Review on elementary number theory for cryptography

Andersen Ang

First created: 2013-Nov. Last update: 2017-Feb-1

All number here are assumed to be *integer*.

1 Prime Factorization

- Any integers that is not prime number can be *uniquely factorized* into products of primes$p$ as

$$a = \prod_{p \in Prime} p^{a_p}$$

e.g. $12 = 2^2 \times 3^1$, $90 = 2^1 \times 3^2 \times 5^1$.

- Recall that $'1'$ is not prime, otherwise ... $12 = 2^2 \times 3^1 \times 1^1 = 2^2 \times 3^1 \times 1^1 \times 1^1 = 2^2 \times 3^1 \times 1^1 \times 1^1 \times 1^1 \times ...$ then the prime factorization is not *unique*

2 Coprime

a, b are *coprime* if they do not share same factor (except 1)
e.g. Factor of 8 : {1,2,4,8}, factor of 15 : {1,2,3,5,15} , they have no same factor (other than 1), so 8,15 coprime

- 2 number are coprime then their Greatest Common Divisor GCD is 1

$$GCD(a, b) = 1 \iff a, b\, coprime$$

- If 2 numbers are not coprime, then they have Greatest common divisor that is larger than 1
- e.g. $8 = 2^3$, $12 = 2^2 \times 3^1$, so their GCD is $2^2 = 4$

3 Concurrence / Mod, Set of residues

- $a \equiv b$ $(mod\ c)$ denotes the remainder of $\frac{a}{c}$ equals to the remainder of $\frac{b}{c}$.
- e.g. 8≡ 15 (mod 7) as they have same remainder.
- In mod p arithmetic, the set of "possible numbers" are $0, 1, 2, ..., p-1$.
- e.g. In mod 3 arithmetic, there are only 3 possible numbers : {0,1,2} , notice that 2 is coprime with 3.
- so the *reduced set of residues* of mod 3 is {2}.
- The complete set of residue of mod p , where p is prime is $\{0, 1, 2, 3..., p-1\}$.
- The reduced set of residue of mod p is a subset of complete set of residue that the element are all coprime with p.

4 Fermat's Theorem

- $a^{p-1} = 1 \ (mod \ p)$ for $\gcd(a, p) = 1$
- e.g. $p = 3$, $a = 10$, then $a^{p-1} = 10^2 = 100 = 1 \ (mod \, 3)$
- Note $gcd(a, p) = 1$ means a, p coprime, so if a, p not coprime, Fermat's theorem does not hold : $a = 6$, $p = 3$, then $a^{p-1} = 6^2 = 36 \neq 1 \, (mod \, 3)$

5 Euler's Phi Function

- The number of element of the reduced set of reside is the Euler's Phi function $\phi(n)$
- For $n = p$,p is prime, $\phi(p) = p - 1$
- For $n = pq$, where p, q coprime, $\phi(pq) = (p - 1)(q - 1)$

6 Euler's Theorem

- Generalized Fermat's Theorem : $a^{\phi(n)} = 1 \ (\text{mod } N)$, for $gcd(a, N) = 1$
- Euler's Theorem is the key for the RSA method in public key.

$$-END-$$