Congruence of Integers

November 14, 2013

Week 11-12

1 Congruence of Integers

Definition 1. Let m be a positive integer. For integers a and b, if m divides $b - a$, we say that a is **congruent** to b **modulo** m, written $a \equiv b \bmod m$.

Every integer is congruent to exactly one of the following integers modulo m:

$$0, 1, 2, \ldots, m-1.$$

Proposition 2 (Equivalence Relation)**.** *Let m be a positive integer. For integers $a, b, c \in \mathbb{Z}$, we have*

(1) $a \equiv a \bmod m$*;*

(2) *If* $a \equiv b \bmod m$*, then* $b \equiv a \bmod m$*.*

(2) *If* $a \equiv b \bmod m$ *and* $b \equiv c \bmod m$*, then* $a \equiv c \bmod m$*.*

Proof. Trivial. □

Proposition 3. *Let* $a \equiv b \bmod m$ *and* $c \equiv d \bmod m$*. Then*

(1) $a + c \equiv b + d \bmod m$*;*

(2) $ac \equiv bd \bmod m$*;*

(3) $a^n \equiv b^n \bmod m$ *for any positive integer* n*.*

Proof. Trivial □

Proposition 4. *Let* a, b, c *be integers,* $a \neq 0$*, and* m *be a positive integer.*

(1) If $a \mid m$*, then* $ab \equiv ac \bmod m$ *iff* $b \equiv c \bmod \frac{m}{a}$*.*

(2) If $\gcd(a,m)=1$*, then* $ab \equiv ac \bmod m$ *iff* $b \equiv c \bmod m$*.*

(3) If p *is a prime and* $p \nmid a$*, then* $ab \equiv ac \bmod p$ *iff* $b \equiv c \bmod p$*.*

Proof. (1) $ab \equiv ac \bmod m \Leftrightarrow ab = ac + km$ for some $k \in \mathbb{Z} \Leftrightarrow b = c + k \cdot \frac{m}{a}$ for some $k \in \mathbb{Z} \Leftrightarrow b \equiv c \bmod \frac{m}{a}$.

(2) If $ab \equiv ac \bmod m$. Then m divides $ab - ac = a(b-c)$ by definition. Since $\gcd(a,m)=1$, we have $m|(b-c)$. Hence $b \equiv c \bmod m$.

(3) In particular, when p is a prime and $p \nmid a$, then $\gcd(a,p)=1$. □

2 Congruence Equation

Let m be a positive integer and let $a, b \in \mathbb{Z}$. The equation

$$ax \equiv b \bmod m \tag{1}$$

is called a **linear congruence equation**. Solving the linear congruence equation (1) is meant to find all integers $x \in \mathbb{Z}$ such that $m|(ax-b)$.

Proposition 5. *Let* $d = \gcd(a,m)$*. The linear congruence equation (1) has a solution if and only if* $d|b$*.*

Proof. Assume that (1) has a solution, i.e., there exists an integer k such that $ax - b = km$. Then $b = ax - km$ is a multiple of d. So $d|b$.

Conversely, if $d|b$, write $b = dc$. By the Euclidean Algorithm, there exist $s, t \in \mathbb{Z}$ such that $d = as + mt$. Multiplying $c(=\frac{b}{d})$ to both sides, we have

$$acs + mct = dc = b.$$

Hence $x = \frac{b}{d}s$ is a solution of (1). □

Let $x = s_1$ and $x = s_2$ be two solutions of (1). It is clear that $x = s_1 - s_2$ is a solution of the equation

$$ax \equiv 0 \bmod m. \tag{2}$$

So any solution of (1) can be expressed as a particular solution of (1) plus a solution of (2). Note that (2) is equivalent to $\frac{a}{d}x \equiv 0 \bmod \frac{m}{d}$; since $\gcd(\frac{q}{d}, \frac{m}{d}) = 1$, it is further equivalent to $x \equiv 0 \bmod \frac{m}{d}$. Thus all solutions of (2) are given by

$$x = \frac{m}{d}k, \quad k \in \mathbb{Z}.$$

Hence all solutions of (1) are given by

$$x = \frac{b}{d}s + \frac{m}{d}k, \quad k \in \mathbb{Z}, \quad \text{where} \quad d = \gcd(a, m).$$

Corollary 6. *If d is a common factor of a, b, m, then the linear congruence equation (1) is equivalent to*

$$\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{m}{d}. \tag{3}$$

Proof. Given a solution $x = s$ of (1). Then $as = b + km$ for some $k \in \mathbb{Z}$. Clearly, $\frac{a}{d}s = \frac{b}{d} + \frac{m}{d}k$. This means that $x = s$ is a solution of (3). Conversely, given a solution $x = s$ of (3), that is, $\frac{a}{d}s = \frac{b}{d} + \frac{m}{d}k$ for some $k \in \mathbb{Z}$. Multiplying d to both sides, we have $as = b + mk$. This means that $x = s$ is a solution of (1). □

Example 1. $3x = 6 \bmod 4$.

Since $\gcd(3, 4) = 1 = 4 - 3$, then all solutions are given by $x = -6 + 4k$, where $k \in \mathbb{Z}$, or

$$x = 2 + 4k, \quad k \in \mathbb{Z}.$$

Example 2.

$$6x \equiv 9 \bmod 15 \Leftrightarrow \frac{6}{3}x \equiv \frac{9}{3} \bmod \frac{15}{3} \Leftrightarrow 2x \equiv 3 \bmod 5.$$

3 The System $\mathbb{Z}_m$

Let $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$, where $m \geq 2$. For $a, b \in \mathbb{Z}_m$, we define

$$a \oplus b = s$$

if $a + b \equiv s$ with $s \in \mathbb{Z}_m$, and define

$$a \odot b = t$$

if $ab \equiv t$ with $t \in \mathbb{Z}_m$.

Proposition 7. *(1) $a \oplus b = b \oplus a$,*

(2) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$,

(3) $a \odot b = b \odot a$,

(4) $(a \odot b) \odot c = a \odot (b \odot c)$,

(5) $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$,

(6) $0 \oplus a = a$,

(7) $1 \odot a = a$.

(8) $0 \odot a = 0$.

An element $a \in \mathbb{Z}_m$ is said to be **invertible** if there is an element $b \in \mathbb{Z}_m$ such that $a \odot b = 1$; if so the element b is called an **inverse** of a in $\mathbb{Z}_m$. If $m \geq 2$, the element $m-1$ is always invertible and its inverse is itself.

Proposition 8. *Let m be a positive integer. Then an element $a \in \mathbb{Z}_m$ is invertible iff* $\gcd(a, m) = 1$.

Proof. Necessity: Let $b \in \mathbb{Z}_m$ be an inverse of a. Then $ab \equiv 1 \bmod m$, that is, $ab + km = 1$ for some $k \in \mathbb{Z}$. Clearly, $\gcd(a, m)$ divides $ab + km$, and subsequently divides 1. It then forces $\gcd(a, m) = 1$.

Sufficiency: Since $\gcd(a, m) = 1$, there exist integers $s, t \in \mathbb{Z}$ such that $1 = as + mt$ by the Euclidean Algorithm. Thus $as \equiv 1 \bmod m$. This means that s is an inverse of a. □

4 Fermat's Little Theorem

Theorem 9. *Let p be a prime number. If a is an integer not divisible by p, then*

$$a^{p-1} \equiv 1 \bmod p.$$

Proof. Consider the numbers $a, 2a, \ldots, (p-1)a$ modulo p in $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. These integers modulo p are distinct, for if $xa \equiv ya \bmod p$ for some $x, y \in \mathbb{Z}_m$, then $x \equiv y \bmod p$, so $x = y$, and since $1, 2, \ldots, p-1$ are distinct. Thus these integers modulo p are just the list $1, 2, \ldots, p-1$. Multiplying these $p-1$ integers together, we have

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \bmod p.$$

Since $(p-1)!$ and p are coprime each other, we thus have

$$a^{p-1} \equiv 1 \bmod p.$$

□

Proposition 10 (Generalized Fermat's Little Theorem)**.** *Let p, q be distinct prime numbers. If a is an integer such that $p \nmid a$ and $q \nmid a$, then*

$$a^{(p-1)(q-1)} \equiv 1 \bmod pq.$$

Proof. By Fermat's Little Theorem we have $a^{p-1} \equiv 1 \bmod p$. Raising both sides to the $(q-1)$th power, we have

$$a^{(p-1)(q-1)} \equiv 1 \bmod p.$$

This means that $p \big| \big(a^{(p-1)(q-1)} - 1\big)$. Analogously, $q \big| \big(a^{(p-1)(q-1)} - 1\big)$. Since p and q are coprime each other, we then have $pq \big| \big(a^{(p-1)(q-1)} - 1\big)$, namely, $a^{(p-1)(q-1)} \equiv 1 \bmod pq$. □

5 Roots of Unity Modulo m

Proposition 11. *Let p be a prime. Let k be a positive integer coprime to $p-1$. Then*

(a) There exists a positive integer s such that $sk \equiv 1 \bmod p-1$.

(b) For each $b \in \mathbb{Z}$ not divisible by p, the congruence equation

$$x^k \equiv b \bmod p$$

has a unique solution $x = b^s$, where s is as in (a).

Proof. (a) By the Euclidean Algorithm there exist integers $s, t \in \mathbb{Z}$ such that $sk - t(p-1) = 1$. Hence $sk \equiv 1 \bmod p-1$.

(b) Suppose that x is a solution to $x^k \equiv b \bmod p$. Since p does not divide b, it does not divide x; i.e., $\gcd(x, p) = 1$. By Fermat's Little Theorem we have $x^{p-1} \equiv 1 \bmod p$. Then $x^{t(p-1)} \equiv 1 \bmod p$. Thus

$$x \equiv x^{1+t(p-1)} \equiv x^{sk} \equiv (x^k)^s \equiv b^s \bmod p.$$

Indeed, $x = b^s$ is a solution as

$$(b^s)^k \equiv b^{sk} \equiv b^{1+t(p-1)} \equiv b \cdot (b^{p-1})^t \equiv b \bmod p.$$

□

Proposition 12. *Let p, q be distinct primes. Let k be a positive integer coprime to both $p-1$ and $q-1$. Then the following statements are valid.*

(a) There exists a positive integer s such that $sk \equiv 1 \bmod (p-1)(q-1)$.

(b) For each $b \in \mathbb{Z}$ such that $p \nmid b$ and $q \nmid b$, the congruence equation

$$x^k \equiv b \bmod pq$$

has a unique solution $x = b^s$, where s is as in (a).

Proof. (a) It follows from the Euclidean Algorithm. In fact, there exists $s, t \in \mathbb{Z}$ such that $sk - t(p-1)(q-1) = 1$. Then $sk \equiv 1 \bmod (p-1)(q-1)$.

(b) Suppose x is a solution for $x^k \equiv b \bmod pq$. Since $p \nmid b$ and $q \nmid b$, we have $p \nmid x$ and $q \nmid x$. By the Generalized Fermat's Little Theorem, we have $x^{(p-1)(q-1)} \equiv 1 \bmod pq$. Then $x^{t(p-1)(q-1)} \equiv 1 \bmod pq$. Hence

$$x \equiv x^{1+t(p-1)(q-1)} \equiv x^{sk} \equiv (x^k)^s \equiv b^s \bmod pq.$$

Indeed $x = b^s$ is a solution,

$$(b^s)^k \equiv b^{sk} \equiv b^{1+t(p1)(q-1)} \equiv b \cdot b^{t(p-1)(q-1)} \equiv b \bmod pq.$$

□

Proposition 13. *Let p be a prime. If a is an integer such that $a^2 \equiv 1 \bmod p$, then either $a \equiv 1 \bmod p$ or $a \equiv -1 \bmod p$.*

Proof. Since $a^2 \equiv 1 \bmod p$, then $p|(a^2-1)$, i.e., $p|(a-1)(a+1)$. Hence we have either $p|(a-1)$ or $p|(a+1)$. In other words, we have either $a \equiv 1 \bmod p$ or $a \equiv -1 \bmod p$. □

6 RSA Cryptography System

Definition 14. An **RSA public key cryptography system** is a tuple (S, N, e, d, E, D), where $S = \{0, 1, 2, \ldots, N-1\}$, $N = pq$, p and q are distinct primes numbers, e and d are positive integers such that $ed \equiv 1 \bmod (p-1)(q-1)$, and $E, D : S \to S$ are functions defined by $E(x) = x^e \bmod n$ and $D(x) = x^d \bmod n$. The number e is known as the **encryption number** and d as the **decryption number**, the maps E and D are known as the **encryption map** and the **decryption map**. The pair (N, e) is called the **public key** of the system. RSA stands for three math guys, Ron Rivest, Adi Shamir and Leonard Adleman.

Theorem 15. *For any RSA cryptography system (S, N, e, d, E, D), the maps E and D are inverse each other, i.e., for all $x \in S$,*

$$D(E(x)) \equiv x \bmod N, \quad E(D(x)) \equiv x \bmod N.$$

The two numbers N, e are given in public.

Proof. Case 1: $x = 0$. It is trivial that $x^{ed} \equiv x \bmod N$.

Case 2: $\gcd(x, N) = 1$. Since $ed \equiv 1 \bmod (p-1)(q-1)$, then $ed = 1 + k(p-1)(q-1)$ for some $k \in \mathbb{Z}$. Thus

$$x^{ed} = x^{1+k(p-1)(q-1)} = x(x^{(p-1)(q-1)})^k$$

Since $x^{(p-1)(q-1)} \equiv 1 \bmod N$, we have

$$x^{ed} \equiv x \bmod N.$$

Case 3: $\gcd(x, N) \neq 1$. Since $N = pq$, we either have $x = ap$ for some $1 \leq a < q$ or $x = bq$ for some $1 \leq b < p$. In the formal case, we have

$$x^{ed} = (ap)^{1+k(p-1)(q-1)} = ((ap)^{q-1})^{k(p-1)}(ap).$$

Note that $q \nmid ap$, by Fermat's Little Theorem, $(ap)^{q-1} \equiv 1 \bmod q$. Thus $(ap)^{q-1} \equiv 1 \bmod q$. Hence $x^{ed} \equiv ap \equiv x \bmod q$. Note that $x^{ed} \equiv (ap)^{ed} \equiv 0 \equiv x \bmod p$. Therefore $p \mid (x^{ed} - x)$ and $q \mid (x^{ed} - x)$. Since $\gcd(p, q) = 1$, we have $pq \mid (x^{ed} - x)$, i.e., $x^{ed} \equiv x \bmod N$. □

Example 3. Let $p = 3$ and $q = 5$. Then $N = 3 \cdot 5 = 15$, $(p-1)(q-1) = 2 \cdot 4 = 8$. The encryption key e can be selected to be the numbers $1, 3, 5, 7$; Their corresponding decryption keys are also $1, 3, 5, 7$, respectively.

$(e, d) = (3, 11)$, $(5, 5)$, $(7, 7)$,(9,1),(11,3), $(13, 5)$, and $(15, 7)$ are encryption-decryption pairs. For instance, for $(e, d) = (11, 3)$, we have

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$E(x)$	1	8	12	4	5	6	13	2	9	10	11	3	7	14

In fact, in this special case the inverse of E is itself, i.e., $D = E^{-1} = E$.

Example 4. Let $p = 11$, $q = 13$. Then $N = pq = 143$, $(p-1)(q-1) = 120$. Then there are RSA systems with $(e, d) = (7, 103)$; $(e, d) = (11, 11)$; and $(e, d) = (13, 37)$. For the RSA system with $(e, d) = (13, 37)$, we have

$$E(2) = 2^{13} \equiv 41 \bmod 143$$

($2^2 = 4$, $2^4 = 16$, $2^8 = 16^2 \equiv 113$, $2^{13} = 2^8 \cdot 2^4 \cdot 2 \equiv 113 \cdot 16 \cdot 2 \equiv 41$); and

$$D(41) = 41^{37} \equiv 2 \bmod 143$$

($41^2 \equiv 108$, $41^4 \equiv 108^2 \equiv 81$, $41^8 \equiv 81^2 \equiv -17$, $41^{16} \equiv 17^2 \equiv 3$, $41^{32} \equiv 9$, $41^{37} = 41^{32} \cdot 41^4 \cdot 41 \equiv 2$). Note that $E(41) \equiv 41^8 \cdot 41^4 \cdot 41 \equiv 28$, we see that $E \neq D$.

Example 5. Let $p = 19$ and $q = 17$. Then $N = 19 \cdot 17 = 323$, $(p-1)(q-1) = 18 \cdot 16 = 288$. Given encryption number $e = 25$; find a decryption number d. ($d = 265$)

Given (N, e); we shall know the two prime numbers p, q in principle since $N = pq$. However, assuming that we cannot factor integers effectively, actually we don't know the numbers p, q. To break the system, the only possible way is to find the number $(p-1)(q-1)$, then use e to find d. Suppose $(p-1)(q-1) = pq - p - q + 1 = N - (p+q) + 1$ is known. Then $p+q$ is known. Thus p, q can be found by solving the quadratic equation $x^2 - (p+q)x + N = 0$. This is equivalent to factorizing the number N.

Example 6. Given $N = pq = 18779$ and $(p-1)(q-1) = 18480$. Then

$$p + q = N - (p-1)(q-1) + 1 = 300.$$

The equation $x^2 - 300x + 18779 = 0$ implies $p = 89, q = 211$.

Note that $(p-1)(q-1) = 88 \cdot 210 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. One can choose $e = 13, 17, 19, 23, 29$, etc. Say $e = 29$, then d can be found as follows: $18480 = 637 \cdot 29 + 7$, $29 = 4 \cdot 7 + 1$;

$$1 = 29 - 4 \cdot 7 = 29 - 4(18480 - 637 \cdot 29) = -4 \cdot 18480 + 2549 \cdot 29.$$

Thus $d = 2549$.