Recap from Number Theory part 3 - Ext Euclid

1) (th) a, n integers $\qquad$ a, n share no common factors

$\exists$ v -order $\quad \underline{a^v = 1} \bmod n \iff \gcd(a,n) = 1$

coprimes

$a^{v+1} \equiv a^v \cdot a \equiv a \bmod n$

<u>proof</u>: $\Rightarrow$ easy $\quad a^{v-1} = a^{-1}$ inverse

$a^v = 1 \bmod n \Rightarrow \gcd(a,n) = 1$

assume (hypoth) $\boxed{d = \gcd(a,n) \neq 1} \Rightarrow d \mid a, \; d \mid n$

$a^v = 1 \bmod n \Rightarrow a^v = nk + 1 \Rightarrow a^v - nk = 1$

$$\left.\begin{aligned} d \mid a &\Rightarrow d \mid a^v \\ d \mid n &\Rightarrow d \mid n \cdot k \end{aligned}\right\} \Rightarrow d \mid \underline{\underline{a^v}} - \underline{\underline{nk}} \Rightarrow d \mid 1$$

contradict

proof : $d = \gcd(a,n) = 1 \Rightarrow \exists v \quad a^v = 1 \mod n$.

$\boxed{P(a) = \{a, a^2, a^3, a^4, \dots\} \mod n}$ set of a powers

– group

$P(a)$ cannot be infinite (mod n are only n values)

$\Rightarrow$ some powers same remainder mod n

repeats $\boxed{a^t = a^u} \mod n \qquad t > u$

$a^t - a^u = 0 \mod n \Rightarrow n \mid (a^t - a^u)$

no factors in common

$\Rightarrow n \mid a^u \cdot (a^{t-u} - 1)$

$\gcd(n, a^u) = 1 \Rightarrow n, a^u$ no common factors

$\Rightarrow n \mid (a^{t-u} - 1) \Rightarrow a^{t-u} = 1 \mod n$

$\boxed{v = t - u}$ order

• set of coprimes$(n) = C(n) = \{0 \le r \le n-1 \mid r, n \text{ coprimes}\}$
remainders $\quad \gcd(r,n)=1$

example $\quad n=6 \quad C(n) = \{1, 5\} \quad \varphi(6)=2$

$n=10 \quad C(n) = \{1, 3, 7, 9\} \quad \varphi(10)=4$

$n=11$ (prime) $\quad C(n) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$\varphi(11)=10$

$n=14 \quad C(14) = \{1, 3, 5, 9, 11, 13\} \quad \varphi(14)=6$

• $\boxed{\varphi(n)} = |C(n)| = \#$ of coprime remainders.
Euler's totient

Th Euler / $\boxed{\text{Lagrange (general groups)}}$ → order_subgroup | order_group

$a \in C(n) \quad \gcd(a,n)=1 \iff \exists\, v = \text{order of } a \quad a^v \equiv \boxed{1} \bmod n$

then $v \mid \varphi(n)$: $\varphi(n)$ is a multiple of v

example $n=14$ $\quad C(n)=\{1,3,5,9,11,13\}$ $\quad \varphi(n)=6$

pick a coprime with n, say $a=5$

Th $\Longrightarrow$ order v of a $\quad v \mid \varphi(n) \Rightarrow v \mid 6$

$5^v \equiv 1 \mod 14$

$5^2 = 25 \equiv 11$

$5^3 = 5 \cdot 11 = 55 \equiv -1$

$5^6 = (5^3)^2 = (-1)^2 = 1$

$\boxed{v=6}$

$a=3$

$3^2 = 9 \equiv -5$

$3^3 = 9 \cdot 3 = 27 \equiv -1$

$3^6 = (-1)^2 = 1$

$\boxed{v=6}$

$a=13$

$a^2 = 13^2 = (-1)^2 = 1$

$\boxed{v=2}$

Lagrange Th: $P(a)=\{a^1, a^2, \ldots, a^v = 1\}$ subgroup of $C(n)$ with multiplication

Lagrange $\Rightarrow$ $|P(a)| \mid |C(n)|$

$\boxed{v \mid \varphi(n)}$

proof (idea) a, n coprimes

$C(n)$ = coprime remainders with n

$P(a)$ = powers-subset $= \{a, a^2, a^3, \ldots a^v = 1\}$

$Q(a)$ = set of quotients "$\frac{C(n)}{P(a)}$"

smallest

- want $|C(n)| = |P(a)| \cdot |Q(a)|$

ex $n=9$ $a=4$ $P(a) = \{4, 4^2 = 16 \equiv 7, 4^3 = 64 \equiv 1\}$ $v=3$

$C(9) = \{1, 2, 4, 5, 7, 8\}$ $\varphi(9) = 6$

C(n) coprime	P(a): /4	/4^2	/4^3	smallest q
1	7	4	1	1
7	4	1	7	
4	1	7	4	
2	5	8	2	2
5	8	2	5	
8	2	5	8	

$Q(4) = \{1, 2\}$

ex: $n=26$, $a=9$ $\quad P(a)=\{9, 9^2\equiv 3, 9^3\equiv 27\equiv 1\}$ $\quad V=3$

$C(26)=\{1,3,5,\boxed{7},9,\boxed{11},15,17,19,\boxed{21},23,25\}$ $\quad \varphi(26)=12$

	coprime	/9	/9^2	/$9^3\equiv 1$	smallest q
$P(a)$	1, 3, 9	3, 9, 1	9, 1, 3	1, 3, 9	1
$P(a)\cdot 5$	5, 15, 19	15, 19, 5	19, 5, 15	5, 15, 19	5
$P(a)\cdot 7$	7, 21, 11	21, 11, 7	11, 7, 21	7, 21, 11	7
$P(a)\cdot 17$	17, 25, 23	25, 23, 17	23, 17, 25	17, 25, 23	17

$Q(9)=\{1,5,7,17\}$

$C(n)=P(a)\times Q(a)$

$=\{1,3,9\}\times\{1,5,7,17\}$

$|C(n)|=|P(a)|\cdot|Q(a)|$

$\varphi(n)=V\cdot$ smooth

$\Rightarrow V \mid \varphi(n)$

Corollary $v \mid \varphi(n) \Rightarrow$ we can use $\varphi(n)$ as order for every a coprime with n.

$n = 26$ $\quad b = 17$ $\quad 17^v \equiv 1$ $\quad$ don't need v

Instead of v, use $\varphi(n) = 12 = v \cdot k$

$$17^{\varphi(n)} = 17^{12} = 17^{v \cdot k} = (17^v)^k \equiv 1^k \equiv 1 \mod 26$$

inverse $17^{-1} = 17^{11}$ because $17^{11} \cdot 17 = 17^{12} \equiv 1 \mod 26$

$$= 17^{\varphi(n)-1}$$

Th a, n coprimes $\Rightarrow a^{\varphi(n)-1} =$ inverse of a

because $a^{\varphi(n)} \equiv 1 \mod n$

How $\varphi(n)$ looks like on particular cases?

- n = prime $\Rightarrow$ $C(n) = \{$all remainders except $0\}$ $\varphi(n) = n-1$

  $a \in C(n)$ Euler Th $a^{\varphi(n)} \equiv 1 \mod n$

  $a^{n-1} \equiv 1 \mod n$ $\quad a^n \equiv a \mod n$ (Fermat's Little Th)

- $n = \text{prime}^k = p^k$

  $C(n) = \{$all remainders$\} \setminus \{$multiples of p remainders$\}$

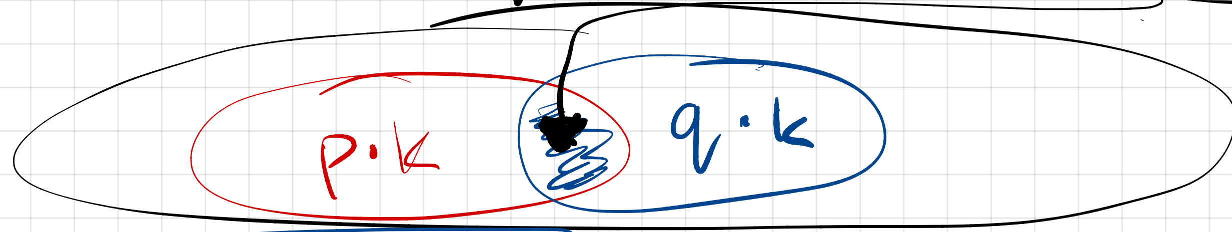
  $n \setminus \{0, p, 2p, 3p, \dots n-p\}$

  $\boxed{0}, \boxed{1}p, \boxed{2}p, \dots - \boxed{(p^{k-1}-1)}p$

$\varphi(n) = |C(n)| = n - p^{k-1} = p^k - p^{k-1} = p^{k-1}(p-1)$

• RSA case $n = p \cdot q$ p, q primes PIE

$$\varphi(n) = \left|\left\{\begin{matrix}\text{coprimes}\\ \text{with } n\end{matrix}\right\}\right| = \left|\left\{\begin{matrix}\text{all}\\ \text{remainders}\end{matrix}\right\}\right| - \left|\left\{\begin{matrix}\text{mult}\\ \text{of}\\ p\end{matrix}\right\}\right| - \left|\left\{\begin{matrix}\text{mult}\\ \text{of}\\ q\end{matrix}\right\}\right| + \left|\left\{\begin{matrix}\text{mult}\\ \text{of}\\ \{p,q\}\end{matrix}\right\}\right|$$



$$= n - \left|\left\{0, p\cdot 1, p\cdot 2, \dots, \left(\tfrac{n}{p}-1\right)\cdot p\right\}\right| - \left|\left\{0, 1q, 2q, \dots, \left(\tfrac{n}{q}-1\right)q\right\}\right| + \left|\{\text{mult of } pq\}\right|$$

$$= n - \left|\{0, 1, 2, \dots, q-1\}\right| - \left|\{0, 1, 2, \dots, p-1\}\right| + \left|\{0\}\right|$$

$$= pq - q - p + 1$$

$$= \boxed{(p-1)(q-1)} = \#\text{ of coprimes remainders with } n = pq$$

RSA SETUP (ahead of ops)

$n = p \cdot q$ BIG PRIMES n = public p, q secret

$\varphi(n) = \boxed{(p-1)(q-1)}$ $\varphi(n)$ secret

e = public key

e coprime with $\varphi(n)$

$\gcd\{e, (p-1)(q-1)\} = 1$

e = encoding key

d = private/decode key

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

$d \cdot e \equiv 1 \mod (p-1)(q-1)$

$ed = \varphi(n) \cdot k + 1$ d = secret

$x^{ed} = (x^{\varphi(n)})^k \cdot x \equiv x$

encode / decode (ops)

x = message (integer)

$\text{encode}(x) =$

$\bar{x} = x^e \bmod n$

$\text{decode}(\bar{x}) =$

$(\bar{x})^d \bmod n$

Th $\text{decode}(\bar{x}) = x$

proof: $\text{decode}(\bar{x}) = (\bar{x})^d \bmod n$

$= (x^e)^d \bmod n = x^{ed} \bmod n$

$= x^{\varphi(n)\cdot k+1} \equiv (x^{\varphi(n)})^k \cdot x$

$= 1 \cdot x \equiv x$

RSA example 1 $\quad p=5 \quad q=13 \quad n=65 \quad \varphi(n)=4\cdot 12=48$

SETUP $\quad e=5 \quad d=e^{-1} \bmod \varphi(n) = 5^{-1} \bmod 48 = 29$

OPS $\quad x=2$ message orig

$$\text{encode}(2) = 2^5 \bmod n = 32 \bmod 65 = 32$$

$$\text{decode}(32) = 32^{29} \bmod 65 = 2 \checkmark$$

$x=16$ orig message

$$\text{encode}(16) = 16^5 \bmod n = 16^5 \bmod 65 =$$

$$1048576 \bmod 65 = 61$$

$$\text{decode}(61) = 61^{29} \bmod 65 = 16 \checkmark$$

RSA ex 2 **SETUP** $p = 3$ $q = 11$ $n = 33$ $\varphi(n) = 2 \cdot 10 = 20$

$e = 7$ & $\varphi(n)$ coprimes $d = e^{-1} \bmod \varphi(n) = 7^{-1} \bmod 20 = 3$

public private

OPS $x = 5$ orig message

$\text{encode}(5) = 5^{7=e} \bmod n = 78125 \bmod 33 = 14$

$\text{decode}(14) = 14^{3=d} \bmod n = 2744 \bmod 33 = 5$ ✓

RSA in practice:

- p, q very large (current 4096 bits?) $\Rightarrow$ operations have to be logarithmic ($\simeq$ 4096 steps)

- Why is hard to crack? e, n = known
  find p, q

  Find "d" $\Leftrightarrow$ factorize $n = p, q$

  Know extremely hard problem for large #

  Computational effort to find p, q > benefit of breaking RSA

- how to find p, q? Can't generate primes #
  - generate random large numbers p, q
  - use "Fermat's Little Th" to check them (not perfect, very high prob)

p = candidate

pick a at random < p

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

yes → maybe p prime

No → p ≠ prime for sure

repeat (new a)