ITC8190
Mathematics for Computer Science
Congruences

Aleksandr Lenin

October 30th, 2018

Two integers a and b are said to be **congruent modulo n** if n divides their difference. In other words, $n|a-b$.

Since congruence is an equivalence relation on the set of integers, any two congruent integers fall in the same equivalence class.

$$a \equiv b \pmod{n} \Longleftrightarrow n|a-b \Longleftrightarrow \exists k \in \mathbb{Z} : a = b + kn \ .$$

I.e.,

$$-1 \equiv 2 \pmod{3} \ , \quad 7 \equiv 1 \pmod{3} \ , \quad 2 \equiv 12 \pmod{5} \ .$$

We can define addition $\oplus$ and multiplication $\otimes$ in number domain $\mathbf{Z}_m$ by

$$a \oplus b = (a + b) \bmod m \ ,$$
$$a \otimes b = (a \cdot b) \bmod m \ .$$

I.e., in $\mathbb{Z}_3$, it holds that

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

and in $\mathbb{Z}_5$:

$$2 \oplus 3 = 0 \ , \qquad 3 \oplus 3 = 3 \otimes 2 = 1 \ , \qquad 3 \otimes 4 = 2 \ .$$

mod m may be viewed as a function $\quad \bmod m : \mathbb{Z} \to \mathbb{Z}_m \ .$
with the following properties:

- mod m is idemponent: $(a \bmod m) \bmod m = a \bmod m$.

$$\begin{aligned}(a \bmod m) \bmod m &= (a + \alpha m) \bmod m \\ &= (a + \alpha m) + \beta m = a + (\alpha + \beta) m \\ &= a \bmod m \ .\end{aligned}$$

- mod m preserves operations (i.e. is a ring homomorphism):

$$\begin{aligned}a \bmod m + b \bmod m &= a + \alpha m + b + \beta m \\ &= a + b + (\alpha + \beta) m \\ &= (a + b) \bmod m \ , \\ a \bmod m \cdot b \bmod m &= (a + \alpha m)(b + \beta m) \\ &= ab + \underbrace{(a\beta + \alpha b + \alpha\beta m)}_{\in \mathbb{Z}} m \\ &= (a \cdot b) \bmod m \ .\end{aligned}$$

Conclusion 1

When computing

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

we can reduce $\bmod m$ *whenever we like, the result will not change.*

Conclusion 2

Operations $\oplus$ *and* $\otimes$ *are somewhat similar to usual addition* $+$ *and multiplication* $\times$ *in* $\mathbb{Z}$*.*

Despite $\oplus$ and $\otimes$ differ from $+$ and $\times$, we will use the usual notation $+$ and $\times$ whenever appropriate, if it will not cause confusion.

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

- Associativity: $a + (b + c) = (a + b) + c$, as well as $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Commutativity: $a + b = b + a$, and $a \cdot b = b \cdot a$
- Distributivity: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$
- Zero: $a + 0 = 0 + a$ (0 is the additive identity)
- Unit: $a \cdot 1 = 1 \cdot a$ (1 is the multiplicative identity)
- Additive inverse $-a$ of element $a \in \mathbb{Z}_m$ is $m - a \in \mathbb{Z}_m$, because

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

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

- Zero divisors: the product of two non-zero elements can be zero. I.e.,

$$2 \cdot 3 \equiv 0 \pmod{6}\ , \qquad 3 \cdot 4 \equiv 0 \pmod{6}\ .$$

- The sum of two positive elements can be zero. I.e.,

$$2 + 3 \equiv 0 \pmod{5}\ , \qquad 5 + 7 \equiv 0 \pmod{12}\ .$$

- Not every element a has a multiplicative inverse $a^{-1} \in \mathbb{Z}_m$ such that $a \cdot a^{-1} = 1$. I.e., $2^{-1} = 3$ in $\mathbb{Z}_5$, since

$$2 \cdot 3 = 6 \equiv 1 \pmod{5}\ ,$$

but 2 is not invertible in $\mathbb{Z}_6$.

Since some elements are not invertible in $\mathbb{Z}_n$, some congruence equations with non-invertible coefficients are not solvable. I.e.,

$$2 \cdot x \equiv 5 \pmod{7}$$

is solvable, and the solution is $x = 6$ because

$$2 \cdot 6 = 12 \equiv 5 \pmod{7} ,$$

but, the equation

$$2 \cdot x \equiv 5 \pmod{6}$$

is not solvable.

Which elements are invertible in $\mathbb{Z}_m$?

Theorem 1

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

Proof.

Let $a \in \mathbb{Z}_m$ be such that $\gcd(a, m) = 1$. Then, by the Bézout identity, there exist integers α and β such that

$$1 = \gcd(a, b) = \alpha a + \beta m \equiv \alpha a \pmod{m} ,$$

which means that $a^{-1} \equiv \alpha \pmod{m}$.

Let a be an invertible element of $\mathbb{Z}_m$. Then there exists $a^{-1} \in \mathbb{Z}_m$ such that $a \cdot a^{-1} \equiv 1 \pmod{m}$. Then $a \cdot a^{-1} + \beta m = 1$ for some $\beta \in \mathbb{Z}$, and by the Bézout identity, it means that $\gcd(a, m) = 1$. □

Theorem 2

Zero divisers are not invertible in $\mathbb{Z}_m$.

Proof.

Let $a \in \mathbb{Z}_m$, $a \neq 0$ be a zero divisor, i.e. there exists $b \in \mathbb{Z}_m$, $b \neq 0$ such that $ab \equiv 0 \pmod{m}$. Assume a is invertible, i.e. there exists $a^{-1} \in \mathbb{Z}_m$ such that $a \cdot a^{-1} \equiv 1 \pmod{m}$. Then

$$\begin{aligned} ab \equiv 0 \pmod{m} &\implies a^{-1}ab \equiv a^{-1} \cdot 0 \pmod{m} \\ &\implies b \equiv 0 \pmod{m}\ , \end{aligned}$$

a contradiction. □

Theorem 3

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

Proof.

If the equation is solvable and $\gcd(a, n) = d$, then there exist integers $\alpha, \beta \in \mathbb{Z}$ such that $a = \alpha d$ and $n = \beta d$, and hence $d | c$, because

$$c = ax \bmod n = ax + kn = \alpha dx + \beta dk = (\alpha x + \beta k) d \ ,$$

If $d = \gcd(a, n)$ and $d | c$, then $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, and hence $\frac{a}{d}$ is invertible modulo $\frac{n}{d}$, and the equation $\frac{a}{d} x \bmod \frac{n}{d} = \frac{c}{d}$ is solvable, i.e. $\exists k \in \mathbb{Z}$:

$$\frac{a}{d} x + k \frac{n}{d} = \frac{c}{d} \implies ax + kn = c \implies ax = c \pmod{n} \ .$$

$\square$

How many invertible elements are there in $\mathbb{Z}_n$?

The **Euler's phi function** (a.k.a. **Euler's totient function**) for any given $n > 0$ returns the number of integers in the range $0, \ldots, n-1$ that are co-prime to n. Let $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e^k}$. Then

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) \quad .$$

This formula works in all cases. However, if n is some prime p, then the formula takes its simplified form

$$\varphi(p) = p - 1 \quad .$$

If $n = n_1 \cdot n_2$, such that $\gcd(n_1, n_2) = 1$, then

$$\varphi(n_1 \cdot n_2) = \phi(n_1) \cdot \phi(n_2) \quad .$$

$$\varphi(36) = \phi(2^2 \cdot 3^2) = 36 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12 \ ,$$
$$\varphi(6) = \phi(2 \cdot 3) = \phi(2) \cdot \phi(3) = (2 - 1)(3 - 1) = 2 \ ,$$
$$\varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2) \cdot (3 - 1) = 4 \cdot \left(1 - \frac{1}{2}\right) \cdot 2 = 4 \ .$$

Indeed, only two integers are co-prime to 6, they are 1 and 5. Integers co-prime to 12 are $\{1, 5, 7, 11\}$, 4 of them in total.

Theorem 4

If $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$ *is the prime decomposition of* n *and* $n > 0$*, then*

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right) \quad .$$

The proof uses inclusion-exclusion principle from counting theory.

Let $P_1, P_2, \ldots, P_k$ be the subsets of 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:

$$|M \setminus \cup_n P_n| = |M| - |P_1| - |P_2| - |P_3| + |P_1 \cap P_2| + |P_2 \cap P_3| + |P_1 \cap P_3| - |P_1 \cap P_2 \cap P_3| \; .$$

General case:

$$|M \setminus \cup_n P_n| = |M| - \Sigma_1 + \Sigma_2 - \Sigma_3 + \ldots_(- 1)^i \Sigma_i + \ldots \quad ,$$

where

$$\Sigma_i = \sum_{j_1,\ldots,j_i} \in c(i) |P_{j_1} \cap \ldots \cap P_{j_i}| \quad ,$$

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.

Proof.

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

This is because $a \in \mathbb{Z}_m$ is invertible if none iff none of $p_1, p_2, \ldots, p_k$ divides a.

$$
\begin{aligned}
|P_i| &= \frac{m}{p_i} \quad , \\
|P_i \cap P_j| &= \frac{m}{p_i p_j} \quad , \\
|P_{i_1} \cap \ldots \cap P_{i_l}| &= \frac{m}{p_{i_1} p_{i_2} \cdots p_{i_l}} \quad .
\end{aligned}
$$

□

And hence:

$$
\begin{aligned}
\phi(n) &= m - \frac{m}{p_1} - \frac{m}{p_2} - \ldots - \frac{m}{p_k} + \frac{m}{p_1 p_2} + \ldots + \frac{m}{p_1 p_k} + \ldots + \frac{m}{p_2 p_k} - \ldots - \frac{m}{p_1 p_2 p_k} - \ldots \\
&= m \cdot \left(1 - \frac{1}{p_1} - \frac{1}{p_2} - \ldots - \frac{1}{p_k} + \frac{1}{p_1 p_2} + \ldots + \frac{1}{p_1 p_k} + \ldots + \frac{1}{p_2 p_k} - \ldots - \frac{1}{p_1 p_2 p_k} - \ldots\right) \\
&= m \cdot \left[\left(1 - \frac{1}{p_2} - \ldots - \frac{1}{p_k} + \ldots + \frac{1}{p_2 p_k} + \ldots\right) - \frac{1}{p_1} \cdot \left(1 - \frac{1}{p_2} - \ldots - \frac{1}{p_k} + \ldots + \frac{1}{p_2 p_k} + \ldots\right)\right] \\
&= m \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2} - \ldots - \frac{1}{p_k} + \ldots + \frac{1}{p_2 p_k} + \ldots\right) \\
&= m \cdot \left(1 - \frac{1}{p_1}\right)\left[\left(1 - \ldots - \frac{1}{p_k}\right) - \frac{1}{p_2} \cdot \left(1 - \ldots - \frac{1}{p_k}\right)\right] = m \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)
\end{aligned}
$$

□

Theorem 5 (Chinese Remainder Theorem (CRT))

If $n_1, n_2, \ldots, n_k$ *are pairwise co-prime integers and if* $a_1, a_2, \ldots, a_k$ *are any integers such that* $0 \leqslant a_i < n_i$ *for every* $i = 1, 2, \ldots, k$*, then the system of congruence equations*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\cdots \\ x &\equiv a_k \pmod{n_k} \end{aligned} \tag{1}$$

has a unqiue solution $0 \leqslant x < N$*, where* $N = \prod_{i=1}^{k} n_k$*, such that* $x \bmod n_i = a_i$ *for every* $i = 1, 2, \ldots, k$*.*

Proof.

Suppose that x and y are both solutions to (1). Then

$$\forall i = 1, 2, \ldots, k : x \bmod n_i = y \bmod n_i = a_i \implies n_i | x - y \ .$$

Since all n_i are pairwise co-prime, their product N also divides $x - y$, and hence $x \equiv y \pmod{N}$. Considering that x and y are nonnegative and less than N, the statement $N | x - y$ is true only if $x = y$. Hence, the solution to the system (1) is unique. □

Theorem 6

Let n_1, n_2 *be co-prime integers and let* a_1, a_2 *be any integers such that* $a_1 < n_1$ *and* $0 \leqslant a_2 < n_2$. *Then the solution to the system of congruence equations*

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

is

$$x \equiv a_1 m_2 n_2 + a_2 m_1 n_1 \quad ,$$

where m_1 *and* m_2 *are the coefficients of the Bézout identity* $m_1 n_1 + m_2 n_2 = 1 = \gcd(n_1, n_2)$.

Proof.

Indeed, considering that by the Bézout identity $m_2 n_2 = 1 - m_1 n_1$,

$$\begin{aligned} x &= a_1 m_2 n_2 + a_2 m_1 n_1 = a_1(1 - m_1 n_1) + a_2 m_1 n_1 \\ &= a_1 + (a_2 - a_1) m_1 n_1 \implies x \equiv a_1 \pmod{n_1} . \end{aligned}$$

Similarly, by the Bézout identity, $m_1 n_1 = 1 - m_2 n_2$, and hence

$$\begin{aligned} x &= a_1 m_2 n_2 + a_2 m_1 n_1 = a_1 m_2 n_2 + a_2(1 - m_2 n_2) \\ &= a_2 + (a_1 - a_2) m_2 n_2 \implies x \equiv a_2 \pmod{n_2} . \end{aligned}$$

□

Theorem 7

Let $n_1, n_2, \ldots, n_k$ *be pairwise co-prime integers and let* $a_1, a_2, \ldots, a_k$ *be any integers such that* $0 \leqslant a_i < n_i$ *for all* $i = 1, 2, \ldots, k$, *and let* $N = n_1 \cdot n_2 \cdot n_k$. *Then the solution of the system of congruence equations*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\cdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

is

$$x \equiv \sum_{i=1}^{k} a_i M_i N_i \pmod{N} \ ,$$

where $N_i = \frac{N}{n_i}$ *and* M_i *is the Bézout coefficient satisfying* $M_i N_i + m_i n_i = 1 = \gcd(N_i, n_i)$.

Proof.

As N_j is a multiple of n_i for $i \neq j$, it holds that

$$x = \sum_{i=1}^{k} a_i M_i N_i = \underbrace{a_1 M_1 N_1}_{\equiv 0 \pmod{n_i}} + \ldots + a_i M_i N_i + \ldots + \underbrace{a_k M_k N_k}_{\equiv 0 \pmod{n}_i}$$

$$\equiv a_i M_i N_i \pmod{n_i} \ .$$

Since $gcd(N_i, n_i) = 1$, the Bézout identity $M_i N_i + m_i n_i = 1$ applies, and hence $M_i N_i = 1 - m_i n_i$. And so

$$x \equiv a_i M_i N_i \pmod{n_i} \equiv a_i(1-m_i n_i) \pmod{n_i} \equiv a_i \pmod{n_i} \ .$$

□

?

THANK YOU
FOR
YOUR
ATTENTION
ANY QUESTIONS?