4. If $n \leq r$, then the number is prime.
5. For $a = 1$ to | sqrt ($\Phi(r)$) $\log(n)$ | do
   if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$, then the number is composite.
6. The number is prime.

6.8 CHINESE REMAINDER THEOREM

According to D. Wells, the problem posed by Sun Tsu (4th century AD) there are certain things whose numbers are not known. Suppose there is some number p which is divided by 2, the remainder is 1, if p is divided by 3, the remainder is 1 and if p is divided by 4, 5 and 6, the remainder is 1. But if it is divided by 7, the remainder is zero. Then what is the smallest value of p. Chinese remainder theorem is used to get the solution of such problem. Using this theorem we get the value of p.

Chinese remainder theorem: There are two relatively prime numbers m and n, which are modulo m and n, the congruence

$$p \equiv a \bmod m$$
$$p \equiv b \bmod n$$

have a unique solution: $p \bmod mn$

Theorem Suppose $n_1, n_2, \ldots, n_r$ are the relatively prime integer numbers and $b_1, b_2, \ldots, b_r$ are the remainders for $n_1, n_2, \ldots, n_r$ respectively. Then the system of congruence, $p \equiv b_i \pmod{n_i}$ for $1 \leq i \leq r$, has a unique solution.

$$N = n_1 * n_2 * \cdots * n_r,$$

which is given by:

$$p \equiv b_1N_1y_1 + b_2N_2y_2 + \cdots + b_rN_ry_r \pmod{N},$$

where $N_i = N/n_i$ and

$$y_i \equiv (N_i)^{-1} \pmod{n_i} \text{ for } 1 \leq i \leq r,$$

where y_i is the multiplicative inverse of $(N_i) \pmod{n_i}$. (Use extended Euclidean algorithm to calculate multiplicative inverse)

Observe that GCD(N_i, n_i) = 1 for $1 \leq i \leq r$. Therefore, all y_i exist. Now, notice that since $N_iy_i \equiv 1 \pmod{n_i}$,

we have $b_iN_iy_i \equiv b_i \pmod{n_i}$ for $1 \leq i \leq r$.

On the other hand, $b_iN_iy_i \equiv 0 \pmod{n_j}$ if $j \neq i$ (since $n_j \mid N_i$ in this case).

Thus, we see that $p \equiv b_i \pmod{n_i}$ for $1 \leq i \leq r$.

If p_0 and p_1 are the solutions, then we would have

$p_0 - p_1 \equiv 0 \pmod{n_i}$ for all i, so $p_0 - p_1 \equiv 0 \pmod{N}$, i.e., they are the same modulo N.

Chinese Remainder Theorem

1. Firstly expressed the problem as a system of congruence,
$$p \equiv b_i (\text{mod } n_i)$$
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
$$N = n_1 * n_2 * \cdots * n_i$$
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 $y_i \equiv (N_i)^{-1} (\text{mod } n_i)$
where y_i is the multiplicative inverse of N_i mod n_i.
5. The value of p is calculated as:
$$p \equiv (b_1 N_1 y_1 + b_2 N_2 y_2 + \ldots + b_r N_r y_r) \text{ mod } N$$
where, p is the solution of the problem.

EXAMPLE 6.30 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.

Solution The factors of 10 are: 2 and 5.
Problem is now expressed as a system of congruence as:
$$p \equiv b_i (\text{mod } n_i)$$
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.

$p = 0 \text{ mod } 2$
$p = 1 \text{ mod } 3$
$p = 0 \text{ mod } 5$
$p = 6 \text{ mod } 7$
$p = 6 \text{ mod } 11$

To solve for p 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:
$$N_2 = 2310/2 = 1155$$
$$N_3 = 2310/3 = 770$$
$$N_5 = 2310/5 = 462$$
$$N_7 = 2310/7 = 330$$
$$N_{11} = 2310/11 = 210$$

Now, find out the multiplicative inverse as:

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

$$y_2 = (1155)^{-1} (\text{mod } 2) = 1$$

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

$$y_5 = (462)^{-1} (\text{mod } 5) = 3$$

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

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

The solution for the above problem is:

$$p \equiv b_1 N_1 y_1 + b_2 N_2 y_2 + \cdots + b_r N_r y_r \ (\text{mod } N),$$

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

$$p = 0(1155)(1) + 1(770)(2) + 0(462)(3) + 6(330)(1) + 6(210)(1)$$

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

$$p = 4780 \text{ mod } 2310 = 160.$$

EXAMPLE 6.31 An old woman purchases a basket of some eggs from the market. While walking on the road she stops for a while and keep her basket of eggs down on the road. A horse running on the road accidentally steps on the basket and crushing all the eggs in the basket. The rider offers to pay the old woman for the damaged eggs. So, he asks her about the total number of eggs she had brought. The old woman does not remember the exact number of eggs in the basket. So she told the rider that when she had taken out two eggs at a time from the basket, there was one egg left. When she had taken out three eggs at a time from the basket, there were two eggs left. When she had taken out five eggs at a time from the basket, there were four eggs left. Find out, the smallest number of eggs an old woman could have had in her basket?

(Above puzzle is mentioned by Oystein Ore taken from Brahma-Sphuta-Siddhanta by Brahmagupta (born 598 AD)):

Solution Problem is now expressed as a system of congruence as:

$$p \equiv b_i \ (\text{mod } n_i)$$

where $n = 2, 3, 5$ and $b = 1, 2, 4$.

$$p = 1 \text{ mod } 2$$

$$p = 2 \text{ mod } 3$$

$$p = 4 \text{ mod } 5$$

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

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

$$N = 2 * 3 * 5 = 30$$

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

$$N_2 = 30/2 = 15$$

$$N_3 = 30/3 = 10$$

$$N_5 = 30/5 = 6$$

Now, find out the multiplicative inverse as:

$$y_i \equiv (N_i)^{-1} (\text{mod } n_i)$$
$$y_2 = (15)^{-1} (\text{mod } 2) = 1$$
$$y_3 = (10)^{-1} (\text{mod } 3) = 2$$
$$y_5 = (6)^{-1} (\text{mod } 5) = 3$$

The solution for the above problem is:

$$p \equiv b_1 N_1 y_1 + b_2 N_2 y_2 + \ldots + b_r N_r y_r (\text{mod } N)$$
$$p = b_2(N_2 * y_2) + b_3(N_3 * y_3) + b_5(N_5 * y_5)$$
$$p = 1(15)(1) + 2(10)(1) + 4(6)(1)$$
$$p = 15 + 20 + 24$$
$$p = 59 \text{ mod } 30 = 29.$$

There are total 29 eggs in the basket.

EXAMPLE 6.32 Monica breeds some pets. She does not know the exact number of pets she has. So she told that when she takes rounds, she observed some things. In the morning there are five pets in each group except one group which has only two pets. In the afternoon there are seven pets in each group except one group which has six pets. In the evening, there are eleven pets in each group. Monica is sure that there are fewer than 150 pets. Find out, the smallest number of pets does she have.

Solution Problem is now expressed as a system of congruence as:

$$p \equiv b_i (\text{mod } n_i)$$

where $n = 5, 7, 11$ and $b = 2, 6, 0$

$$p = 2 \text{ mod } 5$$
$$p = 6 \text{ mod } 7$$
$$p = 0 \text{ mod } 11$$

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

$$N = n_1 * n_2 * \ldots * n_r$$
$$N = 5 * 7 * 11 = 385$$

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

$$N_5 = 385/5 = 77$$
$$N_7 = 385/7 = 55$$
$$N_{11} = 385/11 = 35$$

Now, find out the multiplicative inverse as:

$$y_i \equiv (N_i)^{-1} (\text{mod } n_i)$$
$$y_5 = (77)^{-1} (\text{mod } 5) = 3$$
$$y_7 = (55)^{-1} (\text{mod } 7) = 6$$
$$y_{11} = (35)^{-1} (\text{mod } 11) = 6$$

$77^{-1} \text{ mod } 5 = x \text{ mod } 5$

$1 \text{ mod } 5 = (x \times 77) \text{ mod } 5$

$1 \text{ mod } 5 = (3 \times 77) \text{ mod } 5$

hence $x = 3$

The solution for the above problem is:

$$p \equiv b_1N_1y_1 + b_2N_2y_2 + \ldots + b_rN_ry_r(\text{mod } N),$$
$$p = b_2(N_2 * y_2) + b_3(N_3 * y_3) + b_5(N_5 * y_5)$$
$$p = 2(77)(3) + 6(55)(6) + 0(35)(6)$$
$$p = 462 + 1980 + 0$$
$$p = 2442 \text{ mod } 385$$
$$p = 132$$

There are total 132 pets.

6.9 DISCRETE LOGARITHMS

Discrete logarithms have an important role in Diffie–Hellman and the digital signature algorithms.

From Euler's theorem, for every p and n which are relatively prime we have,

$$p^{\Phi(n)} = 1 \text{ mod}(n)$$

where $\Phi(n)$ is the number of positive integers less than n and relative prime to n.

So in general it is:

$$p^n = 1 \text{ mod } n$$

If p and n are relatively prime, then there is at least one integer n that satisfies above equation.

Suppose $p = 3$ and $n = 13$ are the numbers which are relatively prime. Let us see the power of 3, modulo 13:

$$3^1 = 3 = 3 \text{ mod } 13$$
$$3^2 = 9 = 9 \text{ mod } 13$$
$$3^3 = 27 = 13 * 2 + 1 = 1 \text{ mod } 13$$
$$3^4 = 81 = 13 * 6 + 3 = 3 \text{ mod } 13$$
$$3^5 = 243 = 13 * 18 + 9 = 9 \text{ mod } 13$$

This can prove that $3^3 = 1$ mod 13 and therefore $3^{3+i} = 3^3\ 3^i = 3^i$ mod 13 and hence any two powers of 3 whose exponents differ by 3 are congruent to each other (mod 13).

In general, let F be a finite cyclic group with n elements. We assume that the group is written multiplicatively. Let p be a generator of F; then every element f of F can be written in the form $f = p^k$ for some integer k. Furthermore, any two such integers representing f will be congruent modulo n. We can thus define a function

$$\log_b : F = Z_n$$

(where Z_n denotes the ring of integers modulo n) by assigning to f the congruence class of k modulo n. This function is a group isomorphism, called the *discrete logarithm* to base p.

The familiar base change formula for ordinary logarithms remains valid: If y is another generator of F, then we have

$$\log_y(f) = \log_y(p) \cdot \log_p(f)$$

}

Let p and q be integers, and both are not zero. We know that GCD (p, q) is the greatest common divisor of p and q. Above algorithm gives us the GCD of p and q. We illustrate this theorem using some examples below:

EXAMPLE 6.19 Compute GCD(831, 366) using Euclid's algorithm

Solution

$$831 = 2 * 366 + 265$$
$$366 = 1 * 265 + 101$$
$$265 = 2 * 101 + 63$$
$$101 = 1 * 63 + 38$$
$$63 = 1 * 38 + 25$$
$$38 = 1 * 25 + 13$$
$$25 = 1 * 13 + 12$$
$$13 = 1 * 12 + 1$$
$$12 = 12 * 1 + 0$$

GCD (831, 366) = 1

EXAMPLE 6.20 Compute GCD(2071, 206) using Euclid's algorithm.

Solution

$$2071 = 10 * 206 + 11$$
$$206 = 18 * 11 + 8$$
$$11 = 1 * 8 + 3$$
$$8 = 2 * 3 + 2$$
$$3 = 1 * 2 + 1$$
$$2 = 2 * 1 + 0$$

The GCD(2071, 206) = 1

EXAMPLE 6.21 Compute GCD(2222, 1234) using Euclid's algorithm.

Solution

$$2222 = 1 * 1234 + 988$$
$$1234 = 1 * 988 + 246$$
$$988 = 4 * 246 + 4$$
$$246 = 61 * 4 + 2$$
$$4 = 2 * 2 + 0$$

GCD(2222, 1234) = 2

Example 6.22 Compute GCD(12345, 2345678) using Euclid's algorithm.

Solution

$$2345678 = 190 * 12345 + 128$$
$$12345 = 96 * 128 + 57$$
$$128 = 2 * 57 + 14$$
$$57 = 4 * 14 + 1$$
$$14 = 14 * 1 + 0$$

GCD(12345, 2345678) = 1

6.6.1 Extended Euclidean Algorithm

Suppose p and q are two integer numbers. There exist two integers x and y such that $xp + yq = \text{GCD}(p, q)$. p and b are expressed as trivial combinations: $x = 1x + 0y$ and $y = 0x + 1y$. Now, use extended Euclidean algorithm to find the value of x and y.

Write the two linear combinations vertically as shown below and apply Euclid's algorithm to get $g = \text{GCD}(p, q)$ and the values of x and the y to satisfy the equation $xp + yq = g$.

$$x = 1 \cdot x + 0 \cdot y$$
$$y = 0 \cdot x + 1 \cdot y$$
$$r = 1 \cdot x + (-z) \cdot y$$

Extended Euclidean Algorithm

1. Enter two positive integer numbers p and q such that $p \geq q$.
2. If $q = 0$ then $r = p$, $x_1 = 1$, $y_1 = 0$, and return(r, x_1, y_1).
3. If $q > 0$, do
   (a) $z = p/q$, $r = p \bmod q$, $x_1 = x_3 - zx_2$, $y_1 = y_3 - zy_2$.
   (b) $p = q$, $q = r$, $x_3 = x_2$, $x_2 = x_1$, $y_3 = y_2$, $y_2 = y_1$.
4. $g = p$, $x_1 = x_3$, $y_1 = y_3$, and return (g, x_1, y_1).
5. Print g, x_1 and y_1

EXAMPLE 6.23 Find integers p and q such that $2322p + 654q = 6$ and also find the GCD(2322, 654).

Solution The identity states for 2 numbers x and y with greatest common divisor g, an equation exists that says $g = xp + yq$.

i	x math*	x_i	y math	y_i	r math	r	z math	z
1	Set to 1	1	Set to 0	0		2322		
2	Set to 0	0	Set to 1	1		654	Quotient of 2322/654	3
3	$1 - (3 * 0)$ $x_1 - z_2 * x_2$	1	$0 - (3 * 1)$ $y_1 - z * y_2$	–3	Remainder of 2322/654	360	Quotient of 654/360	1
4	$0 - (1 * 1)$ $x_2 - z_3 * x_3$	–1	$1 - (1 * -3)$ $y_2 - z * y_3$	4	Remainder of 654/360	294	Quotient of 360/294	1
5	$1 - (1 * -1)$ $x_3 - z_4 * x_4$	2	$-3 - (1 * 4)$ $y_3 - z * y_4$	–7	Remainder of 360/294	66	Quotient of 294/66	4
6	$-1 - (4 * 2)$ $x_4 - z_5 * x_5$	–9	$4 - (4 * -7)$ $y_4 - z * y_5$	32	Remainder of 294/66	30	Quotient of 66/30	2
7	$2 - (2 * -9)$ $x_5 - z_6 * x_6$	20	$-7 - (2 * 32)$ $y_5 - z * y_6$	–71	Remainder of 66/30	6	Quotient of 30/6	5
					Remainder of 30/6	0		

*Math indicates the mathematical computations for the values of x, y, z and r.

By taking the last non-zero row, we get: $x = 20$ and $y = -71$ and GCD = 6.

Therefore, $20 * 2322 - 71 * 654 = 6$.

Here, 20 and 71 are relatively prime numbers. This is true for $xm + yn = \text{GCD}(x, y)$.

Note: For the above example, this is not the unique solution. But this method gives the simplest solution.

Alternative Method

$2322p + 654q = 6$

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