Number Theory

-R. Y. Sarode

Divisibility and Modular Arithmetic

Division

- **Definition**: If a and b are integers with $a \neq 0$, then *a divides b* if there exists an integer c such that $b = ac$.
  - When a divides b we say that a is a *factor* or *divisor* of b and that b is a *multiple* of a.
  - The notation $a \mid b$ denotes that a divides b.
  - If $a \mid b$, then b/a is an integer.
  - If a does not divide b, we write $a \nmid b$.

Example: Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Properties of Divisibility

- **Theorem 1**: Let a, b, and c be integers, where $a \neq 0$.

  i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

  ii. If $a \mid b$, then $a \mid bm$ for all integers m;

  iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: *(i)* Suppose $a \mid b$ and $a \mid c$, then it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$$b + c = as + at = a(s + t).$$ Hence, $a \mid (b + c)$

Corollary: If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Division Algorithm

- When an integer is divided by a positive integer, there is a quotient and a remainder.
- **Division Algorithm**: If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$
  - d is called the *divisor*.
  - a is called the *dividend*.
  - q is called the *quotient*.
  - r is called the *remainder*.

div and **mod**

1) $q = a$ **div** d
2) $r = a$ **mod** d

Examples:

- What are the quotient and remainder when 101 is divided by 11?

Solution: The quotient when 101 is divided by 11 is 9 = 101 **div** 11, and the remainder is 2 = 101 **mod** 11.

- What are the quotient and remainder when −11 is divided by 3?

Solution: we have , $-11 = 3(-4) + 1$.

The quotient when −11 is divided by 3 is −4 = −11 **div** 3, and the remainder is 1 = −11 **mod** 3.

Congruence Relation

- **Definition**: If a and b are integers and m is a positive integer, then *a is congruent to b modulo m* if m divides $a - b$.
  - The notation $a \equiv b \pmod{m}$ says that a is congruent to b modulo m.
  - We say that $a \equiv b \pmod{m}$ is a *congruence* and that m is its *modulus*.
  - Two integers are congruent mod m if and only if they have the same remainder when divided by m.
  - If a is not congruent to b modulo m, we write

$$a \not\equiv b \pmod{m}$$

Example: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution:

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$.
- $24 \not\equiv 14 \pmod{6}$ since 6 divides $24 - 14 = 10$ is not divisible by 6.

More on Congruence

- **Theorem** : Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.
- **Proof**:
  - If $a \equiv b \pmod{m}$, then (by the definition of congruence) $m \mid a - b$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
  - Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m \mid a - b$ and $a \equiv b \pmod{m}$.

The Relationship between (mod m) and **mod** m Notations

- The use of "mod" in $a \equiv b \pmod{m}$ is different from its use in $a \bmod m = b$.
  - $a \equiv b \pmod{m}$ is a relation on the set of integers.
  - In $a \bmod m = b$, the notation **mod** denotes a function.

- **Theorem** :

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Congruences of Sums and Products

- **Theorem** : Let m be a positive integer. If $a \equiv b \pmod{m}$ and

  $c \equiv d \pmod{m}$, then

  $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

- **Proof**:
  - Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by last Theorem there are integers s and t with $b = a + sm$ and $d = c + tm$.
  - Therefore,
    - $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
    - $b\,d = (a + sm)\,(c + tm) = ac + m(at + cs + stm)$.
  - Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Example: Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem that

$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$

$77 = 7 \times 11 \equiv 2 \times 1 = 2 \pmod{5}$

Arithmetic Modulo m

- operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication.
  - *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 $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
  - *Commutativity*: If a and b belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
  - *Identity elements*: The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively.
    - If a belongs to $\mathbf{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Arithmetic Modulo *m*

- *Additive inverses*: If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $m - a$ is the additive inverse of a modulo m, and 0 is its own additive inverse.
  - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$
- *Distributivity*: If a, b, and c belong to $\mathbf{Z}_m$, then
  - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and
  - $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

- **Multiplicative inverses** have not been included since they **do not always exist.** multiplicative inverse of a real number x is a real number y such that xy = 1.
- For example, there is no multiplicative inverse of 2 modulo 6.
- Use the definition of addition and multiplication in Z_m ***to find*** $7 +_{11} 9$ ***and*** $7 \cdot_{11} 9$

Solution: Using the definition of addition modulo 11, we find that

- $7 +_{11} 9$ = *(7 + 9)* ***mod 11 = 16 mod 11 = 5,*** and
- $7 \cdot_{11} 9$ = *(7 · 9)* ***mod 11 = 63 mod 11 = 8.***
- Hence $7 +_{11} 9 = 5$ and $7 \cdot_{11} 9 = 8$.

Primes

Definition: A positive integer *p* greater than 1 is called *prime* if the only positive factors of *p* are 1 and *p*. A positive integer that is greater than 1 and is not prime is called *composite*.

Example: The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

Relative Prime Numbers: Two numbers are relatively prime, If GCD of two numbers is 1

The Fundamental Theorem of Arithmetic

Theorem: Every positive 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.

Examples:

- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- $641 = 641$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Greatest Common Divisor

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

One can find greatest common divisors of small numbers by inspection.

Example:What is the greatest common divisor of 24 and 36? **Solution**: gcd(24,36) = 12

Example:What is the greatest common divisor of 17 and 22? **Solution**: gcd(17,22) = 1

Greatest Common Divisor

Definition: The integers a and b are *relatively prime* if their greatest common divisor is 1.
Example: 17 and 22

Definition: The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
Example: Determine whether the integers 10, 17 and 21 are pairwise relatively prime.
Solution: Because $\gcd(10,17) = 1$, $\gcd(10,21) = 1$, and $\gcd(17,21) = 1$, 10, 17, and 21 are pairwise relatively prime.

Example: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.
Solution: Because $\gcd(10,24) = 2$.
10, 19, and 24 are not pairwise relatively prime.

Finding the Greatest Common Divisor Using Prime Factorizations

- Suppose the prime factorizations of a and b are:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \; b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)},$$

- This formula is valid since the integer on the right (of the equals sign) divides both a and b. No larger integer can divide both a and b.

Example: $120 = 2^3 \cdot 3 \cdot 5$ $500 = 2^2 \cdot 5^3$

$\gcd(120,500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$

- Finding the gcd of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Least Common Multiple

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

- The least common multiple can also be computed from the prime factorizations.

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

This number is divided by both a and b and no smaller number is divided by a and b.

Example: $\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)}\ 3^{\max(5,3)}\ 7^{\max(2,0)} = 2^4\ 3^5\ 7^2$

- The greatest common divisor and the least common multiple of two integers are related by:

Theorem 5: Let a and b be positive integers. Then

$$ab = \gcd(a,b) \cdot \text{lcm}(a,b)$$

Euclidean Algorithm

- The Euclidean algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that, if $a > b$ and r is the remainder when a is divided by b, then $\gcd(a,b)$ is equal to $\gcd(b,r)$.

  Example: Find $\gcd(91, 287)$:

  - $287 = 91 \cdot 3 + 14$ Divide 287 by 91
  - $91 = 14 \cdot 6 + 7$ Divide 91 by 14
  - $14 = 7 \cdot 2 + 0$ Divide 14 by 7

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

Stopping condition

Euclidean Algorithm

- The Euclidean algorithm expressed in pseudocode is:

```
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}
```

Correctness of Euclidean Algorithm

Lemma 1: Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a,b) = \gcd(b,r)$.

Proof:

- Suppose that d divides both a & b.Then d also divides $a - bq = r$. Hence, any common divisor of a and b must also be any common divisor of b and r.
- Suppose that d divides both b & r. Then d also divides $bq + r = a$. Hence, any common divisor of a and b must also be a common divisor of b and r.
- Therefore, $\gcd(a,b) = \gcd(b,r)$.

Solve using Euclidean Algorithm

- gcd(2322, 654)
- Let a = 2322, b = 654.
- 2322 = 654·3 + 360 — gcd(2322, 654) = gcd(654, 360)
- 654 = 360·1 + 294 — gcd(654, 360) = gcd(360, 294)
- 360 = 294·1 + 66 — gcd(360, 294) = gcd(294, 66)
- 294 = 66·4 + 30 — gcd(294, 66) = gcd(66, 30)
- 66 = 30·2 + 6 — gcd(66, 30) = gcd(30, 6)
- 30 = 6·5 — gcd(30, 6) = 6

- Therefore, gcd(2322,654) = 6.

gcds as Linear Combinations

Bézout's Theorem: If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$.

Definition: If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa + tb$ are called *Bézout coefficients* of a and b. The equation $\gcd(a,b) = sa + tb$ is called *Bézout's identity*.

- By Bézout's Theorem, the gcd of integers a and b can be expressed in the form $sa + tb$ where s and t are integers. This is a *linear combination* with integer coefficients of a and b.
  - $\gcd(6,14) = (-2)\cdot 6 + 1\cdot 14$
  - It first uses the Euclidean algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers.

Finding gcds as Linear Combinations

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

Solution: First use the Euclidean algorithm to show gcd(252,198) = 18

- $252 = 1 \cdot 198 + 54$ $(54 = 252 - 1 \cdot 198)$ --------(1)
- $198 = 3 \cdot 54 + 36$ $(36 = 198 - 3 \cdot 54)$ --------(2)
- $54 = 1 \cdot 36 + 18$ $(18 = 54 - 1 \cdot 36)$ --------(3)
- $36 = 2 \cdot 18$

- Now working backwards,
  - $18 = 54 - 1 \cdot 36$ (From 3)
  - $18 = 54 - 1 \cdot (198 - 3 \cdot 54)$ (Replacing 36 using (2))
  - $18 = 4 \cdot 54 - 1 \cdot 198$ (Simplifying)
  - $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$
    (Replacing 54 using (1))

Finding gcds as Linear Combinations

Example: Express gcd(102,38) as a linear combination of 102 and 38.

Solution: First use the Euclidean algorithm find gcd.

102=2*38+26

38=1*26+12

26=2*12+2

12=6*2+0, So gcd(102, 38) = 2

Work backwards to find the *Bézout coefficients*

2=26-2*12

=26-2*(38-1*26)

=3*26-2*38

=3*(102-2*38)-2*38

=

So, the *Bézout coefficients* are 3 and -8

Find gcd(93, 219) using bezout coefficient:

```
219 = 93 x 2 + 33        33=219-93*2
 93 = 33 x 2 + 27         27=93- 33*2
 33 = 27 x 1 + 6          6=33-27*1
 27 = 6 x 4 + 3           3=27-6*4
  6 = 3 x 2 + 0
```

Gcd(93, 219) = 3.

```
3 = 27 - 4 x 6
  = 27 - 4 x (33 - 27 x 1)
  = -4 x 33 + 5 x 27
  = -4 x 33 + 5 x (93 - 2 x 33)
  = 5 x 93 - 14 x 33
  = 5 x 93 - 14 x (219 - 2 x 93)
  = -14 x 219 + 33 x 93
```

Therefore a solution to gcd(93, 219) = 219x + 93y is x = -14 and y = 33.

Multiplicative Inverse

- Multiplicative inverse can be calculated for the numbers which are relatively prime.

$$x \bmod n$$

Then multiplicative inverse y can be as follows:

$$x \times y \bmod n = 1$$

By using brute force method or by trial and error method we can get the value of y

Ex. for $3 \bmod 20$

$3 \times y \bmod n = 1$ we can try for numbers like 2,3,4,5,6,7

$\therefore y = 7$

But this is not an efficient method.

Multiplicative Inverse

- Find an inverse of 3 modulo 7 by first finding Bézout coefficients of 3 and 7.
- *Solution: Because gcd(3, 7) = 1,*

  ∴ inverse of 3 modulo 7 exists. by Euclidean algorithm $7 = 2 \cdot 3 + 1$.
  - From this equation we see that $-2 \cdot 3 + 1 \cdot 7 = 1$.
  - This shows that −2 and 1 are Bézout coefficients of 3 and 7.We see that −2 is an inverse of 3 modulo 7.
  - Note that every integer congruent to −2 modulo 7 is also an inverse of 3, such as 5, −9, 12, and so on.
  - **As we know we can't have negative value as mod value.**

Find an inverse of 101 modulo 4620.

- *Solution:* First, we use the Euclidean algorithm to show that gcd*(101, 4620) = 1.*
  - *Then* we will reverse the steps to find Bézout coefficients *a and b such that 101a + 4620b = 1. It will* then follow that *a is an inverse of 101 modulo 4620. The steps used by the Euclidean algorithm* to find gcd*(101, 4620) are*

$4620 = 45 \cdot 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$3 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1.$

- Because the last nonzero remainder is 1, we know that gcd*(101, 4620) = 1. We can now find* the Bézout coefficients for 101 and 4620 by working backwards through these steps, expressing gcd*(101, 4620) = 1*

We obtain $1 = 3 - 1 \cdot 2$

$= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$

$= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$

$= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26$

$= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75$

$= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) = -35 \cdot 4620 + 1601 \cdot 101.$

That $-35 \cdot 4620 + 1601 \cdot 101 = 1$ tells us that −35 and 1601 are Bézout coefficients of 4620 and 101,

and 1601 is an inverse of 101 modulo 4620.

- Here we are calculating multiplicative inverse for 101.

What are the solutions of the linear congruence $3x \equiv 4 \pmod 7$?

- we know that −2 is an inverse of 3 modulo 7.
  - Calculate Multiplicative inverse of 3 mod 7, which is -2 or 5
  - Multiplying both sides of the congruence by −2 shows that
  - $-2 \cdot 3x \equiv -2 \cdot 4 \pmod 7$.

    $x = -8 \pmod 7$

    $x = -1 \pmod 7$

    $x = 6 \pmod 7$

    $x = 6$
  - We need to determine whether every x with $x \equiv 6 \pmod 7$ is a solution.
  - $x \equiv 6 \pmod 7$ Then,
  - it follows that $3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod 7$,

    $18 \equiv 4 \pmod 7$
  - which shows that all such x satisfy the congruence. We conclude that the solutions to the congruence are the integers x such that $x \equiv 6 \pmod 7$, namely, 6, 13, 20, . . . and −1, −8, −15, . . .

Base conversions

- Find the octal expansion of (12345)10.
- Solution: First, divide 12345 by 8 to obtain

$12345 = 8 \cdot 1543 + 1.$

Successively dividing quotients by 8 gives

$1543 = 8 \cdot 192 + 7,$

$192 = 8 \cdot 24 + 0,$

$24 = 8 \cdot 3 + 0,$

$3 = 8 \cdot 0 + 3.$

The successive remainders that we have found, 1, 7, 0, 0, and 3, are the digits from the right to the left of 12345 in base 8. Hence, (12345)10 = (30071)8.

- Find the hexadecimal expansion of (177130)10.
  Solution: First divide 177130 by 16 to obtain $177130 = 16 \cdot 11070 + 10$.

  Successively dividing quotients by 16 gives

$11070 = 16 \cdot 691 + 14$,

$691 = 16 \cdot 43 + 3$,

$43 = 16 \cdot 2 + 11$,

$2 = 16 \cdot 0 + 2$.

The successive remainders that we have found, 10, 14, 3, 11, 2, give us the digits from the right to the left of 177130 in the hexadecimal (base 16) expansion of (177130)10. It follows that (177130)10 = (2B3EA)16.

CHINESE REMAINDER THEOREM

The Chinese remainder theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime, as shown below:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv a_k \pmod{m_k}$$

THE CHINESE REMAINDER THEOREM Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

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

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

Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.
3. Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli (m_1, m_2, …, m_k). Call the inverses M_1^{-1}, M_2^{-1}, …, M_k^{-1}.
4. The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M$$

CHINESE REMAINDER THEOREM

- *Theorem: Let $m_1, m_2, \ldots, m_r$ be positive integers such that m_i and m_j are relatively prime for $i = j$. Let $m = m_1 m_2 \cdots m_r$ and let $u_1, u_2, \ldots, u_r$ be integers. Then there exists exactly one integer u with $0 \leq u < m$ and $u \equiv u_i \bmod m_i$ for all $1 \leq i \leq r$.*
- *To construct a simultaneous solution, first let $M_k = m/m_k$ for $k = 1, 2, \ldots, n$.*
- *That is, M_k is the product of the moduli.*
- *Because m_i and m_k have no common factors greater than 1 when $i = k$, it follows that $\gcd(m_k, M_k) = 1$.*
- *Consequently, we know that there is an integer y_k, an inverse of M_k modulo m_k, such that $M_k y_k \equiv 1 \pmod{m_k}$.*

CHINESE REMAINDER THEOREM

To construct a simultaneous solution, form the sum
$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$.

First, note that because $M_j \equiv 0 \pmod{m_k}$ *whenever* $j = k$, *all terms except the kth term in this sum are congruent to 0 modulo* m_k .

Because $M_k y_k \equiv 1 \pmod{m_k}$ *we see that*
$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, *for* $k = 1, 2, \ldots, n$. *We have shown that x is a simultaneous solution to the n congruences.*

Example

The following is an example of a set of equations with different moduli:

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

The solution to this set of equations is given in the next section; for the moment, note that the answer to this set of equations is x = 23. This value satisfies all equations: $23 \equiv 2 \pmod 3$, $23 \equiv 3 \pmod 5$, and $23 \equiv 2 \pmod 7$.

Example

Find the solution to the simultaneous equations:

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

Solution

We follow the four steps.

1. $M = 3 \times 5 \times 7 = 105$

2. $M_1 = 105 / 3 = 35$, $M_2 = 105 / 5 = 21$, $M_3 = 105 / 7 = 15$

3. The inverses are $M_1^{-1} = 2$, $M_2^{-1} = 1$, $M_3^{-1} = 1$

4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105 = 223 \bmod 105$

Example

Find all integers x which leave a remainder of 1, 2, 3, and 4 when divided by 5, 7, 9, and 11 respectively.

Solution: We are asked to solve the system of congruences:

$x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 7$, $x \equiv 3 \pmod 9$, $x \equiv 4 \pmod{11}$.

We have $M = 5 \cdot 7 \cdot 9 \cdot 11 = 3465$ and

$M1 = M/5 = 693$,

$M2 = M/7 = 495$,

$M3 = M/9 = 385$, and

$M4 = M/11 = 315$.

The inverses are $y1 = 2$, $y2 = 3$, $y3 = 4$, and $y4 = 8$.

Hence $x = 1 \cdot 693 \cdot 2 + 2 \cdot 495 \cdot 3 + 3 \cdot 385 \cdot 4 + 4 \cdot 315 \cdot 8 = 19056$.

So $x = [19056] \bmod 3465 = [1731] \bmod 3465$.

Example

Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12.

Solution

This is a CRT problem. We can form three equations and solve them to find the value of x.

$$x = 3 \bmod 7$$
$$x = 3 \bmod 13$$
$$x = 0 \bmod 12$$

If we follow the four steps, we find x = 276. We can check that 276 = 3 mod 7, 276 = 3 mod 13 and 276 is divisible by 12 (the quotient is 23 and the remainder is zero).

Reference Book

- Cryptography and Information security, second edition,by V. K. Pachghare.