniqueness of q, r , we have that $q = \mu, r = 0$. \square

Proposition 2 (Greatest common factor). Assume that $a, b \in \mathbb{Z}$ and one of a, b is not 0, $\exists x_0, y_0 \in \mathbb{Z}, n = ax_0 + by_0$, such that

1. $\forall x, y \in \mathbb{Z}, n|ax + by$;
2. $\forall m \in \mathbb{N}, m|a \wedge m|b \Rightarrow m|n$.

That is n is the greatest common factor of a, b .

Proof. Define a set $S := \{ax + by | x, y \in \mathbb{Z}, ax + by > 0\}$, and $\min S =: n = ax_0 + by_0$, thus $n \in \mathbb{N}$. For any $x, y \in \mathbb{Z}, \exists! q \in \mathbb{Z}, 0 \leq r < n$, s.t. $ax + by = qn + r$.

$$ax + by = qn + r = q(ax_0 + by_0) + r$$

thus $r = a(x - qx_0) + b(y - qy_0) \in S$. If $r \neq 0$ ($r > 0$), then $r \geq n$, which leads to a contradiction, thus $r = 0$ and $n|ax + by$ for any $x, y \in \mathbb{Z}$.

On the other hand, if $m \in \mathbb{N}, m|a \wedge m|b$, then $\exists \mu, \nu \in \mathbb{Z}$, such that $a = \mu m, b = \nu m$, and $n = ax_0 + by_0 = \mu ax_0 + \nu mby_0 = (\mu ax_0 + \nu by_0)m$, thus $m|n$.

CONTENT:

1. Fundamental Theorem of Arithmetic
2. Integer equation
3. Congruence

Note 1. Dividend a , quotient $q \in \mathbb{Z}$, divisor $b \in \mathbb{N}$, factor $r \in \mathbb{N}_0$.

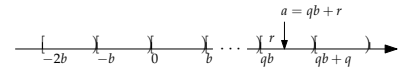


Figure 1: $a = qb + r$.

Note 2. For $b, a \in \mathbb{Z}, b|a$ means $\exists m \in \mathbb{Z}$, s.t. $a = bm$. Notice that we do not restrict b in \mathbb{N} . Thus $\cdot | \cdot$ is a distinct concept with Division whose $r = 0$. For example, we could say $-2 | -4$, but -2 can not be a divisor.

Thus n is the greatest common factor of a, b , denoted as $n = (a, b)$. \square

Proposition 3. Given $\forall a, b, c \in \mathbb{Z}$, $(a, b) = 1 \wedge a|bc \Rightarrow a|c$.

Proof. As we know, $\exists \mu, \nu \in \mathbb{Z}$, s.t. $n = \mu a + \nu b = (a, b) = 1$, then

$$\mu ac + \nu bc = c \Rightarrow \mu + \nu \frac{bc}{a} = \frac{c}{a},$$

since $\mu + \nu \frac{bc}{a} =: m \in \mathbb{Z}$, $c = ma$, thus $a|c$. \square

Theorem 1 (Fundamental Theorem of Arithmetic). Every positive integer $n > 1$ can be represented in exactly one way as a product of prime powers:

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^k p_i^{n_i}$$

where $p_1 < p_2 < \cdots < p_k$ are primes and the n_i are positive integers.

Proof. The existence is trivial, we will show the uniqueness. Suppose there exists another distinct primes series q_1, \cdots, q_l with m_1, \cdots, m_l are positive integers, such that

$$\prod_{i=1}^k p_i^{n_i} = \prod_{j=1}^l q_j^{m_j},$$

suppose that $q_s (s \in \{1, 2, \cdots, l\}) \notin \{p_1, \cdots, p_k\}$; denote $\frac{1}{q_s} \prod_{i=1}^l q_j^{m_j}$ as w , then $w \in \mathbb{Z}$, and $\prod_{i=1}^k p_i^{n_i} = q_s w$, thus $q_s | \prod_{i=1}^k p_i^{n_i}$. Since

$$(q_s, \underbrace{p_1, \cdots, p_1}_{n_1}, \cdots, \underbrace{p_k, \cdots, p_k}_{n_k}) = (q_s, p_1, \cdots, p_k) = 1$$

we have that $q_s | \prod_{i=1}^k p_i^{n_i} \frac{1}{p_1}$. Repeat this process leads to $q_s | p_k$, which is a contradiction. So $q_s \notin$, and $p_1, \cdots, p_k, n_1, \cdots, n_k$ are unique. \square

Integer equation

Exercise 2. Given $a, b, c \in \mathbb{Z}$ show that $(a, b)|c \Leftrightarrow$ equation $ax + by = c$ has integer solution.

Proof. \Rightarrow : $(a, b)|c$, thus $\exists x_0, y_0, m \in \mathbb{Z}$ such that $m(a, b) = m(x_0 a + y_0 b) = c$, thus $x = mx_0, y = my_0$. \Leftarrow : $\exists m, n \in \mathbb{Z}$, such that $a = m(a, b), b = n(a, b)$, thus $c = ax + by = xm(a, b) + yn(a, b) = (a, b)(xm + yn)$, thus $(a, b)|c$. \square

Note 3. Generally, we can prove that $n = \min\{\sum_{i=1}^N a_i x_i \mid x_i \in \mathbb{Z}, \sum_{i=1}^N a_i x_i > 0\}$ is the greatest common factor of any integer a_1, \cdots, a_N .

Note 4. If we prime factorize two numbers a, b , the greatest common factor of the two numbers, denote as (a, b) , is the production of the intersection of their prime factors. The least common multiple, denote as $[a, b]$, is the production of the union.

Thus for $a, b, c \in \mathbb{Z}$, we have that $([a, b], c) = [(a, c), (b, c)]$, and $[(a, b), c] = ([a, c], [b, c])$.

Note 5. Generally, for integers $a_i (i = 0, \cdots, N)$, $\sum_{i=1}^N a_i x_i = a_0$ has integer solution $\Leftrightarrow (a_1, \cdots, a_N) | a_0$.

Now we want to explore how to find all possible $x, y \in \mathbb{Z}$ such that $ax + by = c$? Assume that $a, b, c, x_0, y_0 \in \mathbb{Z}$ and $ax_0 + by_0 = c$. If $x, y \in \mathbb{Z}$, s.t. $ax + by = c \Leftrightarrow a(x_0 - x) = b(y - y_0) \Leftrightarrow \frac{a}{(a,b)}(x_0 - x) = \frac{b}{(a,b)}(y - y_0)$, thus $\frac{a}{(a,b)} \mid \frac{b}{(a,b)}(y - y_0)$. Since $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$, we have that $\frac{a}{(a,b)} \mid (y - y_0)$, that is $\exists t \in \mathbb{Z}$, s.t. $(y - y_0) = t \frac{a}{(a,b)}$ and $(x_0 - x) = t \frac{b}{(a,b)}$. Thus the sufficient and necessary condition of $x, y \in \mathbb{Z}$ is the solution of $ax + by = c$ is

$$y = y_0 + t \frac{a}{(a,b)}, \quad x = x_0 - t \frac{b}{(a,b)}$$

for $\forall t \in \mathbb{Z}$.

Congruence

Definition 1 (Congruence). For $a, b, m \in \mathbb{Z}$, we say that $a \equiv b \pmod{m}$ if $m \mid (a - b)$.

Exercise 3. When $m \in \mathbb{N}$, show that $a \equiv b \pmod{m} \Leftrightarrow r_{a,m} = r_{b,m}$. ($r_{a,m}$ is the factor of a is divided by m)

Proof. \Leftarrow : Trivial. \Rightarrow : $a \equiv b \pmod{m}$ then $\exists \mu \in \mathbb{Z}$ such that $m\mu = (a - b)$. Since $m \in \mathbb{N}$, thus $\exists q_{a,m}, q_{b,m} \in \mathbb{Z}$ and $r_{a,m}, r_{b,m} \in \mathbb{N}_0$ where $0 \leq r_{a,m}, r_{b,m} < m$, such that $a = q_{a,m} \cdot m + r_{a,m}$, $b = q_{b,m} \cdot m + r_{b,m}$ and $(a - b) = m(q_{a,m} - q_{b,m}) + (r_{a,m} - r_{b,m})$. Since the conclusion of Exercise 1, we have $q_{a,m} - q_{b,m} = \mu$ and $r_{a,m} - r_{b,m} = 0$. \square

Thus the intuition of mod is just like the right figure. It is easily to check that congruence is an equivalence relation on \mathbb{Z} .

Exercise 4. Show that $a \equiv b \pmod{m}, a' \equiv b' \pmod{m} \Rightarrow a \pm a' \equiv b \pm b' \pmod{m}$ and $aa' \equiv bb' \pmod{m}$.

Proof. $\exists \mu, v \in \mathbb{Z}$, s.t. $a - b = \mu m$ and $a' - b' = v m$, thus $(\mu \pm v)m = (a \pm a') - (b \pm b')$, thus $a \pm a' \equiv b \pm b' \pmod{m}$. Since $aa' - bb' = aa' - ba' + ba' - bb' = a'(a - b) + b(a' - b') = a'\mu m + bv m = m(a'\mu + bv)$, where $a'\mu + bv \in \mathbb{Z}$, thus $aa' \equiv bb' \pmod{m}$. \square

Before we talk about the "division" in mod relation, we need talk about the "Modular Multiplicative Inverse" in mod.

Proposition 4. Given $a, b, m \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{m} \Leftrightarrow (a, m) \mid b$.

Proof. $ax \equiv b \pmod{m} \Leftrightarrow \exists y \in \mathbb{Z}$ s.t. $ym = ax - b$ that is the equation $ax - my = b$ has integer solutions $\Leftrightarrow (a, -m) \mid b \Leftrightarrow (a, m) \mid b$. \square

Specially, when $(a, m) = 1$, $\exists x \in \mathbb{Z}$ such that $ax \equiv 1 \pmod{m}$ and x is the Modular Multiplicative Inverse of a .

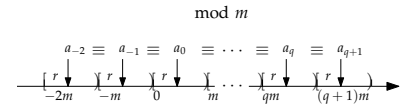


Figure 2: Intuition

Note 6. If $a \equiv b \pmod{m}$, for $n \in \mathbb{Z}$ have $an \equiv bn \pmod{mn}$.

Theorem 2 (The Chinese remained theorem). For $a_1, \dots, a_n, m_1, \dots, m_n \in \mathbb{Z}$, if $(m_i, m'_i) = 1 (i = 1, \dots, n)$ where $m'_j = [m_1, \dots, m_{j-1}, m_{j+1}, \dots, m_n]$, then $\exists x \in \mathbb{Z}$, such that $x \equiv a_i \pmod{m_i} (i = 1, \dots, n)$ at the same time.

Proof. Consider the equations system:

$$\begin{aligned} x &\equiv 1 \pmod{m_1} \\ x &\equiv 0 \pmod{m_2} \\ &\dots \\ x &\equiv 0 \pmod{m_n} \end{aligned}$$

Thus any x that satisfies the last $n - 1$ equations is the multiples of the $[m_2, \dots, m_n] = m_2 \cdots m_n$. Thus $x = tm_2 \cdots m_n, t \in \mathbb{Z}$. Substitute into the first equation, the issue is transformed to whether or not $\exists t, s \in \mathbb{Z}$, s.t. the following equation holds:

$$tm_2 \cdots m_n - sm_1 = 1$$

The answer is positive since $(m_1, m_2 \cdots m_n) = 1$. Thus there exist $x_1 \in \mathbb{Z}$ that satisfies the equation system above. And the same thing for x_2, \dots, x_n . Thus we create a group of orthogonal basis for the equation, and the integer $x = \sum_{i=1}^n a_i x_i$ is the solution of $x \equiv a_i \pmod{m_i} (i = 1, \dots, n)$. \square

Note 7. The condition, $(m_i, m'_i) = 1 (i = 1, \dots, n)$, is equivalent with $m_i (i = 1, \dots, n)$ pairwise co-prime.

Suppose $\exists x_0, x \in \mathbb{Z}$, s.t. $x_0 \equiv a_i \pmod{m_i} (i = 1, \dots, n)$ and $x \equiv a_i \pmod{m_i} (i = 1, \dots, n)$. Then $(x - x_0) \equiv 0 \pmod{m_i} (i = 1, \dots, n)$. Thus $x - x_0$ is the multiples of the least common multiple of m_1, \dots, m_n , that is $x = x_0 + t \prod_{i=1}^n m_i, t \in \mathbb{Z}$, which leads to the all integer solutions of the equation $x \equiv a_i \pmod{m_i} (i = 1, \dots, n)$.

But what if we release the restriction that $m_i (i = 1, \dots, n)$ pairwise co-prime.

Proposition 5. $\exists x \in \mathbb{Z}$, s.t. $x \equiv a \pmod{m} \wedge x \equiv b \pmod{n} \Leftrightarrow (m, n) | (b - a)$.

Proof. \Rightarrow : $\exists \mu, v \in \mathbb{Z}$, s.t. $x - a = \mu m, x - b = vn \Rightarrow b - a = \mu m - vn$, which forms a integer equation, thus $(m, n) | (b - a)$.

\Leftarrow : All $x \in \mathbb{Z}$ that satisfies $x \equiv a \pmod{m}$ has $x - a = \mu m$, for some $\mu \in \mathbb{Z}$. Substitute this formula into the second equation: $a + \mu m \equiv b \pmod{n}$, that is

$$a + \mu m - b = vn$$

for some $\mu, v \in \mathbb{Z}$. That is $\mu m - vn = b - a$ has integer solutions whose sufficient condition is $(m, n) | (b - a)$. \square

So suppose $x_0, x \in \mathbb{Z}$ satisfies the equations system, then $x - x_0 \equiv 0 \pmod{m}$ and $x - x_0 \equiv 0 \pmod{n}$, thus $x = x_0 + t \cdot [m, n], t \in \mathbb{Z}$, this is the all solutions for the equations system.