10/17/16 (1)

Euler ϕ function

✓ $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$ [if p is prime]

☐ if $\gcd(a,b) = 1$, then $\phi(ab) = \phi(a)\cdot\phi(b)$, multiplicative function.

$\phi(2^4 3^5 7^1) = \phi(2^4)\phi(3^5)\phi(7^1)$

$= (2^4 - 2^3)(3^5 - 3^4)(7^1 - 7^0)$

$= 8 \times 162 \times 6$

Calculate $\phi(ab)$

1 2 3 . . . ~~a~~

a+1 a+2 a+3 . . ~~2a~~

2a+1 2a+2 2a+3 . . . ~~3a~~

X

X

~~(b-1)a~~ b=6

(b-1)a+1

b ~~last~~ rows 6

a columns 7

ab # values

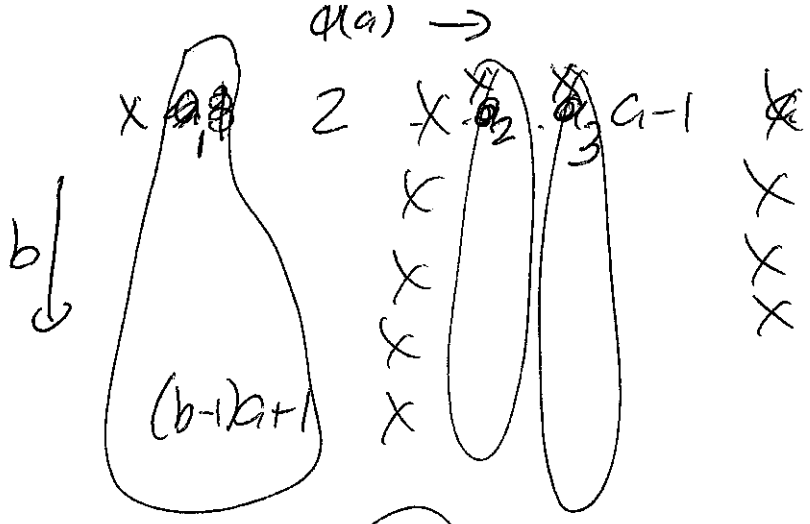
$\phi(a) = 6$

1	~~2~~	3	~~4~~	5	6	~~7~~
~~8~~	~~9~~	10	11	12	13	~~14~~
15	~~16~~	17	~~18~~	19	20	~~21~~
22	23	24	25	26	27	~~28~~
29	~~30~~	31	~~32~~	33	34	~~35~~
36	37	38	~~39~~	40	41	~~42~~

How many factor share with 6?

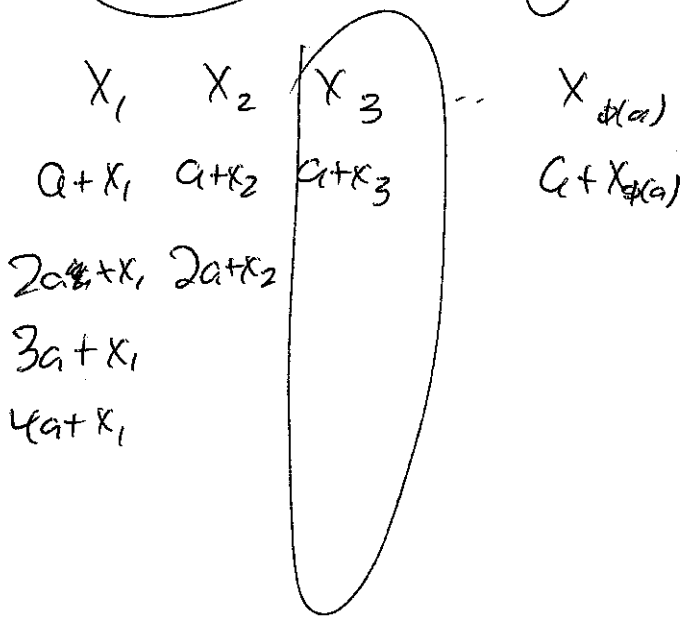
Cross of b values that are multiples of a. (There might be more that SHARE factors with a,)

MORE GENERALLY only $\phi(a)$ columns DON'T get cross off. We are left with $\phi(a) \times b$ values.



Top labels are $x_1, x_2, x_3, \ldots, x_{\phi(a)}$.

$\gcd(x_i, a) = 1$



Investigate an arbitrary column:

$x_k, a+x_k, 2a+x_k, \ldots (b-1)a+x_k$

HOW MANY SHARE A COMMON FACTOR WITH b?

THERE ARE b values in the list.

I will prove that each value in the list is inequivalent mod b. Prove that NO TWO VALUES are equivalent mod b.

$$x_k + ai \equiv x_k + aj \pmod{b}, \quad i \neq j, \quad 0 \leq i, j < b$$

$$ai - aj \equiv 0 \pmod{b}$$

$$a(i-j) \equiv 0 \pmod{b}$$

if $\gcd(a,b) = 1$ and $b \mid (ac)$, then $b \mid c$.

$\Rightarrow \gcd(a,b) = 1$, then $b \mid (i-j)$

↳ Contradicts fact $0 < |i-j| < b$

In every column $\phi(b)$ values survive. $\Rightarrow \phi(ab) = \phi(a)\phi(b)$.

$$\phi(n) = \phi\left(\prod_{p_i \in Prime} p_i^{k_i}\right) = \prod_{\substack{k_i > 0 \\ p_i \in Prime}} \left(p_i^{k_i} - p_i^{k_i - 1}\right)$$

$$= \prod_{\substack{k_i > 0 \\ p_i \in Prime}} p_i^{k_i}\left(1 - \frac{1}{p_i}\right)$$

$$= \prod_{\substack{k_i > 0 \\ p_i \in Prime}} p_i^{k_i} \times \prod_{\substack{k_i > 0 \\ p_i \in Prime}} \left(1 - \frac{1}{p_i}\right)$$

$$\phi(n) = n \prod_{\substack{k_i > 0 \\ p_i \in Prime}} \left(1 - \frac{1}{p_i}\right) = n \prod_{\substack{k_i > 0 \\ p_i \in Prime}} \left(\frac{p_i - 1}{p_i}\right)$$

$$\phi(2^4 3^5 7^1) = 2^4 \times 3^5 \times 7^1 \left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{6}{7}\right)^2$$

$$= \frac{2^4 \times 3^5 \times 7^1 \times 2}{7} = \boxed{2^5 \times 3^5}$$

Euler's Thm

If $\gcd(a,n)=1$ then $a^{\phi(n)} \equiv 1 \bmod n$.

If n is prime, then $\phi(n)=n-1 \Rightarrow$ Fermat's Thm

So, Fermat's Thm is a special case of Euler's Thm!!!

$n=15$ $a=4$

$\phi(n)=8$

$S = \{x_1, x_2, x_3, \ldots, x_{\phi(n)}\}$

where all x_i are in btw 1 and $a-1$ and $\gcd(x_i, n)=1$.

$S=\{1,2,4,7,8,11,13,14\}$

$T = \{ax_1, ax_2, ax_3, \ldots ax_{\phi(n)}\}$ $T=\{4,8,16,28,32,44,52,56\}$

Calculate values of $T \bmod n$ $\{4,8,1,13,2,14,7,11\}$

Prove all values in T unique mod n.

$\gcd(n, ax_i)=1$ for all x_i.

Use proof by contradiction (to prove all unique)

$$ax_i \equiv ax_j \pmod n$$

$$ax_i - ax_j \equiv 0 \pmod n$$

$$a(x_i - x_j) \equiv 0 \pmod n$$

Since $\gcd(a,n)=1$, $\Rightarrow n \mid (x_i - x_j)$

Since $x_i \neq x_j$, $0 < x_i, x_j < n$

$\hookrightarrow 0 < |x_i - x_j| < n-1$

CONTRADICTION!

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

product of S ↘ ↙ product of T

$$\prod_{i=1}^{\phi(n)} ax_i - \prod_{i=1}^{\phi(n)} x_i \equiv 0 \pmod n$$

$$\prod_{i=1}^{\phi(n)} a \cdot \prod_{i=1}^{\phi(n)} x_i - \prod_{i=1}^{\phi(n)} x_i \equiv 0 \pmod n$$

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i - \prod_{i=1}^{\phi(n)} x_i \equiv 0 \pmod n$$

$$\left(\prod_{i=1}^{\phi(n)} x_i\right)\left(a^{\phi(n)} - 1\right) \equiv 0 \pmod n$$

all relatively prime to n ↑

So $\gcd\left(n, \prod_{i=1}^{\phi(n)} x_i\right) = 1$

Thus, $n \mid \left(a^{\phi(n)} - 1\right)$

$$\Rightarrow a^{\phi(n)} - 1 \equiv 0 \pmod n$$

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

Primality Testing

```
for (i=2; i<Math.sqrt(n)+.1; i++)
    if (n%i == 0)
        return false;
return true;
```

If d/o were O(1), this is $O(\sqrt{n})$

Way too slow for large integers with many (24-1000) digits.

Fermat's Thm

If p is prime and $\gcd(a,p)=1$,

then $a^{p-1} \equiv 1 \bmod p$.

↳ tends to be false for most composites.

Idea: ~~Guess~~ Generate a random a.

Calculate $a^{n-1} \bmod n$. If you DON'T get 1, it's composite.

(Check $\gcd(a,n)$ - if it's not 1, n isn't prime)

Try 100 random values of a. If ALL of them pass, say, "IT'S PROBABLY PRIME"

↳ for most numbers n, if n is composite, for over $1/2$ of all possible a's, $a^{n-1} \not\equiv 1 \bmod n$.

561 Chance the algorithm is wrong is $\left(\frac{1}{2}\right)^{100}$.

Carmichael Numbers → "fake" primes, for all a's $a^{n-1} \equiv 1 \bmod n$, but n is composite.

if p is prime, $a^{p-1} \equiv 1 \bmod p$

also $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$

$a^{\frac{p-1}{4}}$?

$a^{\frac{p-1}{8}}$? etc.

1
1
+1
-1

Miller Rabin says I HAVE to see this -1.

Only exception is if sequence starts spitting out 1s from the start.

Looked at wiki pages for:

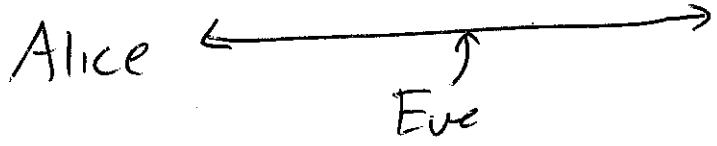
Carmichael Numbers
Miller-Rabin Primality Test
Mersenne Primes* (not required)

Look at code:

MillerRabin.java
DiscLog.java

1976 → Diffie-Hellman Key Exchange,

1977 → RSA Encryption



One-way functions (easy calculate forward, hard to undo, invert)

1972 Clifford Cocks

→ in 3 weeks, 4 years before they were "publicly" discovered, he discovered/invented RSA, followed by Diffie-Hellman.

We must have some public elements!

Public Elements

p - large prime

g - generator

each prime has $\phi(p-1)$ generators.

① Alice picks a secret value a, calculates $g^a \bmod p$ and sends to Bob. (a is private, $g^a \bmod p$ Public)

② Bob picks b, sends $g^b \bmod p$ to Alice. (b is private)

Eve knows $g^a \bmod p$, but can't deduce a.

Alice $\xrightarrow{A = g^a \bmod p}$ Bob

Alice $\xleftarrow{B = g^b \bmod p}$ Bob

③ Alice calculates $B^a \bmod p$

$= (g^b)^a \bmod p$

$\equiv \boxed{g^{ab} \bmod p}$

④ Bob calculates $= A^b \bmod p$

$= (g^a)^b \bmod p$

$= \boxed{g^{ab} \bmod p}$

→ Shared secret key!

Eve knows $g, p, \boxed{g^a \bmod p, g^b \bmod p}$

$(g^a \bmod p)(g^b \bmod p)$

$g^a g^b \equiv g^{\underline{\underline{a+b}}} \bmod p$

$(g^a)^p ? \times \quad (g^a)^{g^b} = g^{a \cdot g^b} \times$

$p = 13 \quad g = 2$

Alice picks 6, $2^6 \bmod 13 = 64 \bmod 13 = 12$

Alice $\xrightarrow{12}$ Bob

Bob picks 4, $2^4 \bmod 13 = 16 \bmod 13 = 3$

Alice $\xleftarrow{3}$ Bob

Alice calculates $3^6 \bmod 13 = 3^3 \times 3^3$

$= 27 \times 27$

$= 1 \times 1 \bmod 13$

Bob takes $12^4 \bmod 13$

$(-1)^4 \bmod 13$

$= \boxed{1}$

$p = 17 \quad g = 3$

Alice picks 11 → $3^{11} \bmod 17 \equiv 7 \bmod 17$

$3^3 \cdot 3^3 \cdot 3^3 \cdot 3^2$

$27 \times 27 \times 27 \times 9 \bmod 17$

$10 \times 10 \times 10 \times 9 \bmod 17$

$100 \times 90 \bmod 17$

15×5

$75 \bmod 17$

$= \boxed{7 \bmod 17}$

Alice → 7 → Bob

Bob pick 5, $3^5 \bmod 17$

$3^3 \times 3^2 \bmod 17$

$27 \times 9 \bmod 17$

$10 \times 9 \bmod 17$

5

Bob → 5 → Alice

Alice Calculates $5^{11} \bmod 17$

Bob Calculate $7^5 \bmod 17$

$(3^5)^{11} = 3^{55}$

$(3^{11})^5 = 3^{55}$

$7^5 = 7^2 \times 7^2 \times 7 \bmod 17$

$49 \times 49 \times 7$

$15 \times 15 \times 7 \bmod 17$

$(-2) \times (-2) \times 7$

$28 \bmod 17$

$\boxed{11}$

$5^{11} \bmod 17$

$25 \times 25 \times 25 \times 25 \times 25 \times 5$

$8 \times 8 \times 8 \times 8 \times 8 \times 5$

$64 \times 64 \times 40$

$13 \times 13 \times 6$

$(-4) \times (-4) \times 6$

16×6

-6

$\boxed{11}$