Foundation of Cryptography

Session 12

Date: 01 March 2021

Dr. V. K. Pachghare

Number Theory

- **Modular Arithmetic**
- **Euclidean Algorithm**
- **Prime Numbers**
- **Fermat's Little Theorem**
- **Euler Totient Function**
- **Extended Euclidean Algorithm**
- **Chinese Remainder Theorem**

Modular Arithmetic

You are familiar to find out the **mod** of any number with some base.

Suppose we have to find out the mod of a number m with base n as: **m mod n**

The mod with respect to base n is (0, 1, 2, … n – 1).

Suppose m = 23 and n = 9, then

23 mod 9 = 5

For any value of m, the value of m mod 9 is from (0, 1, 2, … 8) i.e. up to n – 1.

Mod of negative number

If m is negative, suppose m = –15 and base n = 9 then

–15 mod 9 = –6 mod 9

= (**9** – 6) mod **9**

= 3 mod 9

= 3

Addition of modular numbers

The addition of two numbers p and q with same modular base n is:

$(p \bmod n + q \bmod n) \bmod n = (p + q) \bmod n$

For example:

$15 \bmod 9 + 17 \bmod 9 = (15 \bmod 9 + 17 \bmod 9) \bmod 9$

$= (6 + 8) \bmod 9$

$= 14 \bmod 9 = 5$

OR

$15 \bmod 9 + 17 \bmod 9 = (15 + 17) \bmod 9$

$= (32) \bmod 9 = 5$

Subtraction of modular numbers

The subtraction of two numbers p and q with same modular base n is:

$(p \bmod n - q \bmod n) \bmod n = (p - q) \bmod n$

For example:

$17 \bmod 9 - 15 \bmod 9 = (17 \bmod 9 - 15 \bmod 9) \bmod 9$

$= (8 - 6) \bmod 9 = 2 \bmod 9 = 2$

OR

$17 \bmod 9 - 15 \bmod 9 = (17 - 15) \bmod 9$

$= 2 \bmod 9 = 2$

Multiplication of modular numbers

The multiplication of two numbers p and q with same modular base n is:

(p mod n * q mod n) mod n = (p * q) mod n

For example:

17 mod 9 * 15 mod 9 = (17 mod 9 * 15 mod 9) mod 9

= (8 * 6) mod 9 = 48 mod 9 = 3

OR

17 mod 9 * 15 mod 9 = (17 * 15) mod 9 = (255) mod 9 = 3

Note: $m^a \bmod n = m^{pq} \bmod n$

where $a = p * q$

$= (m^p \bmod n)^q \bmod n$

Suppose $m = 5$, $a = 6$ and base $= 7$

$m^a \bmod n = 5^6 \bmod 7$

Here factors of 6 are $p = 2$ and $q = 3$

then $(m^p \bmod n)^q \bmod n = (5^2 \bmod 7)^3 \bmod 7$

$= (25 \bmod 7)^3 \bmod 7 = 4^3 \bmod 7 = 1$

Find the value of 7^7 mod 9

$7^7 \bmod 9 = 7 * (7^3)^2 \bmod 9$

$7 \bmod 9 = 7$

$7^2 \bmod 9 = 49 \bmod 9 = 4$

$7^3 \bmod 9 = 7 * 7^2 \bmod 9 = 7 * 4 \bmod 9 = 28 \bmod 9 = 1$

$7^6 \bmod 9 = (7^3)^2 \bmod 9 = 1^2 \bmod 9 = 1$

$7^7 = 7^6 * 7 \bmod 9 = 1 * 7 \bmod 9 = 7$

$11^7 \bmod 13$

$11^2 = 121 \pmod{13} = 4$

$11^4 = (11^2)^2 = 4^2 = 16 \pmod{13} = 3$

$11^7 = 11 * 11^2 * 11^4$

$11^7 = (11 * 4 * 3) = 132 = 2 \pmod{13} = 2$

Find the value of unit place digit of 51^{51}

We know that unit place digit can be found by taking mod 10 of the given number.

Here, $51 \bmod 10 = 1$

Therefore, $51^{51} \bmod 10 = 1^{51} \bmod 10 = 1$

Therefore, the unit place digit of 51^{51} is 1.

Find the value of final digit (LSB) of $(((((((7^7)^7)^7)^7)^7)^7)^7)^7$?

$$7^2 \bmod 10 = 49 \bmod 10$$
$$= 9 \bmod 10$$
$$= (-1) \bmod 10 \qquad \text{(since } 9 \bmod 10 = -1 \bmod 10\text{)}$$

$$7^7 = (7^2)^3 * 7$$
$$7^7 \bmod 10 = (7^2)^3 * 7 \bmod 10$$
$$= (-1)^3 * 7 \bmod 10 \qquad \text{(since } 7^2 \bmod 10 = -1\text{)}$$
$$= -7 \bmod 10$$

$$
\begin{aligned}
(7^7)^7 \bmod 10 &= (-7)^7 \bmod 10 \\
&= (-1)^7(7)^7 \bmod 10 \\
&= -1 * (-7) \bmod 10 && \text{(since } 7^7 \bmod 10 = -7\text{)} \\
&= 7 \bmod 10 \\
((7^7)^7) \bmod 10 &= (7)^7 \bmod 10 && \text{(since } (7^7)^7 \bmod 10 = 7\text{)} \\
&= -7 \bmod 10 && \text{(since } 7^7 \bmod 10 = -7\text{)} \\
(((7^7)^7)^7) \bmod 10 &= (-7)^7 \bmod 10 && \text{(since } ((7^7)^7)^7 \bmod 10 = -7\text{)} \\
&= (-1)^7\ (7)^7 \bmod 10 \\
&= -\ (-7) \bmod 10 && \text{(since } 7^7 \bmod 10 = -7\text{)} \\
&= 7 \bmod 10
\end{aligned}
$$

As 7 to the power 7 for odd number of times answer is –7 mod 10 and even number of times answer is 7 mod 10

Therefore, $(((((((7^7)^7)^7)^7)^7)^7)^7)^7 = -7 \bmod 10$

$= 3 \bmod 10$

$= 3$

Euclidean Algorithm

Greatest Common Divisor (GCD)

- Suppose p and q are two numbers.
- GCD (p, q) is the largest number that divides evenly both p and q.
- Euclidean algorithm is used to compute the greatest common divisor (GCD) of two integer numbers.
- This algorithm is also known called as *Euclid's algorithm*.

GCD(p, q) = GCD(q, p mod q)

Euclid's algorithm to compute GCD(p, q):

n = p, m = q

while m > 0

r = n mod m

n = m, m = r

return n

Compute GCD(7, 38)

$38 = 5 \times 7 + 3$

Compute GCD(7, 38)

$38 = 5 \times 7 + 3$

$7 = 2 \times 3 + 1$

Compute GCD(7, 38)

$38 = 5 \times 7 + 3$

$7 = 2 \times 3 + 1$ ---------GCD

$3 = 3 \times 1 + 0$

GCD (7, 38) = 1

Compute GCD(10, 25)

$25 = 2 \times 10 + 5$

Compute GCD(10, 25)

$25 = 2 \times 10 + \underline{\mathbf{5}}$ **-----GCD**

$10 = 2 \times 5 + \mathbf{0}$

GCD (10, 25) = 5

Compute GCD(831, 366)

$831 = 2 \times 366 + 99$

Compute GCD(831, 366)

$831 = 2 \times 366 + 99$

$366 = 3 \times 99 + 69$

Compute GCD(831, 366)

$831 = 2 \times 366 + 99$

$366 = 3 \times 99 + 69$

$99 = 1 \times 69 + 30$

Compute GCD(831, 366)

$831 = 2 \times 366 + 99$

$366 = 3 \times 99 + 69$

$99 = 1 \times 69 + 30$

$69 = 2 \times 30 + 9$

Compute GCD(831, 366)

$831 = 2 \times 366 + 99$

$366 = 3 \times 99 + 69$

$99 = 1 \times 69 + 30$

$69 = 2 \times 30 + 9$

$30 = 3 \times 9 + 3$

Compute GCD(831, 366)

$831 = 2 \times 366 + 99$

$366 = 3 \times 99 + 69$

$99 = 1 \times 69 + 30$

$69 = 2 \times 30 + 9$

$30 = 3 \times 9 + \mathbf{3}$ **(GCD)**

$9 = 3 \times 3 + \mathbf{0}$

GCD (831, 366) = 3

Prime Numbers

- A prime number is divisible only by 1 and itself
- For example: {2, 3, 5, 7, 11, 13, 17, …}

Prime Factorization

- To factor a number *n* is to write it as a product of other numbers.
- $n = a * b * c$
- Or, 100 = 5 * 5 * 2 * 2
- Prime factorization of a number *n* is writing it as a product of prime numbers.
- 143 = 11 * 13

Relatively Prime Numbers

- Two numbers are relatively prime if they have no common divisors other than 1.
- 10 and 21 are relatively prime, in respect to each other, as 10 has factors of 1, 2, 5, 10 and 21 has factors of 1, 3, 7, 21.
- The Greatest Common Divisor (GCD) of two relatively prime numbers can be determined by comparing their prime factorizations and selecting the least powers.

Contd…

- For example, $125 = 5^3$ and $200 = 2^3 * 5^2$
- GCD(125, 200) = $2^0 * 5^2 = 25$
- If the two numbers are relatively prime the GCD will be 1.
- Consider the following: 10(1, 2, 5, 10) and 21(1, 3, 7, 21)
- GCD(10, 21) = 1
- It then follows, that a prime number is also relatively prime to any other number other than itself and 1.

Fermat's Little Theorem

- If p is prime and a is an integer not divisible by p, then . . .
- $a^{p-1} = 1 \pmod{p}$.
- And for every integer a
- $a^{p} = a \pmod{p}$.
- This theorem is useful in public key (RSA) and primality testing.

Find the smallest positive residue *y* in the following congruence.

$$7^{69} = y \bmod 23$$

Here n = 7 and p = 23. as p is prime we can apply Fermat's Little theorem to solve this problem.

Fermat's Little theorem is

$$n^{P-1} = 1 \bmod p$$

By substituting the values of n and p and rewrite the equation:

$$7^{(23-1)} = 1 \bmod 23$$

$$7^{(22)} = 1 \bmod 23$$

we can write 7^{69} as $(7^{22})^3 * 7^3$

therefore $7^{69} = y \bmod 23$

can be written as

$$7^{69} = 7^{66} * 7^3$$

$$7^{69} = (7^{22})^3 * 7^3 \bmod 23$$

$$= (1)^3 * 7^3 \bmod 23$$

$$= 343 \bmod 23 = 21$$

Therefore the smallest positive residue y = 21.

Find all solutions of the following congruence

$$4x = 8 \bmod 11$$

1. Calculate the GCD of 4 and 11.

   GCD(4, 11) = 1

2. As GCD is 1, find the multiplicative inverse.

   The multiplicative inverse of 1 = 4 mod 11 is 3. (As 4 * 3 = 12 mod 11 = 1)

3. $x = 8 * 3 \bmod 11$

   $x = 2 \bmod 11$

All the solutions of the given congruence is $x = 2 \bmod 11$.

Compute the value of $12345^{23456789} \bmod 101$.

By Fermat's Little theorem $n^{p-1} = 1 \bmod p$

where $n = 12345$ and $p = 101$.

$$12345^{(101-1)} \bmod 101 = 1$$

$$12345^{100} \bmod 101 = 1$$

Therefore, $12345^{23456789} \bmod 101$

$$= (12345^{100})^{234567} * 12345^{89} \bmod 101$$

$$= 1 * 12345^{89} \bmod 101$$

$$= 12345^{89} \bmod 101$$

But $12345 \bmod 101 = 23$

Therefore, $23^{89} \bmod 101$

$$23 \bmod 101 = 23$$

$$23^2 \bmod 101 = 24$$

$$23^3 \bmod 101 = 47$$

$$23^4 \bmod 101 = 71$$

$$23^5 \bmod 101 = 17$$

$$23^7 \bmod 101 = 4$$

$$\begin{aligned} 23^{89} \bmod 101 &= (23^7)^{12}\ 23^5 \bmod 101 \\ &= 4^{12} * 17 \bmod 101 \\ &= 5 * 17 \bmod 101 \\ &= 85 \end{aligned}$$

Therefore, the value of $12345^{23456789} \bmod 101 = 85$.

Euler Totient Function: ø(n)

- when doing arithmetic modulo n
- **complete set of residues** is: `0..n-1`
- **reduced set of residues** is those numbers (residues) which are relatively prime to n
  - Eg for n=10,
  - complete set of residues is {0,1,2,3,4,5,6,7,8,9}
  - reduced set of residues is {1,3,7,9}
- number of elements in reduced set of residues is called the **Euler Totient Function ø(n)**

The Euler Φ function is defined as follows: Φ(n) is the number of positive integers less than n that are relatively prime to n.

- Φ(*n*) = how many numbers there are between 1 and *n*-1 that are relatively prime to *n*.
- Φ(4) = 2 (1, 3 are relatively prime to 4)
- Φ (5) = 4 (1, 2, 3, 4 are relatively prime to 5)
- Φ(6) = 2 (1, 5 are relatively prime to 6)
- Φ(7) = 6 (1, 2, 3, 4, 5, 6 are relatively prime to 7)

Euler Totient Function Contd…

- As you can see from Φ(5) and Φ(7), Φ(*n*) will be *n*-1 whenever *n* is a prime number. This implies that Φ(*n*) will be easy to calculate when *n* has exactly two different prime factors: Φ(*P* * *Q*) = (*P*-1)*(*Q*-1), if *P* and *Q* are prime.

The generalise formula to calculate $\Phi(n)$ of a number n is:

$$\Phi(n) = A_1^{m_1} * A_2^{m_2} * A_3^{m_n} * \ldots * A_n^{m_n}$$

$$= n * \left(1 - \frac{1}{A_1}\right) * \left(1 - \frac{1}{A_2}\right) * \left(1 - \frac{1}{A_3}\right) * \ldots \left(1 - \frac{1}{A_n}\right)$$

$$\Phi(n^m) = n^{m-1}\Phi(n) \text{ [identity relating to } \Phi(n^m) \text{ to } \Phi(n)]$$

- For example:
- $9 = 3^2$, $\phi(9) = 9^* (1-1/3) = 6$
- $4 = 2^2$, $\phi(4) = 4^* (1-1/2) = 2$
- $15 = 3^*5$, $\phi(15) = 15^* (1-1/3)^*(1-1/5) = 15^*(2/3)^*(4/5) = 8$

If $n = 5488$, find $\Phi(n)$.

$$\Phi(n) = A_1^{m_1} * A_2^{m_2} * A_3^{m_n} * \ldots * A_n^{m_n}$$

$$= n * \left(1 - \frac{1}{A_1}\right) * \left(1 - \frac{1}{A_2}\right) * 1 - \frac{1}{A_3} * \ldots \left(1 - \frac{1}{A_n}\right)$$

$5488 = 16 * 343$

$= 2^4 * 7^3$; here $A_1 = 2$ and $A_2 = 7$

$$= 5488 * \left(1 - \frac{1}{2}\right) * \left(1 - \frac{1}{7}\right)$$

$$= 5488 * \left(\frac{1}{2}\right) * \left(\frac{6}{7}\right)$$

$= 2352$

Euler's Totient Theorem

- This theorem generalizes Fermat's theorem and is an important key to the RSA algorithm.
- If GCD(a, p) = 1, and $a < p$, then $a^{\varnothing(p)} = 1 \pmod{p}$.
- In other words, If a and p are relatively prime, with a being the smaller integer, then when we multiply a with itself $\varnothing(p)$ times and divide the result by p, the remainder will be 1.

Euler's Totient Theorem Contd…

- Let's test the theorem: $a^{\varnothing(p)} \bmod p = 1$
- If $a = 5$ and $p = 6$
- Then $\varnothing(6) = \varnothing(2 * 3) = \varnothing(2)\ \varnothing(3) = (2-1) * (3-1) = 2$
- So, $5^{\varnothing(6)} = 5^2 = 25$ and $25 = 24+1 = 6*4+1$
- => $25 = 1 \pmod 6$ OR $25 \% 6 = 1$
- It also follows that $a^{\varnothing(p)+1} = a \pmod p$ so that p does not necessarily need to be relatively prime to a.

- $a^{\varnothing(p)} = 1 (\text{mod } p)$
- $a^{b} \text{mod } p = a^{b \text{ mod } \varnothing(p)} \text{ mod } p$

Find the last digit of 7^{2013}.

$7^{2013} \bmod 10 = 7^{2013 \bmod \phi(10)} \bmod 10$ $\{\phi(10)= 4\}$

Therefore $2013 \bmod 4 = 1$

$7^{2013 \bmod \phi(10)} \bmod 10 = 7^{1} \bmod 10 = 7$

Ex 2:

Find the last two digits of 9^{1573}.

$9^{1573} \bmod 100$

Apply $a^{b} \bmod p = a^{b \bmod \varnothing(p)} \bmod p$

$9^{1573} \bmod 100$

$= 9^{1573 \bmod \varnothing(100)} \bmod 100$

Since $1573 \bmod \varnothing(100) = 13$

$= 9^{13} \bmod 100 \quad (9^3 \bmod 100 = 29)$

$9^{13} \bmod 100 = (9^3)^4 \times 9 \bmod 100 = 29^4 \times 9 \bmod 100$

$= (41)^2 \times 9 \bmod 100$ Since $(29^2) \bmod 100 = 41$

$= 29$

Find the last two digits of 4^{1023}.

Note that 4 and 100 do have a common factor!

Solution:

$4^{1023} \bmod 100$

As 4 and 100 have common factors, we will take 25 as modulus.

$4^{1023} \bmod 25$

$4^{1023 \bmod \varnothing(25)} \bmod 25$ ($\varnothing(25) = 20$)

$= 4^3 \bmod 25$ Since $1023 \bmod 20 = 3$

$= 64 \bmod 100$

So last two digits are 64

What are the last two digits of $3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}$ (2011 times) ?

Solution:

We know that ø(100) = 40;

So, we need to compute $3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}$ (2011 time)

and raise 3 to that power.

ø(40) = 16; ø(16) = 8; ø(8) = 4; ø(4) = 2

In particular, $3^k = 3 \bmod 4$ for any value of k.

Working backwards

$3^{3 \bmod \phi(4)} \bmod 4 = 3$ $\quad 3 \bmod \phi(4) = 3 \bmod 2$

$3^3 = 3 \bmod 8$

$3^3 = 11 \bmod 16$

$3^{11} = 27 \bmod 40$

$3^{27} \bmod 100 = 3 \times 3^{26} \bmod 100 = 3 \times (3^{13})^2 \bmod 100$

$= 3 \times (3 \times (3^3)^2)^2)^2 \bmod 100$

$= 87 \bmod 100$

So last two digit = 87

EXTENDED EUCLIDEAN ALGORITHM

(The multiplicative inverse)

3 mod 20

$20 = 3(6) + 2$

$3 = 2(1) + 1$

$2 = 1(2)$

$2 = 20 - 3(6)$

$1 = 3 - 2(1)$

$1 = 3 - 2(1)$

$1 = 3 - [20 - 3(6)]\ (1)$

$1 = 3 - 20(1) + 3(6)$

$1 = 3(7) + 20\ (-1)$

7 is the multiplicative inverse of 3 mod 20

9 mod 26

$26 = 9 * 2 + 8$

$9 = 8(1) + 1$

$8 = 26 – 9(2)$

$1 = 9 – 8(1)$

$1 = 9 – 8(1)$

$1 = 9 – [26 – 9(2)](1)$

$1 = 9(3) + 26(-1)$

Multiplicative inverse of
9 mod 26 is 3

Find integers p and q such that $2322p + 654q = 6$ and also find the GCD(2322, 654).

$2322 = 654(3) + 360$	$360 = 2322 - 654(3)$
$654 = 360(1) + 294$	$294 = 654 - 360(1)$
$360 = 294(1) + 66$	$66 = 360 - 294(1)$
$294 = 66(4) + 30$	$30 = 294 - 66(4)$
$66 = 30(2) + 6(\text{GCD})$	$6 = 66 - 30(2)$
$30 = 6(5) + 0$	

$$6 = 66 - 30(2)$$
$$6 = 66 - [294 - 66(4)](2)$$
$$6 = 66(9) - 294(2)$$
$$6 = [360 - 294(1)](9) - 294(2)$$
$$6 = 360(9) - 294(11)$$
$$6 = 360(9) - [654 - 360(1)](11)$$
$$6 = 360(20) - 654(11)$$
$$6 = [2322 - 654(3)](20) - 654(11)$$
$$6 = 2322(20) - 654(71)$$

Therefore, the values of $p = 20$ and $q = -71$ and GCD = 6.

Find integers p, and q such that 51p + 36q = 3. Also find the GCD (51, 36).

- The identity states for 2 numbers x and y with Greatest Common Divisor g, an equation exists that says g = xp + yq

$51 = 36(1) + 15$	$15 = 51 - 36(1)$
$36 = 15\ (2) + 6$	$6 = 36 - 15(2)$
$15 = 6(2) + \mathbf{3\ (GCD)}$	$3 = 15 - 6(2)$
$6 \ \ = 3(2) + 0$	

$3 = 15 – 6(2)$

$3 = 15 – [36 – 15(2)](2)$

$3 = 15(5) - 36(2)$

$3 = [51 – 36(1)](5) – 36(2)$

$3 = 51(5) - 36(5) - 36(2)$

$3 = 51(5) – 36(7)$

$3 = 51(5) + 36(-7)$

Therefore the values of $p = 5$ and $q = -7$ and GCD = 3.

Chinese Remainder Theorem

Chinese Remainder Theorem

1. Problem first express as a system of congruences

$$p \equiv b_i \pmod{n_i}$$

where n_i are relatively prime numbers: n_1, n_2, n_3 and so on

b_i is the respective remainder for modulo n_i such that b_1 for n_1, b_2 for n_2 and so on.

p is the value of solution.

2. Calculate the value of N

$$N = n_1 * n_2 * \ldots * n_i$$

3. Calculate the value of $N_i = N/n_i$ such that $N_1 = N/n_1$, $N_2 = N/n_2$ and so on

4. Calculate the multiplicative inverse for $y_i \equiv (N_i)^{-1} \pmod{n_i}$

Where y_i is the multiplicative inverse of N_i mod n_i.

5. The value of p is calculated as

$$p \equiv (b_1N_1y_1 + b_2N_2y_2 + \ldots + b_rN_ry_r) \bmod N$$

where p is the solution of the problem.

Find the smallest multiple of 10 which has remainder 1 when divided by 3, remainder 6 when divided by 7 and remainder 6 when divided by 11.

The factors of 10 are: 2 and 5.

Problem is now expressed as a system of congruences as below:

$p \equiv b_i \pmod{n_i}$

where n = 2, 3, 5, 7, and 11 which are relatively prime and **b = 0, 1, 0, 6 and 6** are the remainders for respective value of n.

$p = 0 \bmod 2$,

$p = 1 \bmod 3$,

$p = 0 \bmod 5$,

$p = 6 \bmod 7$

$P = 6 \bmod 11$

To solve for p we get we first calculate the value of N as

$N = n_1 * n_2 * \ldots * n_r$

$N = 2 * 3 * 5 * 7 * 11$

$= 2310$

and find the value of $N_i = N/n_i$ as below:

~~$N_2 = 2310/2 = 1155;$~~

$N_3 = 2310/3 = 770;$

~~$N_5 = 2310/5 = 462;$~~

$N_7 = 2310/7 = 330;$

$N_{11} = 2310/11 = 210$

Now find out the multiplicative inverse as below:

$y_i \equiv (N_i)^{-1} \pmod{n_i}$

~~$y_2 = (1155)^{-1} \pmod 2 = 1$~~

$y_3 = (770)^{-1} \pmod 3 = 2$

~~$y_5 = (462)^{-1} \pmod 5 = 3$~~

$y_7 = (330)^{-1} \pmod 7 = 1$

$y_{11} = (210)^{-1} \pmod{11} = 1$

The solution for above problem is:

$P \equiv b_1N_1y_1 + b_2N_2y_2 + \ldots + b_rN_ry_r \pmod N$,

$p = 0(N_2 * y_2) + 2(N_3 * y_3) + 0(N_5 * y_5) + 6(N_7 * y_7) + 6(N_{11} * y_{11})$

$= \cancel{0(1155)(1)} + 1(770)(2) + \cancel{0(462)(3)} + 6(330)(1) + 6(210)(1)$

$= 0 + 1540 + 0 + 1980 + 1260$

$= 4780 \bmod 2310$

$= 160.$

What is the smallest natural number p with the properties

$p = 1 \bmod 3$

$p = 3 \bmod 8$

$p = 2 \bmod 5$?

Here $n_1 = 3$, $n_2 = 8$ and $n_3 = 5$ and
$b_1 = 1$, $b_2 = 3$ and $b_3 = 2$

$N = n_1 * n_2 * n_3$
$= 3 \times 8 \times 5$
$= 120$

and find the value of $N_i = N/n_i$ as below:
$N_1 = 120/3 = 40$;
$N_2 = 120/8 = 15$;
$N_3 = 120/5 = 24$

Now find out the multiplicative inverse as below:

$y_i \equiv (N_i)^{-1} \pmod{n_i}$

$y_1 = (40)^{-1} \pmod 3 = 1$

$y_2 = (15)^{-1} \pmod 8 = 7$

$y_3 = (24)^{-1} \pmod 5 = 4$

The solution for above problem is:

$P \equiv [b_1N_1y_1 + b_2N_2y_2 + b_3(N_3 * y_3)] \bmod N$

$b_1 = 1$, $b_2 = 3$ and $b_3 = 2$

$N_1 = 40$, $N_2 = 15$, $N_3 = 24$

$y_1 = 1$, $y_2 = 7$, $y_3 = 4$ and $N = 120$

$= 1(40)(1) + 3(15)(7) + 2(24)(4)$

$= 40 + 315 + 19$

$= 547 \bmod 120$

$= 67$

So the solution is 67

An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time, they came out even. What is the smallest number of eggs she could have had?

$P = 1 \pmod 2$

$P = 1 \pmod 3$

$P = 1 \pmod 4$

$P = 1 \pmod 5$

$P = 1 \pmod 6$

$P = 0 \pmod 7$

- $2 = 1 \times 2$
- $3 = 1 \times 3$
- $4 = 1 \times 2 \times 2 = 2^2$
- $5 = 1 \times 5$
- $6 = 1 \times 2 \times 3$
- $7 = 1 \times 7$
- We have to select the factors having highest power.
- So, $2^2 = 4, 3, 5, 7$ are the values of n.

To solve for p we get we first calculate the value of N as

$N = n_1 * n_2 * \ldots * n_r$

$N = 3*4*5*7 = 420$

and find the value of $N_i = N/n_i$ as below:

$N_3 = 420/3 = 140;$

$N_4 = 420/4 = 105;$

$N_5 = 420/5 = 84;$

$N_7 = 420/7 = 60$

Now find out the multiplicative inverse as below:

$y_i \equiv (N_i)^{-1} \pmod{n_i}$

$y_3 = (140)^{-1} \pmod 3 = 2$

$y_4 = (105)^{-1} \pmod 4 = 1$

$y_5 = (84)^{-1} \pmod 5 = 4$

$y_7 = (60)^{-1} \pmod 7 = 2$

The solution for above problem is:

$P \equiv b_1N_1y_1 + b_2N_2y_2 + \ldots + b_rN_ry_r \pmod{N}$,

$p = 1(N_3 * y_3) + 1(N_4 * y_4) + 1(N_5 * y_5) + 0(N_7 * y_7)$

$= 1(140)(2) + 1(105)(1) + 1(84)(4) + 0(60)(2)$

$= 280 + 105 + 336 + 0$

$= 721 \bmod 420$

$= 301$

Solve the simultaneous congruences

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

Here $n_1 = 11$, $n_2 = 16$, $n_3 = 21$ and $n_4 = 25$
$b_1 = 6$, $b_2 = 13$, $b_3 = 9$ and $b_4 = 19$

$N = n_1 * n_2 * n_3 * n_4$
$= 11x\ 16\ x\ 21\ x\ 25$
$= \mathbf{92400}$

and find the value of $N_i = N/n_i$ as below:
$N_1 = 92400/11 = \mathbf{8400}$
$N_2 = 92400/16 = \mathbf{5775}$
$N_3 = 92400/21 = \mathbf{4400}$
$N_4 = 92400/25 = \mathbf{3696}$

Now find out the multiplicative inverse as below:

$y_i \equiv (N_i)^{-1} \pmod{n_i}$

$y_1 = (8400)^{-1} \pmod{11} = 8$

$y_2 = (5775)^{-1} \pmod{16} = 15$

$y_3 = (4400)^{-1} \pmod{21} = 2$

$y_4 = (3696)^{-1} \pmod{25} = 6$

The solution for above problem is:

$$P \equiv [b_1N_1y_1 + b_2N_2y_2 + b_3(N_3 * y_3) + b_4(N_4 * y_4)] \bmod N$$

$b_1 = 6$, $b_2 = 13$, $b_3 = 9$ $b_4 = 19$

$N_1 = 8400$, $N_2 = 5775$, $N_3 = 4400$ $N_4 = 3696$

$y_1 = 8$, $y_2 = 15$, $y_3 = 2$ $y_4 = 6$ and $N = 92400$

$= 6(8400)(8) + 13(5775)(15) + 9(4400)(2) + 19(3696)(6) \bmod 92400$

$= 6 \times 67200 + 13 \times 86625 + 9 \times 8800 + 19 \times 22176$

$= 2029869 \bmod 92400$

$= 51669$

So the solution is 51669

Find a solution using Chinese remainder theorem to 13p = 1 (mod 70)

$70 = 2 \times 5 \times 7$

$13b_1 = 1 \bmod 2$ >> $13b_1 \bmod 2 = 1$ (multiplicative inverse)

$13b_2 = 1 \bmod 5$

$13b_3 = 1 \bmod 7$

Obtaining $b_1 = 1$, $b_2 = 2$, and $b_3 = 6$. Now solve

$p = 1 \pmod 2$

$p = 2 \pmod 5$

$p = 6 \pmod 7$

Here $n_1 = 2$, $n_2 = 5$, $n_3 = 7$

$b_1 = 1$, $b_2 = 2$, $b_3 = 6$

$N = n_1 * n_2 * n_3 * n_4$

$= 2x\ 5\ x\ 7$

$= 70$

and find the value of $N_i = N/n_i$ as below:

$N_1 = 70/2 = \mathbf{35}$

$N_2 = 70/5 = \mathbf{14}$

$N_3 = 70/7 = \mathbf{10}$

Now find out the multiplicative inverse as below:

$y_i \equiv (N_i)^{-1} \pmod{n_i}$

$y_1 = (35)^{-1} \pmod 2 \quad = 1$

$y_2 = (14)^{-1} \pmod 5 \quad = -1$

$y_3 = (10)^{-1} \pmod 7 \quad = 5$

The solution for above problem is:

$P \equiv [b_1N_1y_1 + b_2N_2y_2 + b_3(N_3 * y_3)] \bmod N$

$b_1 = 1, \quad b_2 = 2, \quad b_3 = 6$

$N_1 = 35, \quad N_2 = 14, \quad N_3 = 10$

$y_1 = 1, \quad y_2 = -1, \quad y_3 = 5 \quad$ and $N = 70$

$= 1(35)(1) + 2(14)(-1) + 6(10)(5) \bmod 70$

$= 35 - 28 + 300$

$= 307 \bmod 70$

$= 27 \bmod 70$

So the solution is 27

Find a solution using Chinese remainder theorem to $p^2 = 1 \pmod{144}$

$144 = 16 \times 9 = 2^4 \times 3^2$

GCD (16, 9) = 1

Therefore,

$P^2 = 1 \bmod 16$ having 4 solutions (2^4 here power is 4)

$P = \pm 1$ or $\pm 7 \bmod 16$ ($b_1 \Rightarrow \pm 1, \pm 7$)

$P^2 = 1 \bmod 9$ having 2 solutions (3^2 here power is 2)

$P = \pm 1 \bmod 9$ ($b_1 \Rightarrow \pm 1$)

Obtaining $b_i = \pm 1, \pm 7$.

p = 1 (mod 16)	**p = 1 (mod 9)**
p = 1 (mod 16)	**p = -1 (mod 9)**
p = -1 (mod 16)	**p = 1 (mod 9)**
p = -1 (mod 16)	**p = -1 (mod 9)**
p = 7 (mod 16)	**p = 1 (mod 9)**
p = 7 (mod 16)	**p = -1 (mod 9)**
p = -7 (mod 16)	**p = 1 (mod 9)**
p = -7 (mod 16)	**p = -1 (mod 9)**

Here $n_1 = 16$, $n_2 = 9$

Each case has unique solution for x mod 144

$b_1 = \pm 1, \pm 7$

$N = n_1 * n_2$

$= 16 \times 9$

$= 144$

and find the value of $N_i = N/n_i$ as below:

$N_1 = 144/16 = \mathbf{9}$

$N_2 = 144/9 = \mathbf{16}$

Now find out the multiplicative inverse as below:

$y_i \equiv (N_i)^{-1} \pmod{n_i}$

$y_1 = (9)^{-1} \pmod{16} = 9$

$y_2 = (16)^{-1} \pmod{9} = 4$

The solution for above problem is:

$P \equiv [b_1 N_1 y_1 + b_2 N_2 y_2] \bmod N$

$b_i = \pm 1, \pm 7$

$N_1 = 9, \quad N_2 = 16$

$y_1 = 9, \quad y_2 = 4$

$p = 1(9)(9) + 1(4)(11) \bmod 144$

$= 81 + 64$

$= 145 \bmod 144$

$= 1 \bmod 70$

So the solution is 1

p = 1(9)(9) + (-1)(4)(16) mod 144 **= 81 - 64** **= 17 mod 144** **So the solution is 17**	**p = -1(9)(9) + (1)(4)(16) mod 144** **= -81 + 64** **= -17 mod 144** **So the solution is -17**
p = (-1)(9)(9) + (-1)(4)(16) mod 144 = -81 - 64 = -145 mod 144 **So the solution is -1**	p = (7)(9)(9) + (1)(4)(16) mod 144 = 567 + 64 = 631 mod 144 = 55 mod 144 **So the solution is 55**
p = (7)(9)(9) + (-1)(4)(16) mod 144 = 567 - 64 = 503 mod 144 = 71 mod 144 **So the solution is 71**	p = (-7)(9)(9) + (1)(4)(16) mod 144 = -567 + 64 = -503 mod 144 = -71 mod 144 **So the solution is -71**
p = (-7)(9)(9) + (-1)(4)(16) mod 144 = -567 - 64 = -603 mod 144 = -55 mod 144 **So the solution is -55**	**P = 1, 17, -17, -1, 55, 71, -71, -55**