# The Chinese Remainder Theorem

Ziming Bian

University of California, Santa Barbara

June 7, 2014

# Definition

What is the Chinese remainder theorem?

The Chinese remainder theorem is a result about congruence in number theory and its generalizations in abstract algebra.

The basic form is about a number n that divided by some divisors and leaves remainders

# Example

**Example**: Here we have a look at a basic example.

What is the lowest number n that divided by 3 leaves a remainder of 2, divided by 5 leaves a remainder of 3 , and divided by 7 leaves a remainder of 2

Solution:
Firstly, we need to find a number that can be divided by 5 and 7 and also divided by 3 leaves a remainder of 1 that number is 70

Secondly, we need to find a number that can divided by 3 and 7 and also divided by 5 leaves a remainder of 1 that number is 21

Thirdly, we need to find a number that can be divided by 3 and 5 and also divided by 7 leaves a remainder of 1 that number is 15

And the number we find is divided by 3 leaves a remainder 2 then $70 \times 2 = 140$

It is also divided by 5 leaves a remainder 3 then we have $21 \times 3 = 63$

Then it is divided by 7 leaves a remainder 2 then we have $15 \times 2 = 30$

Then 140+63+30=233 because 63 and 30 are all divided by 3 then 233 and 140 have the same remainder divided by 3.
The same thing happened with 233 and 63 divided by 5 and 233 and 30 divided by 7. Then 233 is the number satisfied the question.
And the lowest common multiple of 3,5,7 are 105 so $233 - 105 \times 2 = 23$ is the answer we need to find.

# Principle of the Chinese Remainder Theorem

We suppose that for $n \geq 2$, we have $m_1, m_2, m_3, ..., < m_n$ which are coprime to each other.
We suppose $M = m_1 \times m_2 \times m_3 \times ... \times m_n$
Then we have
$M = m_1 \times M_1 = m_2 \times M_2 = m_3 \times M_3 = ... = m_n \times M_n$
For the following congruences:
$x \equiv c_1 \pmod{m_1}$
$x \equiv c_2 \pmod{m_2}$
...
$x \equiv c_n \pmod{m_n}$
The congruence $x \equiv M_1 a_1 c_1 + M_2 a_2 c_2 + ... + M_n a_n c_n$ have unique positive integer solution. ($a_i$ satify $M_i a_i \equiv 1 \bmod m_i$, i=1,2,...,n)

# The Chinese remainder theorem in polynomial

We suppose that $m_1(x)$,$m_2(x)$,...,$m_n(x)$ are coprime to each other, then we can have polynomials $a_1(x)$,$a_2(x)$,...,$a_n(x)$
Then there must exist an polynomial, which satisfy:
$f(x) \equiv a_1(x)$ (mod $m_1$(x))
$f(x) \equiv a_2(x)$ (mod $m_2$(x))
...
$f(x) \equiv a_n(x)$ (mod $m_n$(x))
When the degree of f(s) is not higher than m(x)
$(m(x) = m_1(x)m_2(x)...m_n(x))$
There is only one f(x)

When $m_i(x) = X - B_i \in Q[x]$, i=1,2,...,n,
$m_i(x) = m_i(b_i)$ (mod$(x - b_i)$)
Then
$f(x) = a_1(x)$ (mod $m_1(x - b_1)$)
$f(x) = a_2(x)$ (mod $m_2(x - b_2)$)
...
$f(x) = a_n(x)$ (mod $m_n(x - b_n)$)
the degree of f(x) is not higher than n there is only one f(x)
$f(x) = a_i\ (mod(x - bi))$ is same as $f(b_i) = a_i$(i=1,2,...,n)
Then we can have if there are $b_i(i = 1, 2, ..., n)$ and every $b_i$ is different, and any $a_i(i = 1, 2, , n)$ there exist only one f(x) the degree is lower than n to let $f(b_i) = a_i(i = 1, 2, ..., n)$

If we can find the polynomial $M_i(x)$ i=1,2,..., n to let
$M_i(x) = 1(\text{mod}x - b_i))$ $M_i(x) = 0(\text{mod(x}-b_j))$, $M_i(x) = 0$
$(mod(x - bj))$ $i \neq j$
Then we can find $f(x) = a_1 M_1(x) + a_2 M_2(x) + + a_n M_n(x)$

$$= \sum_{n}^{j=1} a_j \prod_{n}^{i=1} \frac{x - b_i}{b_j - b_i} (i \neq j)$$

This is the Lagrange interpolation polynomial

# Example

Calculate $0^2 + 1^2 + 2^2 + \ + (n-1)^2$
Proof: We suppose the polynomial
$f(n) = 0^2 + 1^2 + 2^2 + \ + (n-1)^2$; n states for the number of terms.
Then we have f(0)=0,f(1)=0,f(2)=1,f(3)=5
Then we can have f(n)=0 $* M_1(n) + 0 * M_2(n) + 1 * M_3(n) + 5 * M_4(n)$=1 $\times \frac{(n-0)(n-1)(n-3)}{(2-0)(2-1)(2-3)}$+5 $* \frac{(n-0)(n-1)(n-2)}{(3-0)(3-1)(3-2)}$
$= \frac{1}{6}(n(n-1)(2n-1)$

# Example

If the f(x) have the remainder of each $x^2+1, x^2+2$ with $4x+4, 4x+8$
What is the remainder of f(x) divided by $(x^2+1)(x^2+2)$
Solution: $f(x) = 4x+4 \; mod(x^2+1)$
$f(x) = 4x+8 \; mod(x^2+2)$
And because $x^2+1$ and $x^2+2$ are relatively prime
$(-1)x^2+1+x^2+2=1$
Then we can get f(x)=$(4x+4)(x^2+2)+(4x+8)(-1)(x^2+1)$ mod$(x^2+1)(x^2+2)$
Then the answer is $4x-4x^2$

# Example

If $f(x) \equiv 4 \mod(x-1)$, $f(x) \equiv 8 \mod(x-2)$, $f(x) \equiv 16 \mod(x-3)$

What is remainder of f(x) divided by $(x-1)(x-2)(x-3)$?

Solution:Let $f(x) = p(x)(x-1)(x-2)(x-3) + r(x)$

Degree of r(x) is lower than 3

We can have this from the problem

$r(1) = f(1) = 4$

$r(2) = f(2) = 8$

$r(3) = f(3) = 16$

Then we can get the $r(x) =$

$4 \times \frac{4(x-2)(x-3)}{(1-2)(1-3)} + 8 \times \frac{(x-1)(x-3)}{(2-1)(2-3)} + 16 \times \frac{(x-1)(x-2)}{(3-1)(3-2)} = 2x^2 - 2x + 4$

# Secret sharing using Chinese Remainder Theorem

$A_1, A_2, ..., A_n$ are n relatively prime numbers
If there is integer y that have the remainder of $B_1, B_2, ..., B_n$ divided by $A_1, ..., A_n$.
Then we need to find what Y is.
Let $M = A_1 \times A_2 \times ... \times A_n$
$X_1$ are all the integers that can be divided by $A_2, A_3, ..., A_n$
$Y_1$ are all the integers that can be divided by $A_2 \times ... \times A_n$ and leaves remainder of $B_1$ divided by $A_1$.
$X_2$ are all the integers that can be divided by $A_1 \times A_2 \times ... \times A_n$
$Y_2$ are all the integers that can be divided by $A_1 \times A_2 \times ... \times A_n$ and leaves a remainder $B_2$ divided by $A_2$

$X_i$ are all the integers that can be divided by
$A_1, A_2, A_i - 1, A_i + 1, ..., An$
$Y_i$ are all the integers that can be divided by
$A_1, A_2, A_I - 1, A_I + 1, A_n$ and leaves a remainder of $B_i$ divided by $A_i$
$X_1 = A_2 \times A_3 \times ... \times A_n \times m = \frac{M \times m}{A_1}$
$X_2 = A_1 \times A_3 \times ... \times A_n \times m = \frac{M \times M}{A_2}$
m are any integers
$X_n = A_1 \times A_2 \times ... \times A_N - 1 \times M = \frac{M \times m}{An}$
If $F_i$ satisfied both $X_i$ and $Y_i$, and $F_i$ is the smallest positive integer in $Y_i$
$Y_1 = F_1 + A - 1 \times A_2 \times ... \times A_n \times M = F_1 + M \times m$
...
$Y_n = F_n + A_1 \times A_2 \times ... \times A_n \times m = F_n + M \times m$
Then $Y = Y_1 + Y_2 + Y_3 + ..Y_N = F_1 + F_2 + \ + F_N + M \times m$

Let the Y be the cleartext and $B1, ...Bn$ be the ciphertext.
$A_1, ...A_n$ and N be the key.
The steps are like these:
First choose $A_1, ...A_n$ to be the key
Then to calculate product of these numbers M
Third calculate the $F_1, F_2, ..., F_n$
Then $Y = Y_1 + Y_2 + ...Y_n = F_1 + F_2 + F_3 + ... + F_n + M \times m$
We can have $m = \frac{Y-(F_1+F_2++F_n)}{M}$
At last let Y divided by $A_1, ...A_n$ to get the remainders $B1, ...Bn$ to be the ciphertext.

# Deciphering

We know the ciphertext $B_1...B_N$ and the key $A_1...A_n$ and N and calculate the $F_1...F_N$
We can get Y by the
$Y = Y_1 + Y_2 + ...Y_n = F_1 + F_2.. + F_N + M \times m$

Cleartext $X = 200$ key$= 5, 7, 11$ ciphertext$= 1, 6$
$F_1 = 231$,$F_2 = 55$,$F_3 = 175$
$m = 2001 - (231 + 55 + 175)(5 \times 7 \times 11) = 4$ be the other secret key.
Decipher:
$Y = y_1 + ..y_n = F_1 + f_2 + ..F_n + M \times m =$
$221 + 175 + 55 + 5 \times 7 \times 11 \times 4 = 2001$

# Thank you

Thanks for listening!!!