Chinese Remainder Theorem (Applications)

DR. ODELU VANGA

COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY
SRI CITY, INDIA

Linear Congruences, Inverses

A congruence of the form $ax \equiv b \pmod{m}$ is called a *linear congruence*.

- To *solve* the congruence is to find the x's that satisfy it.

An *inverse of a, modulo m* is any integer a' such that $a'a \equiv 1 \pmod{m}$.

- If we can find such an a', notice that we can then solve $ax \equiv b$ by multiplying through by it.
- Implies $a'ax \equiv a'b$, thus $1 \cdot x \equiv a'b$, thus $x \equiv a'b$ (mod m).

Theorem: If $\gcd(a,m)=1$ and $m>1$, then a has a unique (modulo m) inverse a'.

- Proof: By theorem 1, $\exists st$: $sa+tm = 1$, so $sa+tm \equiv 1 \pmod{m}$.

  Since $tm \equiv 0 \pmod{m}$, $sa \equiv 1 \pmod{m}$. Thus s is an inverse of a (mod m).

  From the result, if $ra \equiv sa \equiv 1$ then $r \equiv s$.

  Thus this inverse is unique mod m. (All inverses of a are in the same congruence class as s.)

Note: Linear congruences are the basis to perform arithmetic with large integers.

Example:
Find an inverse of 4 modulo 9

Since $\gcd(4, 9) = 1$, we know that there is an inverse of 4, modulo 9.

Using the Euclidean algorithm to find the greatest common divisor:

$$9 = 2 \times 4 + 1$$

Rewrite:

$$9 - 2 \times 4 = 1$$

So, -2 is an inverse of 4 module 9

We have: -2 x 4 = -8. And -8 mod 9 = 1.

What are the solutions of the linear congruence $4x \equiv 5 \pmod 9$?

Since we know that -2 is an inverse for $4 \bmod 9$,

we can multiply both sides of the linear congruence:

$$-2 \times 4x \equiv -2 \times 5 \pmod 9$$

Since $-8 \equiv 1 \pmod 9$ and $-10 \equiv 8 \pmod 9$,

it follows that if x is a solution, then $x \equiv -10 \equiv 8 \pmod 9$.

We now have $4x \equiv 4 \times 8 \equiv 5 \pmod 9$ which shows that all such x satisfy the congruence.

So, solutions x such that $x \equiv 8 \pmod 9$, namely, 8, 17, 26, …, and -1, -10, etc.

$k = (a, b)$

$a^{-1} \bmod m$ exists

Puzzle

There are certain things whose number is unknown.

- When divided by 3, the remainder is 2;
- when divided by 5, the remainder is 3; and
- when divided by 7, the remainder is 2.

What is the number of things?

What's x such that:

$$\left.\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7}? \end{aligned}\right\}$$

Chinese Remainder Theorem

Theorem: (Chinese remainder theorem.)

Let $m_1,\ldots,m_n > 0$ be relatively prime.

Then the system of equations $x \equiv a_i \pmod{m_i}$ (for i=1 to n)

has a unique solution modulo $m = m_1 \cdot \ldots \cdot m_n$.

Proof: Let $M_i = m/m_i$.

Since $\gcd(m_i, M_i)=1$, $\exists y_i$ such that $y_i M_i \equiv 1 \pmod{m_i}$.

Now let $x = \sum_i a_i y_i M_i$.

Since $m_i | M_k$ for $k \neq i$, $M_k \equiv 0 \pmod{m_i}$, so $x \equiv a_i y_i M_i \equiv a_i \pmod{m_i}$.

Thus, the congruences hold.

(Uniqueness is an exercise.)

Computer Arithmetic with Large Integers

By Chinese Remainder Theorem, an integer a where $0 \le a < m = \prod m_i$, $\gcd(m_i, m_{j \neq i}) = 1$,

can be represented by a's residues mod m_i:

$$\mathbf{(a \bmod m_1,\ a \bmod m_2,\ \ldots,\ a \bmod m_n)}$$

Implicitly, consider the set of equations $x \equiv a_i \pmod{m_i}$, With $a_i = a \bmod m_i$.

By the CRT, unique $x \equiv a \bmod m$, with $m = \prod m_i$ is a solution.

How to represent uniquely all integers less than 12 by pairs, where the first component is the remainder of the integer upon division by 3 and the second component is the remainder of the integer upon division by 4?

Finding the remainder of each integer divide by 3 and 4, we obtain:

a = (a mod 3, a mod 4) e.g. 5 = ((5 mod 3), (5 mod 4)) = (2, 1)

0=(0,0);	**1=(1,1);**	**2=(2,2);**	**3=(0,3);**
4=(1,0);	**5=(2,1);**	**6=(0,2);**	**7=(1,3);**
8=(2,0);	**9= (0,1);**	**10 = (1,2);**	**11= (2,3)**

Note we have the right "number of pairs"; one for each number up to 4x3 -1.

Computer Arithmetic with Large Integers

To perform arithmetic upon large integers represented in this way,

- Simply perform operations on these separate residues!
  - Each of these might be done in a single machine operation.
  - The operations may be easily parallelized on a vector machine.
- Works so long as the desired result $< m$.

Suppose we can perform operation with integers less than 100 can be done easily; we can restrict ourselves to integers less than 100, if we represent the integers using their remainders modulo pairwise relatively prime integers less than 100; e.g., 99, 98, 97, 95.

99×98×97×95

By the Chinese remainder theorem, any number up to

$$99\times 98 \times 97 \times 95 = 89{,}403{,}930$$ ✓

can be represented uniquely by its remainders when divided by these four moduli.

For example, the number **123684** can be represented as

(123684 mod 99; 123684 mod 98; 123684 mod 97; 123684 mod 95) = (33,8,9,89) ✓

413456 can be represented as

(413456 mod 99; 413456 mod 98; 413456 mod 97; 413456 mod 95) = (32,92,42,16)

To perform a sum we only have to sum the residues:

(33, 8, 9, 89)+(32, 92 , 42, 16)

= (65 mod 99. 100 mod98, 51mod97, 105mod95)

= (65, 2, 51, 10)

To find the sum we just have to solve the system of linear congruences:

$$\left.\begin{aligned} x &\equiv 65 \pmod{99} \\ x &\equiv 2 \pmod{98} \\ x &\equiv 51 \pmod{97} \\ x &\equiv 10 \pmod{95} \end{aligned}\right\}$$

Solution: 537140 = **123684 + 413456**

“Bigger” Example

For example, the following numbers are relatively prime:

$m_1 = 2^{25}-1 = 33{,}554{,}431 = 31 \cdot 601 \cdot 1{,}801$

$m_2 = 2^{27}-1 = 134{,}217{,}727 = 7 \cdot 73 \cdot 262{,}657$

$m_3 = 2^{28}-1 = 268{,}435{,}455 = 3 \cdot 5 \cdot 29 \cdot 43 \cdot 113 \cdot 127$

$m_4 = 2^{29}-1 = 536{,}870{,}911 = 233 \cdot 1{,}103 \cdot 2{,}089$

$m_5 = 2^{31}-1 = 2{,}147{,}483{,}647$ (prime)

Thus, we can uniquely represent all numbers up to

$$m = \prod m_i \approx 1.4\times 10^{42} \approx 2^{139.5}$$

by their residues r_i modulo these five m_i.

- *E.g.*, $10^{30} = (r_1 = 20{,}900{,}945;\ \ r_2 = 18{,}304{,}504;\ \ r_3 = 65{,}829{,}085;$
  $r_4 = 516{,}865{,}185;\ \ r_5 = 1{,}234{,}980{,}730)$

To add two such numbers in this representation,
Just add their corresponding residues using machine-native 32-bit integers.
Take the result mod 2^k-1:

If result is ≥ the appropriate 2^k-1 value, subtract out 2^k-1

Note: No carries are needed between the different pieces!

What's x such that: $x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

$x \equiv a_i \pmod{m_i}$
$m = \prod m_i$
$y_i = M_i^{-1} \pmod{m_i}$
$M_i = m / m_i$
$x = \sum_i a_i y_i M_i \pmod m$

Using the Chinese Remainder theorem let:

$m = 3\times5\times7 = 105$

$M_1 = m/3 = 105/3 = 35$; 2 is an inverse of $M_1 = 35 \pmod 3$ (since $35\text{x}2\equiv1 \pmod 3$)

$M_2 = m/5 = 105/5 = 21$; 1 is an inverse of $M_2 = 21 \pmod 5$ (since $21\text{x}1\equiv1 \pmod 5$)

$M_3 = m/7 = 15$; 1 is an inverse of $M_3 = 15 \pmod 7$ (since $15\text{x}1\equiv1 \pmod 7$)

So $x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233 \equiv 23 \pmod{105}$

So answer: 23

What is the x value in Z_{15} such that

$$x \equiv 1 \; mod \; 3$$
$$x \equiv 4 \; mod \; 5$$

$a_1 = 1$, $m_1 = 3$ $m = 3 \times 5 = 15$

$a_2 = 4$, $m_2 = 5$ $M_1 = 5$

$M_2 = 3$

$x = a_1 y_1 M_1 + a_2 y_2 M_2 \pmod{15}$

$= 34 \pmod{15}$

$= 4$

$y_1 = M_1^{-1} \pmod 3 = ?$

$y_2 = M_2^{-1} \pmod 5 = ?$

$$x \equiv 6 \pmod{11}$$
$$x \equiv 13 \pmod{16}$$
$$x \equiv 9 \pmod{21}$$
$$x \equiv 19 \pmod{25}$$

Solve ?

$a_1 = 6$ $a_2 = 13$ $a_3 = 9$ $a_4 = 19$

$m_1 = 11$ $m_2 = 16$ $m_3 = 21$ $m_4 = 25$

$(m_i, m_j) = 1$, for $i \neq j$

$$m = \prod m_i = m_1 m_2 m_3 m_4$$
$$= 11 \times 16 \times 21 \times 25$$

$$M_1 = m/m_1 = 16 \times 21 \times 25 = 8400$$
$$M_2 = m/m_2 = 11 \times 21 \times 25 = 5775$$
$$M_3 = m/m_3 = 11 \times 16 \times 25 = 4400$$
$$M_4 = m/m_4 = 11 \times 16 \times 21 = 3696$$

$$\boxed{\begin{aligned} y_1 &= M_1^{-1} \pmod{m_1} = 8 \\ y_2 &= M_2^{-1} \pmod{m_2} = 15 \\ y_3 &= M_3^{-1} \pmod{m_3} = 2 \\ y_4 &= M_3^{-1} \pmod{m_4} = 6 \end{aligned}}$$

$$x = 209869 \pmod{92400}$$
$$= 51669 \text{ ??}$$

Ex: Find all solutions of $x^2 \equiv 1 \pmod{144}$

Sol: $144 = 2^4 \cdot 3^2$ and $\gcd(2^4, 3^2) = 1$

$m_1 = 16$, $m_2 = 9$

$$\boxed{\begin{aligned} x^2 &\equiv 1 \pmod{16} \\ x^2 &\equiv 1 \pmod{9} \end{aligned}}$$

Home work.??