Euclidean Algorithm

Fact 01 : $\gcd(a,0) = a$

Fact 02 : $\gcd(a,b) = \gcd(b,r)$ $\quad [r = a\%b]$

Ex: $\gcd(36,10) = \gcd(10,6) = \gcd(6,4) = \gcd(4,2)$

$= \gcd(2,0) = 2$

Algorithm :

```
r1 ← a , r2 ← b
while(r2 > 0)
{
    q ← r1/r2
    r ← r1 − q × r2
    r1 ← r2
    r2 ← r
}
gcd(a,b) ← r1
```

When $\gcd(a,b) = 1$ we say that a & b are relatively prime.

Ex 01 : GCD(2740, 1760) = ?

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

$\therefore$ GCD (2740, 1760) = 20

Ex02 : GCD(25, 60) = ?

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

GCD (25, 60) = 5

Extended Euclidean Algorithm

Given two integers a and b

we often need to find other two integers

s & t such that

$$s \times a + t \times b = \gcd(a,b)$$

Algorithm:

$r_1 \leftarrow a, \; r_2 \leftarrow b$

$s_1 \leftarrow 1, \; s_2 \leftarrow 0$

$t_1 \leftarrow 0, \; t_2 \leftarrow 1$

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2$

$r \leftarrow r_1 - q \times r_2$

$r_1 \leftarrow r_2$

$r_2 \leftarrow r$

$s \leftarrow s_1 - q \times s_2$

$s_1 \leftarrow s_2$

$s_2 \leftarrow s$

$t \leftarrow t_1 - q \times t_2$

$t_1 \leftarrow t_2$

$t_2 \leftarrow t$

}

$\gcd(a, b) \leftarrow r_1$

$s \leftarrow s_1$

$t \leftarrow t_1$

Ex 03 : $\gcd(161, 28) = ?$ $s = ?$ $t = ?$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

$\therefore \gcd(161, 28) = 7$

$s = -1$

$t = 6$

$-1 \times 161 + 6 \times 128 = 7$

Given $a = 0$ and $b = 45$, find gcd (a, b) and the values of s and t.

Solution

We use a table to follow the algorithm.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	0	45	0	1	0	1	0	1	0
	45	0		0	1		**1**	0	

We get gcd $(0, 45) = 45$, $s = 0$, and $t = 1$. This indicates why we should initialize s_2 to 0 and t_2 to 1.

Given $a = 17$ and $b = 0$, find gcd (a, b) and the values of s and t.

Solution

We use a table to follow the algorithm.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	17	0		1	0		0	1	

Note that we need no calculation for q, r, and s. The first value of r_2 meets our termination condition. We get gcd $(17, 0) = 17$, $s = 1$, and $t = 0$. This indicates why we should initialize s_1 to 1 and t_1 to 0. The answers can be tested as shown below:

Multiplicative Inverse

In Z_n, two numbers a and b are the multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

Ex: $3 \times 7 \equiv 1 \pmod{10}$

If the modulus is 10, then the multiplicative inverse of 3 is 7.

'a' has a multiplicative inverse in Z_n if and only if $\gcd(n, a) = 1$

Ex: There is no multiplicative inverse of 8 in Z_{10} because $\gcd(10, 8) = 2 \neq 1$.

The extended euclidean algo finds the multiplicative inverse of b in Z_n when n and b are given and $\gcd(n, b) = 1$.

The multiplicative inverse of b is the value of t after being mapped to Z_n.

Algorithm :

$r_1 \leftarrow n$, $r_2 \leftarrow b$

$t_1 \leftarrow 0$, $t_2 \leftarrow 1$

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2$

$r \leftarrow r_1 - q \times r_2$

$r_1 \leftarrow r_2$

$r_2 \leftarrow r$

$t \leftarrow t_1 - q \times t_2$

$t_1 \leftarrow t_2$

$t_2 \leftarrow t$

}

if $(r_1 == 1)$ then $b^{-1} \leftarrow t_1$

Ex 04 : Find the multiplicative inverse of 11 in Z_{26}.

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	

$\gcd(26, 11) = 1 \rightarrow$ M.I. exists

$t_1 = -7$

$\therefore$ M.I $= (-7) \bmod 26 = 19$

$\therefore$ 11 and 19 are multiplicative inverse in Z_{26}.

$(11 \times 19) \bmod 26 = 1$

Euler's Totient Function

$\phi(n) \rightarrow$ Finds the number of integers that are both smaller than n and relatively prime to n.

Rule 01: $\phi(1) = 0$

Rule 02: $\phi(p) = p-1$ if p is prime

Rule 03: $\phi(mn) = \phi(m) \times \phi(n)$

if m and n are relatively prime

Rule 04: $\phi(p^e) = p^e - p^{e-1}$ if p is prime.

If $n = p_1^{e_1} \times p_2^{e_2} \times p_3^{e_3} \times \ldots \times p_k^{e_k}$

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdot (p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

Ex 05: $\phi(13) = 13-1 = 12$

$$\phi(10) = \phi(2 \times 5) = \phi(2) \times \phi(5)$$
$$= 1 \times 4 = 4$$

$$\phi(240) = \phi(2^4 \times 3^1 \times 5^1)$$
$$= (2^4 - 2^3) \cdot (3^1 - 3^0) \cdot (5^1 - 5^0)$$
$$= 8 \times 2 \times 4 = 64$$

Fermat's Little Theorem

First version:

If p is a prime and a is an integer such that p does not divide a then

$$a^{p-1} \equiv 1 \mod p$$

Second version:

If p is a prime and a is an integer then

$$a^{p} \equiv a \mod p$$

Ex 06:

$$6^{10} \mod 11 = 6^{11-1} \mod 11 = 1$$

$$\begin{aligned} 3^{12} \mod 11 &= (3^{11} \times 3) \mod 11 \\ &= (3^{11} \mod 11)(3 \mod 11) \\ &= (3 \times 3) \mod 11 \\ &= 9 \end{aligned}$$

Multiplicative Inverse using F.L.T

If p is a prime and a is an integer such that p does not divide a then

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

Ex07:
$$8^{-1} \bmod 17 = 8^{17-2} \bmod 17$$
$$= 8^{15} \bmod 17$$
$$= 15$$

$$5^{-1} \bmod 23 = 5^{23-2} \bmod 23$$
$$= 5^{21} \bmod 23$$
$$= 14$$

Euler's Theorem

First Version:

If a and n are coprime, then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Second Version:

If $n = p \times q$, $a < n$, K is an integer

then $$a^{K\phi(n)+1} \equiv a \pmod n$$

Ex 08: $6^{24} \bmod 35 = 6^{\phi(35)} \bmod 35$

$= 1$

$20^{62} \bmod 77 = (20 \bmod 77)\left(20^{\phi(77)+1} \bmod 77\right) \bmod 77$

$= (20 \times 20) \bmod 77$

$= 15$

Multiplicative Inverse Using Euler's Theorem

If n and a are coprime then,

$$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$$

Ex 09: $8^{-1} \bmod 77 = 8^{\phi(77)-1} \bmod 77 = 8^{59} \bmod 77$

$= 29 \bmod 77$

$71^{-1} \bmod 100 = 71^{\phi(100)-1} \bmod 100 = 71^{39} \bmod 100$

$= 31 \bmod 100$

$$\boxed{ax \equiv b \pmod{n}}$$

If $\gcd(a, n) = d$

↳ if d does not divide b, there is no solution.

→ if d divides b, there are d solutions.

Let us see how we can solve equations involving a single variable—that is, equations of the form $ax \equiv b \pmod{n}$. An equation of this type might have no solution or a limited number of solutions. Assume that the gcd $(a, n) = d$. If $d \nmid b$, there is no solution. If $d|b$, there are d solutions.

If $d|b$, we use the following strategy to find the solutions:

1. Reduce the equation by dividing both sides of the equation (including the modulus) by d.
2. Multiply both sides of the reduced equation by the multiplicative inverse of a to find the particular solution x_0.
3. The general solutions are $x = x_0 + k\,(n/d)$ for $k = 0, 1, \ldots, (d - 1)$.

__Ex-01:__ $10x \equiv 2 \pmod{15}$

Sol^n: $\gcd(10, 15) = 5$ and 5 does not divide 2

$\therefore$ There is no solution.

__Ex-02:__ $14x \equiv 12 \pmod{18}$

Sol^n: $\gcd(14, 18) = 2$ and 2 divided 12.

$\therefore$ We have exactly 2 solutions.

Now,

$$14x \equiv 12 \pmod{18}$$

$$\Rightarrow 7x \equiv 6 \pmod{9}$$

$$\Rightarrow x = 6(7^{-1}) \pmod{9}$$

$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \bmod 9 = 6$

$x_1 = x_0 + 1 \times (18/2) = 6 + 9 = 15$

Ans: $6, 15$

Ex-03: $3x + 4 \equiv 6 \pmod{13}$

$\Rightarrow 3x \equiv 2 \pmod{13}$

$\gcd(3, 13) = 1$ and 1 divides 2.

We have exactly 1 solution.

Now,

$3x \equiv 2 \pmod{13}$

$\Rightarrow x = (2 \times 3^{-1}) \bmod 13$

$\Rightarrow x = (2 \times 9) \bmod 13$

$\Rightarrow x = 5$

(Ans)

Ex 04: $12x \equiv 17 \pmod{19}$

$\gcd(12, 19) = 1$ and 1 divides 17.

We have exactly 1 solution.

Now,

$12x \equiv 17 \pmod{19}$

$\Rightarrow x = (17 \times 12^{-1}) \bmod 19$

$\Rightarrow x = (17 \times 8) \bmod 19$

$\therefore x = 3$

Time complexity of Euclidean & Extended Euclidean Algorithm $= O(\log(\min(a,b)))$

BINARY GCD

```
function binaryGCD(int u, int v) {
    //simple termination cases
    if v equals 0 : return u;
    if u equals 0 : return v;

// If u and v are both even, then gcd(u, v) = 2·gcd(u/2, v/2), because 2 is a common divisor
    if ((u is even) and (v is even)){
        return binaryGCD(u >> 1, v >> 1) << 1;
    }

// If u is even and v is odd, then gcd(u, v) = gcd(u/2, v), because 2 is not a common divisor
    else if (u is even){
        return binaryGCD(u >> 1, v);
    }

// If u is odd and v is even, then gcd(u, v) = gcd(u, v/2)
    else if (v is even){
        return binaryGCD(u, v >> 1);
    }

// If u and v are both odd, and u ≥ v, then gcd(u, v) = gcd((u − v)/2, v)
    else if (u >= v){
        return binaryGCD((u-v) >> 1, v);
    }

// If both are odd and u < v, then gcd(u, v) = gcd((v − u)/2, u)
    else{
        return binaryGCD(u, (v-u) >> 1);
    }
}
```

ANY 2 CONSECUTIVE FIBONACCI NUMBERS ARE RELATIVELY PRIME :-

Proof : In order to prove that

$\gcd(F_n, F_{n+1}) = 1$

We must first know that $\gcd(a, a+b) = \gcd(a, b)$

Suppose d is a divisor of both a and $a+b$.

$\therefore \quad a = dk, \quad a+b = dj$

$\Rightarrow b = dj - a$

$\Rightarrow b = dj - dk$

$\Rightarrow b = d(j-k)$

$\therefore d$ is also a divisor of b.

It means that

$$d \mid a \text{ and } d \mid a+b \Rightarrow d \mid a \text{ and } d \mid b$$

$$d \mid a \text{ and } d \mid b \Rightarrow d \mid a \text{ and } d \mid a+b$$

for any divisor d.

$\therefore \gcd(a, a+b) = \gcd(a, b)$

Now the real proof:

Base Case: $\gcd(F_0, F_1) = \gcd(0, 1) = 1$

$\therefore F_0$ and F_1 are relatively prime.

Inductive Step:

For the inductive hypothesis, we assume that

$\gcd(F_K, F_{K+1}) = 1$

We have to prove that $\gcd(F_{K+1}, F_{K+2}) = 1$.

Now,

$$\gcd(F_{K+1}, F_{K+2}) = \gcd(F_{K+1}, F_{K+1} + F_K)$$

$$= \gcd(F_{K+1}, F_K)$$

$$= \gcd(F_K + F_{K+1})$$

$$= 1$$

[Voila]

⊞ What does Extended Euclid (F_K, F_{K+1}) return?

Sol^n:

Proposition $P(n)$: For all $n \geq 2$,

$$\gcd(F_n, F_{n+1}) = \underbrace{\left[(-1)^n F_{n-1}\right]}F_n + \underbrace{\left[(-1)^{n+1} F_{n-2}\right]}F_{n+1} = 1$$

Extended Euclid will return these two.

Base Case:

For $n=2$, $\gcd(F_2, F_3) = \left[(-1)^2 F_{2-1}\right] F_2 + \left[(-1)^{2+1} F_{2-2}\right] F_{2+1}$

$\Rightarrow \gcd(1,2) = F_1 F_2 + (-1) F_0 F_3$

$\Rightarrow \gcd(1,2) = 1 \times 1 - 1 \times 0 \times 2$

$\Rightarrow \gcd(1,2) = 1$

$\therefore$ Base Case holds.

Inductive Hypothesis:

Let $P(K)$ is true, that is,

$$1 = \gcd(F_K, F_{K+1}) = \left[(-1)^K F_{K-1}\right] F_K + \left[(-1)^{K+1} F_{K-2}\right] F_{K+1} \quad \text{—(1)}$$

and we have to prove that $P(K+1)$ is also true.
That is, we need prove,

$$\gcd(F_{K+1}, F_{K+2}) = \left[(-1)^{K+1} F_K\right] F_{K+1} + \left[(-1)^{K+2} F_{K-1}\right] F_{K+2}$$
$$= 1$$

We know that, $F_{K+2} = F_{K+1} + F_K$

From (1) =>

$$1 = [(-1)^K F_{K-1}](F_{K+2} - F_{K+1}) + [(-1)^{K+1} F_{K-2}] F_{K+1}$$

$$= F_{K+1}\left((-1)^{K+1} F_{K-2} + (-1)^{K+1} F_{K-1}\right) + F_{K+2}\left((-1)^K F_{K-1}\right)$$

$$= F_{K+1} (-1)^{K+1} (F_{K-2} + F_{K-1}) + F_{K+2} \left((-1)^K F_{K-1}\right)$$

$$= F_{K+1} (-1)^{K+1} F_K + F_{K+2} \left((-1)^K F_{K-1}\right)$$

$$= [(-1)^{K+1} F_K] F_{K+1} + [(-1)(-1)(-1)^K F_{K-1}] F_{K+2}$$

$$= [(-1)^{K+1} F_K] F_{K+1} + [(-1)^{K+2} F_{K-1}] F_{K+2}$$

$\therefore$ P(K+1) also holds.

[Proved]

[All CREDIT GOES TO MAHADI HASAN]

RSA

```
RSA_Key_Generation
{
    Select two large primes p and q [p ≠ q]
    n ← p × q
    φ(n) ← (p−1)(q−1)
    Select e such that 1 < e < φ(n) and
            e is coprime to φ(n)
    d ← e^{-1} mod φ(n)
    Public key ← (e, n)
    Private key ← d
}
```

```
RSA_Encryption (P, e, n)
{
    C ← P^e mod n
}
```

```
RSA_Decryption (C, d, n)
{
    P ← C^d mod n
}
```

☐ RSA would be trivial to crack knowing the factorization into two primes of n in the public key, explain why RSA would be trivial to crack knowing $\phi(n)$.

<u>Solⁿ</u>:

$$\phi(n) = (p-1)(q-1) = pq - q - p + 1$$

$$= (n+1) - (p+q)$$

$$(n+1) - \phi(n) - p = q \quad \text{--- (1)}$$

Now, $n = pq \Rightarrow n = p\left(n+1-\phi(n)-p\right)$ [from (1)]

$$\Rightarrow n = -p^2 + (n+1-\phi(n))\,p$$

$$\Rightarrow p^2 - (n+1-\phi(n))\,p + n = 0$$

$$\therefore p = \frac{n+1-\phi(n) \pm \sqrt{(n+1-\phi(n))^2 - 4n}}{2}$$

because of symmetry, the two solutions for p will be the two prime factors of n.

Here is a short example:

Let $n = 13 \times 29 = 377$

$$\phi(n) = (13-1)(29-1) = 336$$

$$\therefore p = \frac{377+1-336 \pm \sqrt{(377+1-336)^2 - 4\times 377}}{2}$$

$$= \frac{42 \pm 16}{2} = 13, 29$$

In conclusion, knowledge of $\phi(n)$ allows one to factor n in time $O(1)$.

4. Consider an RSA key set with $p = 11$, $q = 29$, $n = 319$ and $e = 3$. What value of d should be used in the secret key? What is the encryption of the message $M = 100$?

<u>Sol</u>

Sol^n:

$$d = e^{-1} \bmod \phi(n)$$

$$= e^{-1} \bmod (p-1)(q-1)$$

$$= 3^{-1} \bmod 280$$

$\therefore \; d = 187$ [use Extended Euclid]

Now,

message $M = 100$

$$C = M^e \bmod n = 100^3 \bmod 319$$

$$= 254$$

In an RSA cryptosystem, a particular user uses two prime numbers $p = 13$ and $q = 17$ to generate his public and private keys. If the public key is 35, then the private key is = ?

Sol^n:

$e = 35$

$$d = e^{-1} \bmod \phi(n) = 35^{-1} \bmod (13-1)(17-1)$$

$$= 35^{-1} \bmod 192$$

q	r_1	r_2	r	t_1	t_2	t
5	192	35	17	0	1	-5
2	35	17	1	1	-5	11
17	17	1	0	-5	11	-192
	1	0		11	-192	

$\therefore \; d = 35^{-1} \bmod 192 = 11$

(Ans)