The Euclidean Algorithm

Recall that the Greatest Common Divisor (GCD) of two integers A and B is the largest integer that divides both A and B.

The Euclidean Algorithm is a technique for quickly finding the GCD of two integers.

The Algorithm

The Euclidean Algorithm for finding GCD(A,B) is as follows:

If A = 0 then GCD(A,B)=B, since the GCD(0,B)=B, and we can stop.

If B = 0 then GCD(A,B)=A, since the GCD(A,0)=A, and we can stop.

Write A in quotient remainder form (A = B⋅Q + R)

Find GCD(B,R) using the Euclidean Algorithm since GCD(A,B) = GCD(B,R)

Example:

Find the GCD of 270 and 192

A=270, B=192

Use long division to find that 270/192 = 1 with a remainder of 78. We can write this as: 270 = 192 * 1 +78

Find GCD(192,78), since GCD(270,192)=GCD(192,78)

A=192, B=78

Use long division to find that 192/78 = 2 with a remainder of 36. We can write this as:

192 = 78 * 2 + 36

Find GCD(78,36), since GCD(192,78)=GCD(78,36)

A=78, B=36

Use long division to find that 78/36 = 2 with a remainder of 6. We can write this as:

78 = 36 * 2 + 6

Find GCD(36,6), since GCD(78,36)=GCD(36,6)

A=36, B=6

Use long division to find that 36/6 = 6 with a remainder of 0. We can write this as:

36 = 6 * 6 + 0

Find GCD(6,0), since GCD(36,6)=GCD(6,0)

A=6, B=0

A ≠0

B =0, GCD(6,0)=6

So we have shown:

GCD(270,192) = GCD(192,78) = GCD(78,36) = GCD(36,6) = GCD(6,0) = 6

GCD(270,192) = 6

Fermat's Theorem

Fermat's theorem states the following: If *p* is prime and *a* is a positive integer not divisible by *p*, then

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

$p = 5, a = 3$, $a^{p-1} = 3^4 = 81 \equiv 1 \pmod 5$

this theorem requires that *a* be relatively prime to *p*

An alternative form of Fermat's theorem is also useful: If *p* is prime and *a* is a positive integer, then

$a^p \equiv a \pmod p$

$p = 5, a = 3$, $a^p = 3^5 = 243 \equiv 3 \pmod 5 = a \pmod p$

$p = 5$, $a = 10$ $a^p = 10^5 = 100000 \equiv 10 \pmod 5 = 0 \pmod 5 = a \pmod p$

Euler's Totient Function

Before presenting Euler's theorem, we need to introduce an important quantity in number theory, referred to as Euler's totient function and written $\phi(n)$, **defined as the number of positive integers less than *n* and relatively prime to *n*.** By convention, $\phi(1) = 1$

Determine $\phi(37)$ and $\phi(35)$.

Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus $\phi(37) = 36$.

To determine $\phi(35)$, we list all of the positive integers less than 35 that are relatively prime to it:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18,

19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

There are 24 numbers on the list, so $\phi(35) = 24$.

It should be clear that for a prime number *p*,

$\boldsymbol{\phi(p) = p-1}$

Now suppose that we have two prime numbers *p* and *q*, with *p. q*. Then we can show that for $n = p.q$,

$\boldsymbol{\phi(n) = \phi(p.q) = \phi(p) \times \phi(q) = (p - 1) \times (q - 1)}$

$\phi(21) = \phi(3) \times \phi(7) = (3 - 1) \times (7 - 1) = 2 \times 6 = 12$

where the 12 integers are {1,2,4,5,8,10,11,13,16,17,19,20}

when n is prime number, m any integer number

$\boldsymbol{\phi(n^m) = \phi(n^{m-1}) \times (n-1)}$

$\phi(16) = \phi(2^4) = 2^3 \times 1 = 8$

Where the 8 integers are {1,3,5,7,9,11,13,15}

Example:

Find $\phi(24)$, $\phi(100)$, $\phi(57)$

$\phi(24)= \phi(3)* \phi(8)= \phi(3)* \phi(2^3)=2*2^2*1=8$;; $\phi(24)= \phi(4*6)= \phi(2^2*2*3)= \phi(2^3*3)=8$

$\phi(100)= \phi(25*4)= \phi(5^2)* \phi(2^2)=5*4*2*1=40$

$\phi(57)= \phi(19*3)=18*2=36$

Inverse computation

1-where ϕ is Euler's totient function. *a* is coprime to *m*. Therefore, a modular multiplicative inverse can be found directly:

$\mathbf{a^{\phi(m)-1}=a^{-1}}$

Example:

find 3x =1 (mod 10)

$a = 3$; $m = 10$; $\phi(10) = 4$;

x= 3^{4-1} mod 10=7

3*7 mod 10=1

2-in the special case where *m* is a prime, $\phi(m)=m-1$, and a modular inverse is given by

$\mathbf{a^{m-2}=a^{-1}}$

$\mathbf{a^{-1}=a^{m-2}}$

Example:
Find 2x=1 (mod 11)
$a = 2$; $m = 11$
x=$2^{11-2}=2^9$ mod 11=6
2*6 mod 11=1
3-Extended Euclidean algorithm

Example:
17x=1 mod 43

43=17*2+9	9=43-17*2
17=9*1+8	8=17-9*1
9=8*1=1	1=9-8*1
8=1*8+0	

8=17-9*1
1=9-(17-9*1)
1=9-17+9
1=2*9-17
1=2(43-17*2)-17
1=2*43-4*17-17
1=2*43-5*17
X=-5 mod 43   x=43-5=38
17*38 mod 43=1
Note: if you have (3^7 mod 5)
3^7mod 5=((3^2 mod 5)*(3^2 mod 5)*(3^2 mod 5)*(3 mod 5))mod 5=(4*4*4*3) mod 5=192 mod 5 = 2