Discrete Mathematics for Computer Science

Lecture 8: Number Theory

Dr. Ming Tang

Department of Computer Science and Engineering
Southern University of Science and Technology (SUSTech)
Email: tangm3@sustech.edu.cn

SUSTech Southern University of Science and Technology

Arithmetic Modulo m

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties of ordinary addition and multiplication of integers:

Closure: If a and b belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.

Associativity: If a, b, and c belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.

Identity elements: $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Additive inverses: If $a \neq 0$ and $a \in \mathbf{Z}_m$, then $m - a$ is an additive inverse of a modulo m. That is, $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.

Commutativity: If $a, b \in \mathbf{Z}_m$, then $a +_m b = b +_m a$.

Distributivity: If $a, b, c \in \mathbf{Z}_m$, then

$$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$$

$$(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$$

Algorithm: Binary Modular Exponentiation

Compute b^n **mod** m: Let $n = (a_{k-1}...a_1a_0)_2$.

$$b^n = b^{a_{k-1}\cdot 2^{k-1}+\cdots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}} \cdots b^{a_1\cdot 2} \cdot b^{a_0}$$

Recall that

$$ab \textbf{ mod } m = ((a \textbf{ mod } m)(b \textbf{ mod } m))\textbf{mod } m.$$

Successively finds b **mod** m, b^2 **mod** m, b^4 **mod** m, . . . , $b^{2^{k-1}}$ **mod** m, and multiplies together the terms b^{2^j}, where $a_j = 1$.

procedure *modular exponentiation*(b: integer, $n = (a_{k-1}a_{k-2}...a_1a_0)_2$, m: positive integers)
$x := 1$
$power := b$ **mod** m
for $i := 0$ to $k - 1$
    if $a_i = 1$ **then** $x := (x \cdot power)$ **mod** m
    $power := (power \cdot power)$ **mod** m
return x {x equals b^n **mod** m }

Algorithm: Binary Modular Exponentiation

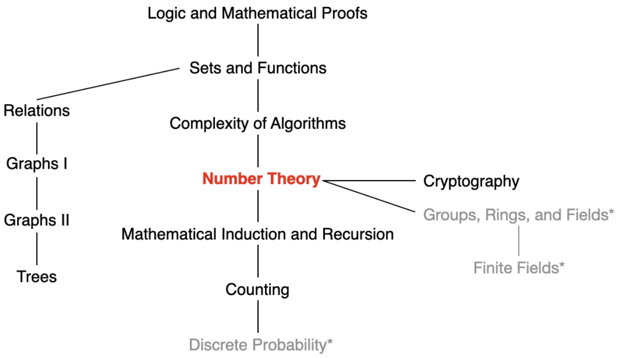
Use the algorithm to find 3^{644} mod 645:

procedure *modular exponentiation*(b: integer, $n = (a_{k-1}a_{k-2}\ldots a_1a_0)_2$, m: positive integers)
$x := 1$
$power := b$ **mod** m
for $i := 0$ to $k - 1$
  if $a_i = 1$ **then** $x := (x \cdot power)$ **mod** m
  $power := (power \cdot power)$ **mod** m
return x {x equals b^n **mod** m }

The algorithm initially sets $x = 1$ and $power = 3 \textbf{ mod } 645 = 3$. The binary expansion of 644 is $(1010000100)_2$. Here are the steps used:

$i = 0$: Because $a_0 = 0$, we have $x = 1$ and $power = 3^2 \textbf{ mod } 645 = 9 \textbf{ mod } 645 = 9$;
$i = 1$: Because $a_1 = 0$, we have $x = 1$ and $power = 9^2 \textbf{ mod } 645 = 81 \textbf{ mod } 645 = 81$;
$i = 2$: Because $a_2 = 1$, we have $x = 1 \cdot 81 \textbf{ mod } 645 = 81$ and $power = 81^2 \textbf{ mod } 645 = 6561 \textbf{ mod } 645 = 111$;
$i = 3$: Because $a_3 = 0$, we have $x = 81$ and $power = 111^2 \textbf{ mod } 645 = 12{,}321 \textbf{ mod } 645 = 66$;
$i = 4$: Because $a_4 = 0$, we have $x = 81$ and $power = 66^2 \textbf{ mod } 645 = 4356 \textbf{ mod } 645 = 486$;
$i = 5$: Because $a_5 = 0$, we have $x = 81$ and $power = 486^2 \textbf{ mod } 645 = 236{,}196 \textbf{ mod } 645 = 126$;
$i = 6$: Because $a_6 = 0$, we have $x = 81$ and $power = 126^2 \textbf{ mod } 645 = 15{,}876 \textbf{ mod } 645 = 396$;
$i = 7$: Because $a_7 = 1$, we find that $x = (81 \cdot 396) \textbf{ mod } 645 = 471$ and $power = 396^2 \textbf{ mod } 645 = 156{,}816 \textbf{ mod } 645 = 81$;
$i = 8$: Because $a_8 = 0$, we have $x = 471$ and $power = 81^2 \textbf{ mod } 645 = 6561 \textbf{ mod } 645 = 111$;
$i = 9$: Because $a_9 = 1$, we find that $x = (471 \cdot 111) \textbf{ mod } 645 = 36$.

This Lecture



Number Theory: divisibility and modular arithmetic, integer representations, primes and greatest common divisors, linear congruences, ...

Primes

A integer p that is greater than 1 is called a prime if the only positive factors of p are 1 and p.

- Note: factor is a number that divides another number, leaving no remainder.

A positive integer that is greater than 1 and is not prime is called composite.

Fundamental Theorem of Arithmetic: Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Primes and Composites

How to determine whether a number is a prime or a composite?

Approach 1: test if each number $x < n$ divides n.

Approach 2: test if each prime number $x < n$ divides n.

Approach 3: test if each prime number $x \leq \sqrt{n}$ divides n.

Primes and Composites

If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof: If n is composite, then it has a positive integer factor a such that $1 < a < n$ by definition. This means that $n = ab$, where b is an integer greater than 1.

Assume that $a > \sqrt{n}$ and $b > \sqrt{n}$. Then, $ab > n$, which leads to a contradiction. So either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Thus, n has a divisor less than $\sqrt{n}$.

By the Fundamental Theorem of Arithmetic, this divisor is either prime, or is a product of primes. In either case, n has a prime divisor less than $\sqrt{n}$.

Primes

There are infinitely many primes.

Proof: We will prove this theorem using a proof by contradiction.We assume that there are only finitely many primes, p_1, p_2, . . . , p_n. Let

$$Q = p_1 p_2 \ldots p_n + 1.$$

By the fundamental theorem of arithmetic, Q is prime or else it can be written as the product of two or more primes.

However, none of the primes p_j divides Q, for if $p_j | Q$, then p_j divides $Q - p_1 p_2 \ldots p_n = 1$.

- Note: Let a, b, c be integers. If $a|b$ and $a|c$, then $a|(b + c)$.

Hence, there is a prime not in the list $p_1, p_2, \ldots, p_n$. This prime is either Q, if it is prime, or a prime factor of Q.

This is a contradiction because we assumed that we have listed all the primes. Consequently, there are infinitely many primes.

Greatest Common Divisor (GCD)

Let a and b be integers, not both 0. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, denoted by $\gcd(a, b)$.

Example: What is the greatest common divisor of 24 and 36?
$\gcd(24, 36) = 12$.

Integers a and b are relatively prime if their greatest common divisor is 1.

Example: Are integers 17 and 22 relatively prime? Yes, because $\gcd(17, 22) = 1$.

Greatest Common Divisor (GCD)

A systematic way to find the $\gcd$ is factorization.

Let $a = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} ... p_n^{b_n}$. Then,

$$\gcd(a, b) = p^{\min(a_1, b_1)} p^{\min(a_2, b_2)} ... p^{\min(a_n, b_n)}$$

Least Common Multiple (LCM)

Let a and b be positive integers. The least common multiple of a and b is the smallest positive integer that is divisible by both a and b, denoted by $\mathrm{lcm}(a, b)$.

We can also use factorization to find the lcm.

Let $a = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} ... p_n^{b_n}$. Then,

$$\mathrm{lcm}(a, b) = p^{\max(a_1, b_1)} p^{\max(a_2, b_2)} ... p^{\max(a_n, b_n)}.$$

Euclidean Algorithm

Computing the greatest common divisor of two integers directly from the prime factorizations can be time consuming since we need to find all factors of the two integers.

Luckily, we have an efficient algorithm, called **Euclidean algorithm**. This algorithm has been known since ancient times and named after the ancient Greek mathmaticain Euclid.

Euclidean Algorithm

For two integers 287 and 91, we want to find $\gcd(287, 91)$.

Step 1: $287 = 91 \cdot 3 + 14$

Step 2: $91 = 14 \cdot 6 + 7$

Step 3: $14 = 7 \cdot 2 + 0$

$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$

The Euclidean Algorithm in Pseudocode

ALGORITHM 1 The Euclidean Algorithm.

```
procedure gcd(a, b: positive integers)
x := a
y := b
while y ≠ 0
    r := x mod y
    x := y
    y := r
return x{gcd(a, b) is x}
```

Step 1: $287 = 91 \cdot 3 + 14$

Step 2: $91 = 14 \cdot 6 + 7$

Step 3: $14 = 7 \cdot 2 + 0$

The number of divisions required to find $\gcd(a, b)$ is $O(\log b)$, where $a \geq b$.

(This will be proven in later sections. Mathematical induction.)

Validity of Euclidean Algorithm

Lemma: Let $a = bq + r$, where a, b, q and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Proof: We will show that the common divisors of a and b are the same as the common divisors of b and r, which leads to $\gcd(a, b) = \gcd(b, r)$.

- So suppose that d divides both a and b. Then it follows that d also divides $a - bq = r$. Hence, any common divisor of a and b is also a common divisor of b and r.
- Suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of b and r is also a common divisor of a and b.

Since they have the same set of common divisors, they have the same greatest common divisor, i.e., $\gcd(a, b) = \gcd(b, r)$.

Validity of Euclidean Algorithm

Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$.

$$
\begin{array}{lll}
r_0 & = r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\
r_1 & = r_2 q_2 + r_3 & 0 \leq r_3 < r_2, \\
 & \cdot & \\
 & \cdot & \\
 & \cdot & \\
r_{n-2} & = r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\
r_{n-1} & = r_n q_n \,. &
\end{array}
$$

$$\gcd(a, b) = \gcd(r_0, r_1) = \ldots = \gcd(r_{n-1}, r_n) = gcd(r_n, 0) = r_n$$

- Note: $r_n | r_n$ and $r_n | 0$

GCD as Linear Combinations

$\gcd(a, b)$ can be expressed as a linear combination with integer coefficients of a and b.

Example: $\gcd(6, 14) = 2$, and $2 = (-2) \cdot 6 + 1 \cdot 14$.

Bezout's Theorem: If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

This equation is called Bezout's identity.

GCD as Linear Combinations

We can use extended Euclidean algorithm to find Bezout's identity.

Example: Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

Solution: To show that $\gcd(252, 198) = 18$, the Euclidean algorithm uses these divisions:

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18. \end{aligned}$$

Substituting the above expressions:

$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$$

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198.$$

Corollaries of Bezout's Theorem

Lemma: If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Proof: Since $\gcd(a, b) = 1$, by Bezout's Theorem there exist s and t such that $1 = sa + tb$. This yields $c = sac + tbc$.

Since $a|bc$, we have $a|tbc$. Then, since $a|sac$, we have $a|(sac + tbc)$, i.e., $a|c$.

Lemma: If p is prime and $p|a_1 a_2 ... a_n$, then $p|a_i$ for some i.

(This will be proven in later sections. Mathematical induction.)

SUSTech Southern University of Science and Technology

Uniqueness of Prime Factorization

Theorem: A prime factorization of a positive integer, where the primes are in nondecreasing order, is unique.

Proof (by contradiction): Suppose that the positive integer n can be written as a product of primes in two distinct ways:

$$n = p_1 p_2 ... p_s \text{ and } n = q_1 q_2 ... q_t$$

Remove all common primes from the factorizations to get

$$p_{i_1} p_{i_2} ... p_{i_u} = q_{j_1} q_{j_2} ... q_{j_v}$$

Thus, $p_{i_1} | q_{j_1} q_{j_2} ... q_{j_v}$. It then follows that p_{i_1} divides q_{j_k} for some k, contradicting the assumption that p_{i_1} and q_{j_k} are distinct primes.

Dividing Congruences by an Integer

Theorem: Let m be a positive integer. Let a, b, c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Example:

- $14 \equiv 8 \pmod{6}$, but $7 \not\equiv 4 \pmod{6}$
- $14 \equiv 8 \pmod{3}$, and $7 \equiv 4 \pmod{3}$

Proof: Since $ac \equiv bc \pmod{m}$, we have $m \mid ac - bc$, i.e., $m \mid c(a - b)$. Because $\gcd(c, m) = 1$, it follows that $m \mid a - b$.

Mersenne Primes

Prime numbers of the form $2^p - 1$, where p is a prime.

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$, $2^7 - 1 = 127$ are Mersenne primes.
- $2^{11} - 1 = 2047 = 23 \cdot 89$ is not a Mersenne prime.
- The largest known prime numbers are Mersenne primes.

Largest Known Prime, 49th Known Mersenne Prime Found!

January 7, 2016 — GIMPS celebrated its 20th anniversary with the discovery of the largest known prime number, $2^{74,207,281}$-1.

50th Known Mersenne Prime Found!

January 3, 2018 — Persistence pays off. Jonathan Pace, a GIMPS volunteer for over 14 years, discovered the 50th known Mersenne prime, $2^{77,232,917}$-1 on December 26, 2017. The prime number is calculated by multiplying together 77,232,917 twos, and then subtracting one. It weighs in at 23,249,425 digits, becoming the largest prime number known to mankind. It bests the previous record prime, also discovered by GIMPS, by 910,807 digits.

51st Known Mersenne Prime Found!

December 21, 2018 — The Great Internet Mersenne Prime Search (GIMPS) has discovered the largest known prime number, $\mathbf{2^{82,589,933}}$**-1**, having 24,862,048 digits. A computer volunteered by Patrick Laroche from Ocala, Florida made the find on December 7, 2018. The new prime number, also known as M82589933, is calculated by multiplying together 82,589,933 twos and then subtracting one. It is more than one and a half million digits larger than the previous record prime number.

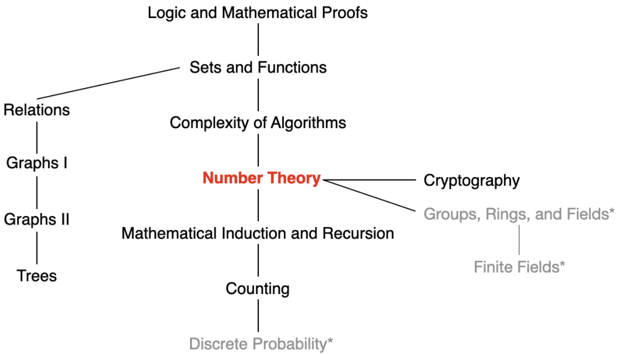
SUSTech Southern University of Science and Technology

Conjectures about Primes

Goldbach's Conjecture $(1+1)$: Every even integer $n > 2$, is the sum of two primes.

Twin-prime Conjecture: There are infinitely many twin primes (i.e., pairs of primes that differ by 2).

This Lecture



Number Theory: divisibility and modular arithmetic, integer representations, primes, greatest common divisors, linear congruences

Linear Congruences

A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

Systems of linear congruences have been studied since ancient times.

今有物不知其数 三三数之剩二 五五数之剩三 七七数之剩二 问物几何

About 1500 years ago, the Chinese mathematician Sun-Tsu asked: "There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?"

Modular Inverse

An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an inverse of a modulo m.

One method of solving linear congruences makes use of an inverse a modulo m (if it exists):

From $ax \equiv b \pmod{m}$, it follows that $\bar{a}ax \equiv \bar{a}b \pmod{m}$.

Note that $\bar{a}ax \textbf{ mod } m = ((\bar{a}a \textbf{ mod } m)(x \textbf{ mod } m)) \textbf{ mod } m = x \textbf{ mod } m$.

Thus, $x \textbf{ mod } m = \bar{a}ax \textbf{ mod } m = \bar{a}b \textbf{ mod } m$, which implies that

$$x \equiv \bar{a}b \pmod{m}.$$

When does an inverse of a modulo m exist?

Inverse of a modulo m

Theorem: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. The inverse is unique modulo m. That is,

- there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and
- every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.)

Proof: Since $\gcd(a, m) = 1$, there are integers s and t such that

$$sa + tm = 1.$$

Hence $sa + tm \equiv 1 \pmod{m}$. Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$. This means that s is an inverse of a modulo m.

How to prove the uniqueness of the inverse?

Suppose that b and c are both inverses of a modulo m. Then $ba \equiv 1 \pmod{m}$ and $ca \equiv 1 \pmod{m}$. Hence, $ba \equiv ca \pmod{m}$. Because $\gcd(a, m) = 1$ it follows that $b \equiv c \pmod{m}$.

How to find inverses?

Using extended Euclidean algorithm:

Example: Find an inverse of 101 modulo 4620. That is, find $\bar{a}$ such that $\bar{a} \cdot 101 \equiv 1 \pmod{4620}$.

$$\begin{aligned}
4620 &= 45\cdot 101 + 75 \\
101 &= 1\cdot 75 + 26 \\
75 &= 2\cdot 26 + 23 \\
26 &= 1\cdot 23 + 3 \\
23 &= 7\cdot 3 + 2 \\
3 &= 1\cdot 2 + 1 \\
2 &= 2\cdot 1
\end{aligned}$$

$$\begin{aligned}
1 &= 3 - 1\cdot 2 \\
1 &= 3 - 1\cdot(23 - 7\cdot 3) = -1\cdot 23 + 8\cdot 3 \\
1 &= -1\cdot 23 + 8\cdot(26 - 1\cdot 23) = 8\cdot 26 - 9\cdot 23 \\
1 &= 8\cdot 26 - 9\cdot(75 - 2\cdot 26) = 26\cdot 26 - 9\cdot 75 \\
1 &= 26\cdot(101 - 1\cdot 75) - 9\cdot 75 \\
&= 26\cdot 101 - 35\cdot 75 \\
1 &= 26\cdot 101 - 35\cdot(4620 - 45\cdot 101) \\
&= -35\cdot 4620 + 1601\cdot 101
\end{aligned}$$

That $-35 \cdot 4620 + 1601 \cdot 101 = 1$ tells us that -35 and 1601 are Bezout coefficients of 4620 and 101. We have

$$1 \textbf{ mod } 4620 = 1601 \cdot 101 \textbf{ mod } 4620.$$

Thus, 1601 is an inverse of 101 modulo 4620.

Using Inverses to Solve Congruences

Solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

Recall: From $ax \equiv b \pmod{m}$, it follows that $\bar{a}ax \equiv \bar{a}b \pmod{m}$.

Note that $\bar{a}ax \textbf{ mod } m = ((\bar{a}a \textbf{ mod } m)(x \textbf{ mod } m)) \textbf{ mod } m = x \textbf{ mod } m$.

Thus, $x \textbf{ mod } m = \bar{a}ax \textbf{ mod } m = \bar{a}b \textbf{ mod } m$, which implies that

$$x \equiv \bar{a}b \pmod{m}.$$

Example: What are the solutions of the congruence $3x \equiv 4 \pmod{7}$?

Solution: We found that -2 is an inverse of 3 modulo 7. Multiply both sides of the congruence by -2. Since $-8 \equiv 6 \pmod{7}$, we have $x \equiv 6 \pmod{7}$, namely, 6, 13, 20, . . . and -1, -8, ...

Number of Solutions to Congruences

The previous approach (based on the inverse of a modulo m) works for only the scenario with $\gcd(a, m) = 1$.

Theorem*: Let $\gcd(a, m) = d$. Let $m' = m/d$ and $a' = a/d$. The congruence $ax \equiv b \pmod{m}$ has solutions if and only if $d \mid b$.

- If $d \mid b$, then there are exactly d solutions, where by "solution" we mean a congruence class mod m
- If x_0 is a solution, then the other solutions are given by $x_0 + m', x_0 + 2m', ..., x_0 + (d-1)m'$.

Proof:

"only if": Let x_0 be a solution, then $ax_0 - b = km$. Thus, $ax_0 - km = b$. Since $d \mid ax_0 - km$, we must have $d \mid b$.

"if": Suppose that $d \mid b$. Let $b = kd$. Since $\gcd(a, m) = d$, there exist integers s and t such that $d = as + mt$. Multiplying both sides by k. Then, $b = ask + mtk$. Let $x_0 = sk$. Then $ax_0 \equiv b \pmod{m}$.

Number of Solutions to Congruences

Theorem*: Let $\gcd(a, m) = d$. Let $m' = m/d$ and $a' = a/d$. The congruence $ax \equiv b \pmod{m}$ has solutions if and only if $d \mid b$.

- If $d \mid b$, then there are exactly d "solutions", where by "solution" we mean a congruence class mod m.
- If x_0 is a solution, then the other solutions are given by $x_0 + m', x_0 + 2m', ..., x_0 + (d-1)m'$.

Proof:

"The number of solutions is d": Consider two solutions x_0 and x_1. $ax_0 \equiv b \pmod{m}$ and $ax_1 \equiv b \pmod{m}$ imply that $m \mid a(x_1 - x_0)$ and $m' \mid a'(x_1 - x_0)$. This implies further that $x_1 = x_0 + km'$.

To finish the proof, observe that as k runs through the values $0, 1, ..., d-1$ (the residues mod d), the congruence classes $[x_0 + (m/d)k]_m$ run through all the solutions.

The Chinese Remainder Theorem

Systems of linear congruences have been studied since ancient times.

今有物不知其数 三三数之剩二 五五数之剩三 七七数之剩二 问物几何

About 1500 years ago, the Chinese mathematician Sun-Tsu asked: "There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?"

- $x \equiv 2 \pmod{3}$
- $x \equiv 3 \pmod{5}$
- $x \equiv 2 \pmod{7}$

The Chinese Remainder Theorem

Theorem (The Chinese Remainder Theorem): Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than 1 and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then, the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\ldots$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$.
(That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

The Chinese Remainder Theorem

Proof: To show such a solution exists: Let $M_k = m/m_k$ for $k = 1, 2, ..., n$ and $m = m_1 m_2 ... m_n$. Thus, $M_k = m_1 ... m_{k-1} m_{k+1} ... m_n$.

Since $\gcd(m_k, M_k) = 1$, there is an integer y_k, an inverse of M_k modulo m_k, such that $M_k y_k \equiv 1 \pmod{m_k}$. Let

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n.$$

It is checked that x is a solution to the n congruences:

$$x \textbf{ mod } m_k = (a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n) \textbf{ mod } m_k$$

Since $M_k = m/m_k$, we have $x \textbf{ mod } m_k = a_k M_k y_k \textbf{ mod } m_k$. Since $M_k y_k \equiv 1 \pmod{m_k}$, we have $a_k M_k y_k \textbf{ mod } m_k = a_k \textbf{ mod } m_k$. Thus,

$$x \equiv a_k \pmod{m_k}.$$

SUSTech Southern University of Science and Technology

The Chinese Remainder Theorem

How to prove the uniqueness of the solution modulo m?

Proof: Suppose that x and x' are both solutions to all the congruences. As x and x' give the same remainder, when divided by m_k, their difference $x - x'$ is a multiple of each m_k for all $k = 1, 2, ..., n$.

As m_1, m_2, . . . , m_n be pairwise relatively prime positive integers, their product m divides $x - x'$, and thus x and x' are congruent modulo m, i.e., $x \equiv x'$ $(\mathbf{mod}\ m)$.

This implies that given a solution x with $0 \leq x < m$, all other solutions are congruent modulo m to this solution.

The Chinese Remainder Theorem: Example

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

1. Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, and $M_3 = m/7 = 15$.
2. Compute the inverse of M_k modulo m_k:
   - $35 \cdot 2 \equiv 1 \pmod{3}$ $y_1 = 2$
   - $21 \equiv 1 \pmod{5}$ $y_2 = 1$
   - $15 \equiv 1 \pmod{7}$ $y_3 = 1$
3. Compute a solution x:
   $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23 \pmod{105}$
4. The solutions are all integers x that satisfy $x \equiv 23 \pmod{105}$.

Back Substitution

We may also solve systems of linear congruences with pairwise relatively prime moduli $m_1, m_2, \ldots m_n$ by back substitution.

Example:

(1) $x \equiv 1 \pmod{5}$
(2) $x \equiv 2 \pmod{6}$
(3) $x \equiv 3 \pmod{7}$

According to (1), $x = 5t + 1$, where t is an integer.

Substituting this expression into (2), we have $5t + 1 \equiv 2 \pmod{6}$, which means that $t \equiv 5 \pmod{6}$. Thus, $t = 6u + 5$, where u is an integer.

Substituting $x = 5t + 1$ and $t = 6u + 5$ into (3), we have $30u + 26 \equiv 3 \pmod{7}$, which implies that $u \equiv 6 \pmod{7}$. Thus, $u = 7v + 6$, where v is an integer.

Thus, we must have $x = 210v + 206$. Translating this back into a congruence,

$$x \equiv 206 \pmod{210}.$$

The Chinese Remainder Theorem

What if $m_1, m_2, \ldots, m_n$ are positive integers greater than 1, but they are not pairwise relatively prime?

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$\ldots$
$x \equiv a_n \pmod{m_n}$

Translate these congruence into a set of congruence that together are equivalent to the given congruence:

For $x \equiv a_k \pmod{m_k}$, suppose m_k can be written as $m_k = b_k^1 b_k^2 \cdot b_k^r$, where b_k^1, b_k^2, ..., b_k^r are all primes. Then, $x \equiv a_k \pmod{m_k}$ is equivalent to the following set of congruence:

$x \equiv a_k \pmod{b_k^1}$
$x \equiv a_k \pmod{b_k^2}$
$\ldots$
$x \equiv a_k \pmod{b_k^r}$

SUSTech Southern University of Science and Technology

Modular Arithmetic in CS

Modular arithmetic and congruencies are used in CS:

- Pseudorandom number generators
- Hash functions
- Cryptography

Next Lecture