Elementary Number Theory

Ahto Buldas

September 10, 2018

Division

For any $m > 0$, we define $\mathbb{Z}_m = \{0, 1, \ldots m-1\}$

For any $n, m \in \mathbb{Z}$ $(m > 0)$, there are unique $q \in \mathbb{Z}$ and $r \in \mathbb{Z}_m$ such that:

$$n = qm + r \quad ,$$

where r is called the *reminder* (of n modulo m) and is denoted by

$$r = n \mod m \quad .$$

If $r = 0$, we say that *m divides n* (or *n is divisible by m*) and write $m \mid n$.

If $0 \leq n < m$, then $r = n$; if $m \leq n < 2m$, then $r = n - m \in \mathbb{Z}_m$, etc.

If $-m \leq n < 0$, then $r = n + m$; if $-2m \leq n < -m$, then $r = n + 2m$, etc.

Equivalence of Numbers modulo m

If $a \bmod m = b \bmod m$ (i.e. if $a - b = km$ for a $k \in \mathbb{Z}$, or $m \mid (a - b)$), then we write

$$a \equiv b \pmod{m} \ ,$$

and say that a and b are *equivalent modulo m*.

For example $-1 \equiv 2 \pmod{3}$, $7 \equiv 1 \pmod{3}$, $2 \equiv 12 \pmod{5}$, etc.

$\mathbb{Z}_m$ as a Number Domain

We can define addition and multiplication in $\mathbb{Z}_m$ denoted by $\oplus$ ja $\otimes$ in the next way:

$$\begin{aligned} a \oplus b &= (a+b) \mod m \ , \\ a \otimes b &= (a \cdot b) \mod m. \end{aligned}$$

For example, in $\mathbb{Z}_3$:

$$2 \oplus 2 = 2 \otimes 2 = 1, \quad 1 \oplus 2 = 0 \ ,$$

and in $\mathbb{Z}_5$:

$$2 \oplus 3 = 0, \quad 3 \oplus 3 = 1 = 3 \otimes 2 \quad \text{and} \quad 3 \otimes 4 = 2 \ .$$

Properties of the Function $\bmod m\colon \mathbb{Z} \to \mathbb{Z}_m$

◦ $\bmod m$ is a *projector*: $(a \bmod m) \bmod m = a \bmod m$.

◦ $\bmod m$ preserves the operations (i.e. is a *homomorphism*):

If $a' = a \bmod m$, $b' = b \bmod m$ ja $c' = c \bmod m$, then

$$\begin{aligned} a + b = c \quad &\Longrightarrow \quad a' \oplus b' = c' \\ a \cdot b = c \quad &\Longrightarrow \quad a' \otimes b' = c' \end{aligned} \; .$$

Conclusion 1: When computing

$$a + b \cdot (c + d \cdot (e + f)) \ldots \quad \bmod m$$

we can reduce $\bmod m$ whenever we want.

Conclusion 2: $\oplus$ and $\otimes$ are somewhat similar to ordinary $+$ and $\cdot$

Properties of the $\mathbb{Z}_m$ Number Domain

Though $\oplus$ and $\otimes$ differ from $+$ and $\cdot$, we mostly use $+$ and $\cdot$ if this will not cause confusion.

The following properties hold in $\mathbb{Z}_m$:

- *Commutativity:* $a + b = b + a, \quad a \cdot b = b \cdot a$
- *Associativity:* $(a + b) + c = a + (b + c), \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- *Zero:* $a + 0 = 0 + a = a, \quad a \cdot 0 = 0 \cdot a = 0$
- *Unit:* $a \cdot 1 = 1 \cdot a = a$
- *Distributivity:* $(a + b) \cdot c = a \cdot c + b \cdot c,$

Somewhat Unusual Properties of $\mathbb{Z}_m$

◦ The *inverse* $-a$ of an element $a \in \mathbb{Z}_m$ is $m - a \in \mathbb{Z}_m$, because:

$$a + (m - a) = m \equiv 0 \pmod{m} \ .$$

◦ *Zero divisors:* the product of two non-zero elements can be zero. For example, in $\mathbb{Z}_6$:

$$2 \cdot 3 \equiv 0 \pmod{6} \ .$$

◦ Not every element a has an *inverse* a^{-1} in $\mathbb{Z}_m$:

$$a \cdot a^{-1} \equiv 1 \ .$$

For example, zero divisors never have inverses.

Motivation from Cryptography

In cryptography, the operations should be invertible, because any encrypted message should later be decrypted.

Both mod addition and multiplication are extensively used in cryptography.

Modular addition $\oplus$ is invertible, i.e. $a \oplus x = b$ is always solvable.

Modular multiplication $\otimes$ is not always invertible, i.e. $a \otimes x = b$ can be unsolvable.

For example, $2 \cdot x \equiv 5 \pmod 6$ is not solvable.

The equation $2 \cdot x \equiv 5 \pmod 7$ is solvable: $x = 6$, because

$$2 \cdot 6 = 12 \equiv 5 \pmod 7 .$$

Greatest Common Divisor

By the greatest common divisor $\gcd(a, b)$ of two non-negative numbers a and b (not both zero!) we mean the largest d that divides both numbers, i.e.:

$$\gcd(a, b) = \max\{d\colon d \mid a \text{ and } d \mid b\} \ .$$

Theorem

An element $a \in \mathbb{Z}_m$ is invertible if and only if $\gcd(a, m) = 1$.

Computing $\gcd(a, b)$: Euclid's Algorithm

For $a > b \geq 0$:

$$\gcd(a,b) = \begin{cases} a & \text{if } b = 0 \\ \gcd(b, a \bmod b) & \text{if } b \neq 0 \end{cases} \quad (1)$$

The work of Euclid's algorithm can be represented as a sequence:

$$\gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{m-1}, r_m) = \gcd(r_m, 0) \ ,$$

where $r_0 = a$, $r_1 = b$, and $r_{k+1} = r_{k-1} \bmod r_k < r_k$ for any $k > 1$.

This algorithm *stops* (an m with $r_{m+1} = 0$ exist), because otherwise

$$r_0 > r_1 > r_2 > \ldots > r_k > \ldots$$

is an infinite decreasing sequence of natural numbers, which does not exist.

Correctness of Euclid's Algorithm

Clearly $\gcd(a,0)=a$. We prove $\gcd(a,b)=\gcd(b,a \bmod b)$, if $a>b>0$.

If $D_{a,b}=\{d\colon d \mid a \text{ and } d \mid b\}$ is the set of all common divisors of a and b:

$$\gcd(a,b)=\max D_{a,b} \quad \text{and} \quad \gcd(b,a \mod b)=\max D_{b,a \mod b} \ .$$

It is sufficient to prove that $D_{a,b}=D_{b,a \bmod b}$. This is indeed the case, as:

◦ If $d \mid a$ ja $d \mid b$, then $d \mid (a \bmod b)=a-kb$, and hence $D_{a,b}\subseteq D_{b,a \bmod b}$

◦ If $d \mid (a \bmod b)$ and $d \mid b$, then also $d \mid a$, because $a=(a \bmod b)+kb$, and hence $D_{a,b}\supseteq D_{b,a \bmod b}$.

Efficiency of Euclid's Algorithm

Theorem

Euclid's algorithm finds $\gcd(a,b)$ *using* $1.44 \cdot \log_2 b + 1$ *divisions.*

Let $r_0 > r_1 > \dots r_{n-1} > r_n$ be the sequence produced by Euclid's algorithm so that $r_n = \gcd(a,b)$. Let $\phi = \frac{1+\sqrt{5}}{2}$, i.e. $1 + \phi^{-1} = \phi$. We show by induction that $r_k \geq \phi^{n-k}$ for $1 \leq k \leq m$, i.e. $b = r_1 \geq \phi^{n-1}$.

As $r_{k+1} = r_{k-1} \bmod r_k = r_{k-1} - q_k r_k$, we have $r_{k-1} = q_k r_k + r_{k+1}$, where $q_k \geq 1$ because of $r_{k-1} > r_k$.

Basis: $r_n = \gcd(a,b) \geq 1 = \phi^0$. As $r_{n+1} = 0$ and $q_n r_n = r_{n-1} > r_n$, we have $q_n \geq 2$ and hence $r_{n-1} \geq 2 > \phi^1$.

Step: If $r_{k+1} \geq \phi^{n-k-1}$ and $r_k \geq \phi^{n-k}$, then

$$r_{k-1} = q_k r_k + r_{k+1} \geq r_k + r_{k+1} = \phi^{n-k-1} + \phi^{n-k} = \phi^{n-k}(1+\phi^{-1}) = \phi^{n-k+1}$$

Conclusions

Conclusion 1: If $a > b \geq 0$, then there exist $\alpha, \beta \in \mathbb{Z}$ such that

$$\gcd(a, b) = \alpha a + \beta b \ .$$

Conclusion 2: $\gcd(a, b) = 1$ if and only if $\exists \alpha, \beta \in \mathbb{Z}$, such that

$$\alpha a + \beta b = 1 \ .$$

Proof: If $\gcd(a, b) = 1$, then use Conclusion 1. If $\exists \alpha, \beta \in \mathbb{Z}$ such that

$$\alpha a + \beta b = 1 \ , \tag{2}$$

$d \mid a$ and $d \mid b$, then $d \mid 1$ by (2), i.e. $\gcd(a, b) = 1$.

Conclusion 3: If $\gcd(a, m) = 1$, then $\exists b \in \mathbb{Z}_m$, such that $b \cdot a \bmod m = 1$.

Proof: Given $\alpha, \beta \in \mathbb{Z}$, so that $\alpha a + \beta m = 1$, define $b = \alpha \mod m$.

Finding Inverses with Euclid's Algorithm

Find $\frac{1}{3} \bmod 26$. Let $a = 3$ and $b = 26$.

3	26	a	b
3	2	a	$b - 8a$
1	2	$a - (b - 8a) = 9a - b$	$b - 8a$
1	0	$9a - b$	$b - 8a - 2(9a - b) = -26a + 3b$

Hence, $9 \cdot 3 - 26 = 1$, which means $9 \cdot 3 \equiv 1 \pmod{26}$

Solvability of $ax \bmod n = c$

Theorem

The equation $ax \bmod n = c$ (where $c \in \mathbb{Z}_n$) is solvable iff $\gcd(a,n) \mid c$.

Proof.

If the equation is solvable and $d = \gcd(a,n)$, then $\exists a', n', k \in \mathbb{Z}$ so that $a = a'd$, $n = n'd$, and hence $d \mid c$, because:

$$c = ax \mod n = ax - kn = a'dx - kn'd = (a'x - kn')d \ .$$

If $d = \gcd(a,n) \mid c$, then $\gcd(\frac{a}{d}, \frac{n}{d}) = 1$, which means that $\frac{a}{d}$ has inverse modulo $\frac{n}{d}$ and the equation $\frac{a}{d}x \bmod \frac{n}{d} = \frac{c}{d}$ is solvable, i.e. $\exists k \in \mathbb{Z}$:

$$\frac{a}{d}x - k\frac{n}{d} = \frac{c}{d} \ , \text{ and hence } ax - kn = c \in \mathbb{Z}_n \ ,$$

which means that $ax \mod n = c$. □

How Many Invertible Elements $\bmod m$ are there?

Answer to that question is called the *Euler's function* $\varphi(m)$.

Computing $\varphi(m)$ requires the prime-factorization of m.

A *prime number* is a number if it has exactly two divisors. For example: 2, 3, 5, 7, 11, 13, etc.

Theorem (Fundamental Theorem of Arithmetics)

Every integer $m > 0$ has a unique prime factorization:

$$p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k} \quad ,$$

where $p_1 < p_2 < \ldots < p_k$ are prime numbers.

For example: $60 = 2^2 \cdot 3^1 \cdot 5^1$.

Some Lemmas

Lemma 1: Every composite $m \geq 2$ is a product of primes.
Proof: Let m be the *smallest* composite number that is not a product of primes. Hence, there exist composite numbers $m_1, m_2 < m$, so that $m = m_1 \cdot m_2$. Hence, m_1 and m_2 are products of primes and so must be m. A contradiction.

Lemma 2: If $\gcd(a_1, b) = 1 = \gcd(a_2, b)$, then $\gcd(a_1 \cdot a_2, b) = 1$.
Proof: As there are $\alpha_1, \beta_1, \alpha_2, \beta_2$, so that $\alpha_1 a_1 + \beta_1 b = 1 = \alpha_2 a_2 + \beta_2 b$:

$$1 = \underbrace{(\alpha_1 a_1 + \beta_1 b)}_{1} \underbrace{(\alpha_2 a_2 + \beta_2 b)}_{1} = \underbrace{\alpha_1 \alpha_2}_{\alpha} \cdot a_1 a_2 + \underbrace{(\beta_1 + \alpha_1 a_1 \beta_2)}_{\beta} \cdot b \ ,$$

we have $\gcd(a_1 a_2, b) = 1$.

Fundamental Theorem of Arithmetics: Proof

Theorem

Every composite $m \geq 2$ has a unique prime-factorization $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, where $p_1 \leq p_2 \leq \ldots \leq p_k$.

Proof.

Let m be *the smallest* number that has two different prime-factorisations:

$$p_1 p_2 \ldots p_k = m = q_1 q_2 \ldots q_\ell \ .$$

Hence, $p_i \neq q_j$, because otherwise $m' = m/p_i < m$ also has two different factorizations. Thus, $\gcd(p_1, q_1) = \gcd(p_2, q_1) = \ldots = \gcd(p_k, q_1) = 1$, which by the assumption $q_1 \mid m$ and Lemma 2 implies a contradiction:

$$q_1 = \gcd(m, q_1) = \gcd(p_1 p_2 \cdot \ldots \cdot p_k, q_1) = 1 \ .$$

□

Computing the Euler's Function

Theorem

If $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$ *is the prime decomposition, then*

$$\begin{aligned} \varphi(m) &= \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdot \left(p_2^{e_2} - p_2^{e_2-1}\right) \cdot \ldots \cdot \left(p_k^{e_k} - p_k^{e_k-1}\right) \\ &= m \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) . \end{aligned}$$

The proof uses the inclusion-exclusion principle from counting theory.

Inclusion-Exclusion Principle

Let $P_1, \ldots, P_k$ be subsets of a set M. We want to count those elements of M that belong to none of P_n, i.e. we want to compute $|\, M \setminus \cup_n P_n \,|$.

If $k = 1$, then $|\, M \setminus \cup_n P_n \,| = |M| - |P_1|$.
If $k = 2$, then $|\, M \setminus \cup_n P_n \,| = |M| - |P_1| - |P_2| + |P_1 \cap P_2|$.
If $k = 3$, then:

$$\begin{aligned} |\, M \setminus \cup_n P_n \,| &= |M| - |P_1| - |P_2| - |P_3| \\ &\quad + |P_1 \cap P_2| + |P_1 \cap P_3| + |P_2 \cap P_3| - |P_1 \cap P_2 \cap P_3| \quad . \end{aligned}$$

General case: $|\, M \setminus \cup_n P_n \,| = |M| - \Sigma_1 + \Sigma_2 - \Sigma_3 + \ldots + (-1)^i \Sigma_i + \ldots$.

where $\Sigma_i = \sum_{(j_1,\ldots,j_i) \in c(i)} |P_{j_1} \cap \ldots \cap P_{j_i}|$ and the summation is over the set $c(i)$ of all i-combinations of indices $1, 2, \ldots, k$. There are $\binom{k}{i}$ of them.

Inclusion-Exclusion Principle and Euler's function

Let $M = \mathbb{Z}_m$, where $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$. Let P_n be the set of elements in $\mathbb{Z}_m$ divisible by p_n. Then $\varphi(m) = \mid M \setminus \cup_n P_n \mid$

This is because $a \in \mathbb{Z}_m$ is invertible iff none of $p_1, \ldots p_k$ divides a.

$|P_i| = \frac{m}{p_i}$, $\quad |P_i \cap P_j| = \frac{m}{p_i p_j} \quad \ldots \quad |P_{i_1} \cap \ldots \cap P_{i_\ell}| = \frac{m}{p_{i_1} p_{i_2} \cdots p_{i_\ell}}$.

and hence:

$$\begin{aligned}\varphi(m) &= m - \frac{m}{p_1} - \ldots - \frac{m}{p_k} + \frac{m}{p_1 p_2} + \ldots + \frac{m}{p_{k-1} p_k} - \frac{m}{p_1 p_2 p_3} - \ldots \\ &= m \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) .\end{aligned}$$