Modular Arithmetic

1 Basic modular arithmetic

1.1 Definition

if a,b are integers and m is a positive integer then a is congruent to b modulo m iff m—(a-b). Notation $a \equiv b(modm)$
Example: 8≡ 5(mod3) because $3|(8-5)$; $-5 \equiv 9(\text{mod}7)$ because $7|(-5-9)$

1.2 Lemma

If a,b,m are integers and $m > 0$ then $a \equiv b(modm)$ iff $rem(a,m) = rem(b,m)$

1.3 Lemma

Let m be a positive integer and let $a \equiv b(modm)$ and $c \equiv d(modm)$ Then

$$a + c \equiv b + d(\text{mod}m) \quad \text{and} \quad ac \equiv bd(\text{mod}m)$$

2 Linear congruences

Congruences work a lot like equations, but there are some differences:

- if $ac \equiv bc(\text{mod}m)$ and $c \not\equiv 0(\text{mod}m)$ it is possible that $a \not\equiv b(\text{mod}m)$. For example $2 \cdot 3 \equiv 4 \cdot 3(\text{mod}6)$, but $2 \neq 4(\text{mod}6)$
- If $a \equiv b(\text{mod}m)$ and $c \equiv d(\text{mod}m)$, it is possible that $a^c \not\equiv d^d(\text{mod}m)$
- A congruence of the form $ax \equiv b(\text{mod}m)$ is called a **linear congruence**
- Such congruences often appear in applications of number theory
- Solving such a congruence means finding all c (by default, in the range $\{0, 1, ..., m-1\}$) such that $ac \equiv b(\text{mod}m)$, such c might not be unique

2.1 Example

Solve $3x + 1 \equiv 5(\text{mod}7)$
Subtract 1 from both sides, get $3x \equiv 4(\text{mod}7)$
Now multiply both sides by 5, have $15x = 20(\text{mod}7)$
Since 15≡ 1(mod7) and $20 \equiv 6(\text{mod}7)$, have $x \equiv 6(\text{mod}7)$. So $x = 6$

3 Multiplicative inverses

- An easy way to solve equation $ax = b$ is to multiply both parts by a^{-1}
- We cannot do this within integers, but we often can when working modulo m
- Call $\bar{a}$ the (multiplicative) inverse of a modulo m if $\bar{\mathbf{a}}a \equiv 1(\text{mod}m)$
- Multiplicative inverses do not always exist, e.g. $2\bar{a} \not\equiv 1(\text{mod}4)$ for any $\bar{a}$

3.1 Theorem

If gcd(a,m)=1 then the inverse of a modulo m exists, and is unique (that is, there is a unique $0 \leqslant \bar{a} < m$ with $\bar{a}a \equiv 1(\text{mod}m)$)

3.2 Proof

We show existence, and leave uniqueness as an exercise
Since gcd(a,m)=1, we have sa+tm=1 for some s, t. Then $sa \equiv 1(\text{mod}m)$
Let $s = qm + r$ where $0 \leqslant r < m$, then $ra = (s - qm)a \equiv sa \equiv 1(\text{mod}m)$ so r is the required inverse

- note that s can be found by using euclid's algorithm. Then r is easy to find

4 The Chinese remainder theorem

4.1 Theorem

Let $m_1, ..., m_n$ be pairwise relatively prime positive integers and $a_1, ..., a_n$ arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. That is, there is a unique solution x with $- \leqslant x < m$ and every other solution is congruent to x modulo m.

4.2 Proof

Let $M_k = m/m_k$
We have $gcd(M_k, m_k)$. Hence $M_k y_k \equiv q(\bmod m_k)$ for some y_k
Let $x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n$
We show that $x \equiv a_k (\bmod m_k)$ for all k.
Notice that $M_j \equiv 0(\bmod m_k) if j \neq k$. Hence $x \equiv a_k M_k y_k \equiv a_k (\bmod m_k)$

5 Computer arithmetic with large numbers

- Suppose $m_1, m_2, ..., m_n$ are all pairwise relatively prime (and all $\geqslant 2$)
- By the chinese remainder theorem, any number $0 \leqslant a < m$ can all be uniquely represented by the n-tuple $(a_1, a_2, ..., a_n)$ where $a_i = rem(a, m_i)$ for all i
- Example: let $m_1 = 3$ and $m_2 = 4$. Then the numbers < 12 are represented as

$$\begin{array}{rcl rcl rcl} 0 & = & (0,0) & 4 & = & (1,0) & 8 & = & (2,0) \\ 1 & = & (1,1) & 5 & = & (2,1) & 9 & = & (0,1) \\ 2 & = & (2,2) & 6 & = & (0,2) & 10 & = & (1,2) \\ 3 & = & (0,3) & 7 & = & (1,3) & 11 & = & (2,3) \end{array}$$

- To perform arithmetic with large numbers, choose the moduli $m_1, ..., m_n$ so that $m = m_1 \cdots m_n >$ the result of the operations you want to carry out
- Then arithmetic can be performed with representations of numbers
- Example: compute $2 \cdot 5$. Instead, multiply (2,2) and (2,1) component wise. 1st component modulo 3 and 2nd modulo 4. Get (1,2) which represents 10
- Advantages: can work with very large numbers and can compute in parallel
- Particularly good choices for m_i: numbers of the form $2^p - 1$

6 Fermat's Little theorem

6.1 Theorem

If p is a prime and a is not a multiple of p then $a^{p-1} \equiv 1(\bmod p)$
Furthermore, for every integer a, $a^p \equiv a(\bmod p)$

6.2 Example

- We know how to find inverses modulo prime p (via Euclid's algorithm)
- The above theorem gives an alternate approach: $a^{p-2} \cdot a \equiv 1(\bmod p)$ hence $rem(a^{p-2}, p)$ is the required inverse

Find the multiplicative inverse of 6 modulo 17
Solution: we need to compute $rem(6^{15}, 17)$, which can be done as follows.

$$6^2 \equiv 36 \equiv 2(\bmod 17)$$
$$6^4 \equiv \left(6^2\right)^2 \equiv 2^2 \equiv 4(\bmod 17)$$
$$6^8 \equiv \left(6^4\right)^2 \equiv 4^2 \equiv 16(\bmod 17)$$
$$6^{15} \equiv 6^8 \cdot 6^4 \cdot 6^2 \cdot 6 \equiv 16 \cdot 4 \cdot 2 \cdot 6 \equiv 3(\bmod 17)$$

Therefore, $rem(6^1 6, 17) = 3$ is the required inverse. Indeed $3 \cdot 6 \equiv 1(\bmod 17)$

7 Euler's theorem

Recall Euler's ϕ-function. $\phi(n)$ is the number of integers $1 \leqslant a \leqslant n$ that are relatively prime with n.
Euler's theorem generalises Fermat's little theorem to non-prime moduli

7.1 Theorem

If n is a positive integer and $gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1(\bmod n)$

7.2 Method

- If n is a prime then $\phi(n) = n - 1$, so this is indeed a generalisation
- If gcd(a,n)=1, then, as we proved, the inverse of a modulo n exists and can be found using Euclid's algorithm
- By Euler's Theorem, it can also be found as $rem(a^{\phi(n)-1}, n)$
- Can a have a multiplicative inverse modulo n is $gcd(a, n) > 1$? No
  - If the inverse $\bar{a}$ exists we have $\bar{a}a \equiv 1(\bmod n)$, i.e. $\bar{a}a - 1 = kn$ for some k
  - Rewrite as $\bar{a}a + (-k)n = 1$, it follows that $gcd(a, n) = 1$

8 Computing Euler's ϕ-function

8.1 Lemma

If m_1 and m_2 are relatively prime then $\phi(m_1 \cdot m_2) = \phi(m_1) \cdot \phi(m_2)$.
If p is prime then $\phi(p^k) = p^k - p^{k-1}$

8.2 Proof

By the chinese remainder theorem, there is a 1 to 1 correspondence between

- numbers x with $0 \leqslant x < m_1 m_2$ and
- pairs $(1_2, a_2)$ such that $0 \leqslant a_i < m_i$ and $x \equiv a_i(\bmod m_i)$ for $i = 1, 2$

Since $a_i = rem(x, m_i)$ we have $gcd(x, m_i) = gcd(a_i, m_i)$ for i=1,2
We have $gcd(x, m_1, m_2) = gcd(x, m_1) \cdot gcd(x, m_2) = gcd(a_1, m_1) \cdot gcd(a_2, m_2)$ (the first equality holds because $gcd(m_1, m_2) = 1$)
In particular, $gcd(x, m_1 m_2) = 1$ iff $gcd(a_1, m_1) = gcd(a_2, m_2) = 1$. This immediately implies $\phi(m_1 cdot m_2) = \phi(m_1) \cdot \phi(m_2)$

8.3 Example

$$\phi(75) = \phi\left(3 \cdot 5^2\right) = \phi(3) \cdot \phi\left(5^2\right) = \left(3^1 - 3^0\right) \cdot \left(5^2 - 5\right) = 40$$