Prime Numbers

密碼學與應用

海洋大學資訊工程系
丁培毅

Prime Numbers

- **Prime number**: an integer p>1 that is divisible only by 1 and itself, ex. 2, 3,5, 7, 11, 13, 17…
- **Composite number**: an integer n>1 that is not prime
- **Fact**: there are infinitely many prime numbers. (by Euclid)

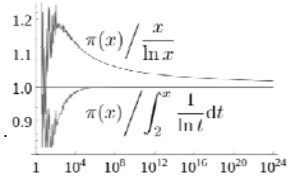
pf:
- on the contrary, assume a_n is the largest prime number
- let the finite set of prime numbers be $\{a_0, a_1, a_2, \ldots. a_n\}$
- the number $b = a_0 * a_1 * a_2 * \ldots * a_n + 1$ is not divisible by any a_i
  i.e. b does not have prime factors $\leq a_n$

2 cases:
- if b has a prime factor d, $b > d > a_n$, then "d is a prime number that is larger than a_n" … contradiction
- if b does not have any prime factor less than b, then "b is a prime number that is larger than a_n" … contradiction

Prime Number Theorem

- **Prime Number Theorem**:
  - Let π(x) be the number of primes less than x
  - Then
    $$\pi(x) \approx \frac{x}{\ln x}$$
    in the sense that the ratio $\pi(x) / (x/\ln x) \to 1$ as $x \to \infty$
  - Also, $\pi(x) \geq \frac{x}{\ln x}$ and for $x \geq 17$, $\pi(x) \leq 1.10555 \frac{x}{\ln x}$
- Ex: number of 100-digit primes

$$\pi(10^{100}) - \pi(10^{99}) \approx \frac{10^{100}}{\ln 10^{100}} -$$



Factors

- Every composite number can be expressible as a product a·b of integers with 1 < a, b< n
- Every positive integer has a unique representation as a product of prime numbers raised to different powers.
  - Ex. $504 = 2^3 \cdot 3^2 \cdot 7$, $1125 = 3^2 \cdot 5^3$

Factors

- Lemma: p is a prime number and $p \mid a \cdot b \Longrightarrow p \mid a$ or $p \mid b$, more generally, p is a prime number and $p \mid a \cdot b \cdot \ldots \cdot z$ $\Longrightarrow$ p must divide one of a, b, …, z
  - proof:
    - case 1: $p \mid a$
    - case 2: $p \nmid a$,
      - $p \nmid a$ and p is a prime number $\Rightarrow \gcd(p, a) = 1 \Rightarrow 1 = a\,x + p\,y$
      - multiply both side by b, $b = \underline{b\,a}\,x + b\,\underline{p}\,y$
      - $p \mid a\,b \Rightarrow p \mid b$
    - In general: if $p \mid a$ then we are done, if $p \nmid a$ then $p \mid bc\ldots z$, continuing this way, we eventually find that p divides one of the factors of the product

Unique Prime Factorization Theorem

- Theorem: Every positive integer is a product of primes. This factorization into primes is unique, up to reordering of the factors.

  • Empty product equals 1.
  • Prime is a one factor product.

  - Proof: product of primes
    - assume there exist positive integers that are not product of primes
    - let n be the smallest such integer
    - since n can not be 1 or a prime, n must be composite, i.e. $n = a \cdot b$
    - since n is the smallest, both a and b must be products of primes.
    - $n = a \cdot b$ must also be a product of primes, contradiction
  - Proof: uniqueness of factorization
    - assume $n = r_1^{c_1} r_2^{c_2} \cdots r_k^{c_k} p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} = r_1^{c_1} r_2^{c_2} \cdots r_k^{c_k} q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}$ where p_i, q_j are all distinct primes.
    - let $m = n / (r_1^{c_1} r_2^{c_2} \cdots r_k^{c_k})$
    - consider p_1 for example, since p_1 divide $m = q_1 q_1 .. q_1 q_2 \ldots q_t$, p_1 must divide one of the factors q_j, contradict the fact that "p_i, q_j are distinct primes"

("Fair-MAH")

Fermat's Little Theorem

- If p is a prime, $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$

Proof:
- let $S = \{1, 2, 3, \ldots, p-1\}$ (Z_p^*), define $\psi(x) \equiv a \cdot x \pmod p$ be a mapping $\psi: S \to Z$
- $\forall x \in S, \psi(x) \neq 0 \pmod p \Rightarrow \forall x \in S, \psi(x) \in S$, i.e. $\psi: S \to S$

  if $\psi(x) \equiv a \cdot x \equiv 0 \pmod p \Rightarrow x \equiv 0 \pmod p$ since $\gcd(a, p) = 1$
- $\forall x, y \in S$, if $x \neq y$ then $\psi(x) \neq \psi(y)$

  if $\psi(x) \equiv \psi(y) \Rightarrow a \cdot x \equiv a \cdot y \Rightarrow x \equiv y$ since $\gcd(a, p) = 1$
- from the above two observations, $\psi(1), \psi(2), \ldots \psi(p-1)$ are distinct elements of S
- $1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv \psi(1) \cdot \psi(2) \cdot \ldots \cdot \psi(p-1) \equiv (a \cdot 1) \cdot (a \cdot 2) \cdot \ldots \cdot (a \cdot (p-1))$
  $\equiv a^{p-1} (1 \cdot 2 \cdot \ldots \cdot (p-1)) \pmod p$
- since $\gcd(j, p) = 1$ for $j \in S$, we can divide both side by 1, 2, 3, … p-1, and obtain $a^{p-1} \equiv 1 \pmod p$

Fermat's Little Theorem

- Ex: $2^{10} = 1024 \equiv 1 \pmod{11}$

  $2^{53} = (2^{10})^5 2^3 \equiv 1^5 2^3 \equiv 8 \pmod{11}$

  i.e. $2^{53} \equiv 2^{53 \bmod 10} \equiv 2^3 \equiv 8 \pmod{11}$

- if n is prime, then $2^{n-1} \equiv 1 \pmod n$
  i.e. if $2^{n-1} \neq 1 \pmod n$ then n is not prime ←(∗)
  usually, if $2^{n-1} \equiv 1 \pmod n$, then n is prime
  - exceptions: $2^{561-1} \equiv 1 \pmod{561}$ although $561 = 3 \cdot 11 \cdot 17$
    $2^{1729-1} \equiv 1 \pmod{1729}$ although $1729 = 7 \cdot 13 \cdot 19$
  - (∗) is a quick test for eliminating composite number

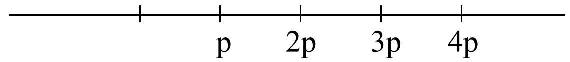
Euler's Totient Function $\phi(n)$

- $\phi(n)$: the number of integers $1 \le a < n$ s.t. $\gcd(a,n)=1$
  ex. $n=10$, $\phi(n)=4$ the set is $Z_{10}^* = \{1,3,7,9\}$
- properties of $\phi(\bullet)$
  - $\phi(p) = p-1$, if p is prime
  - $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$, if p is prime
  - $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $\gcd(n,m)=1$ *multiplicative property*
  - $\phi(n \cdot m) = \phi((d_1/d_2/d_3)^2) \cdot \phi(d_2^3) \cdot \phi(d_3^3) \cdot \phi(n/d_1/d_2) \cdot \phi(m/d_1/d_3)$
    if $\gcd(n,m)=d_1$, $\gcd(n/d_1,d_1)=d_2$, $\gcd(m/d_1,d_1)=d_3$
  - $\phi(n) = n \prod_{\forall p|n} (1-1/p)$

ex. $\phi(10)=(2-1)\cdot(5-1)=4$ $\phi(120)=120(1-1/2)(1-1/3)(1-1/5)=32$

How large is $\phi(n)$?

- $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large
- Probability that a random number r is multiples of a prime number p? $1/p$ *think of 2 (even numbers), 3, 5, ...* **r** must be of the form **kp**



- Probability that two independent random numbers r_1 and r_2 both have a given prime number p as a factor? $1/p^2$
- The probability that they do not have p as a common factor is thus $1 - 1/p^2$
- The probability that two numbers r_1 and r_2 have no common prime factor? $P = (1-1/2^2)(1-1/3^2)(1-1/5^2)(1-1/7^2)\ldots$

Pr{ r_1 and r_2 relatively prime }

- Equalities:

$$\frac{1}{1-x} = 1+x+x^2+x^3+\ldots$$

$$1 + 1/2^2 + 1/3^2 + 1/4^2 + 1/5^2 + 1/6^2 + \ldots = \pi^2/6$$

- $P = (1-1/2^2)(1-1/3^2)(1-1/5^2)(1-1/7^2) \cdot \ldots$
  $= ((1+1/2^2+1/2^4+\ldots)(1+1/3^2+1/3^4+\ldots) \cdot \ldots)^{-1}$
  $= (1+1/2^2+1/3^2+1/4^2+1/5^2+1/6^2+\ldots)^{-1}$
  $= 6/\pi^2$
  ≈ 0.61

each positive number has a unique prime number factorization
ex. $45^2 = 3^4 \cdot 5^2$

How large is $\phi(n)$?

- $\phi(n)$ is the number of integers less than n that are relative prime to n
- $\phi(n)/n$ is the probability that a randomly chosen integer is relatively prime to n
- Therefore, $\phi(n) \approx n \cdot 6/\pi^2$
- P_n = Pr { n random numbers have no common factor }
  - n independent random numbers all have a given prime p as a factor is $1/p^n$
  - They do not all have p as a common factor $1 - 1/p^n$
  - $P_n = (1+1/2^n+1/3^n+1/4^n+1/5^n+1/6^n+\ldots)^{-1}$ is the Riemann zeta function $\zeta(n)$ http://mathworld.wolfram.com/RiemannZetaFunction.html
  - Ex. $n=4$, $\zeta(4) = \pi^4/90 \approx 0.92$

Euler's Theorem

true when n is prime

true even when $n = p^k$

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

Proof: ✡ let S be the set of integers $1 \le x < n$, with $\gcd(x, n) = 1$

✡ define $\psi(x) \equiv a \cdot x \pmod n$ be a mapping $\psi: S \to Z$

✡ $\forall x \in S$ and $\gcd(a, n) = 1$,
$\psi(x) \neq 0 \pmod n$
$\gcd(\psi(x), n) = 1$
$\Rightarrow \forall x \in S, \psi(x) \in S$, i.e. $\psi: S \to S$

if $\psi(x) \equiv a \cdot x \equiv 0 \pmod n \Rightarrow x \equiv 0 \pmod n$

$\gcd(a, n)=1$ and $\gcd(x, n)=1$ (no common prime factors)

✡ $\forall x, y \in S$, 'if $x \neq y$ then $\psi(x) \not\equiv \psi(y) \pmod n$'

if $\psi(x) \equiv \psi(y) \Rightarrow a \cdot x \equiv a \cdot y \Rightarrow x \equiv y$ since $\gcd(a, n) = 1$

✡ from the above two observations, $\forall x \in S$, $\psi(x)$ are distinct elements of S (i.e. $\{\psi(x) \mid \forall x \in S\}$ is S)

✡ $\prod_{x \in S} x \equiv \prod_{x \in S} \psi(x) \equiv a^{\phi(n)} \prod_{x \in S} x \pmod n$

✡ since $\gcd(x, n) = 1$ for $x \in S$, we can cancel one by one $x \in S$ of both sides, and obtain $a^{\phi(n)} \equiv 1 \pmod n$

Euler's Theorem

✧ Example: What are the last three digits of 7^{803}?

i.e. we want to find $7^{803} \pmod{1000}$

$1000 = 2^3 \cdot 5^3$, $\phi(1000) = 1000(1-1/2)(1-1/5) = 400$

$7^{803} \equiv 7^{803 \pmod{400}} \equiv 7^3 \equiv 343 \pmod{1000}$)

✧ Example: Compute $2^{43210} \pmod{101}$?

$101 = 1 \cdot 101$, $\phi(101) = 100$

$2^{43210} \equiv 2^{43210 \pmod{100}} \equiv 2^{10} \equiv 1024 \equiv 14 \pmod{101}$

A second proof of Euler's Theorem

Euler's Theorem: $\forall a \in Z_n^*, a^{\phi(n)} \equiv 1 \pmod n$

✧ We have proved the above theorem by showing that the function $\psi(x) \equiv a \cdot x \pmod n$ is a permutation.

✧ We can also prove it through Fermat's Little Theorem & CRT

➢ consider $n = p \cdot q$, $\phi(n) = (p-1)(q-1)$

$\forall a \in Z_p^*, a^{p-1} \equiv 1 \pmod p \Rightarrow (a^{p-1})^{q-1} \equiv a^{\phi(n)} \equiv 1 \pmod p$

$\forall a \in Z_q^*, a^{q-1} \equiv 1 \pmod q \Rightarrow (a^{q-1})^{p-1} \equiv a^{\phi(n)} \equiv 1 \pmod q$

$\gcd(p,q)=1 \Rightarrow p \cdot q \mid a^{\phi(n)}-1$, i.e. $\forall a \in Z_n^* (p \nmid a \text{ and } q \nmid a)$, $\underline{a^{\phi(n)} \equiv 1 \pmod n}$

➢ consider $n = p^r$, $\phi(n) = p^{r-1}(p-1)$

$\forall a \in Z_{p^r}^*, a^{p-1} \equiv 1 \pmod p \Rightarrow a^{p-1} = 1 + \lambda p$

$a^{\phi(n)} = (1+\lambda p)^{p^{r-1}} = 1 + C_1^{p^{r-1}} \lambda p + C_2^{p^{r-1}} (\lambda p)^2 + \ldots$

$= 1 + p^{r-1} \lambda p + p^{r-1}(p^{r-1}-1)/2\, (\lambda p)^2 + \ldots$

$a^{\phi(n)} \equiv (1+\lambda p)^{p^{r-1}}$
$\equiv 1 \pmod n$

A second proof (cont'd)

➢ consider $n = p^r \cdot q^s$, $\phi(n) = p^{r-1}(p-1)\, q^{s-1}(q-1)$

$\forall a \in Z_{p^r}^*, a^{p-1} \equiv 1 \pmod p \Rightarrow (a^{p-1})^{p^{r-1}} \equiv 1 \pmod{p^r}$

$\Rightarrow (a^{(p-1)p^{r-1}})^{(q-1)\, q^{s-1}} \equiv a^{\phi(n)} \equiv 1 \pmod{p^r} \Rightarrow p^r \mid a^{\phi(n)}-1$

$\forall a \in Z_{q^s}^*, a^{q-1} \equiv 1 \pmod q \Rightarrow (a^{q-1})^{q^{s-1}} \equiv 1 \pmod{q^s}$

$\Rightarrow (a^{(q-1)q^{s-1}})^{(p-1)\, p^{r-1}} \equiv a^{\phi(n)} \equiv 1 \pmod{q^s} \Rightarrow q^s \mid a^{\phi(n)}-1$

$\gcd(p^r,q^s)=1 \Rightarrow p^r q^s \mid a^{\phi(n)}-1$, i.e. $\forall a \in Z_n^* (p \nmid a \text{ and } q \nmid a)$, $\underline{a^{\phi(n)} \equiv 1 \pmod n}$

➢ consider $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, $\phi(n) = n \prod_{\forall p \mid n} (1-1/p)$ **Unique Prime Factorization**

$\forall a \in Z_{p_i^{r_i}}^*, a^{p_i-1} \equiv 1 \pmod{p_i} \Rightarrow (a^{p_i-1})^{p_i^{r_i-1}} \equiv 1 \pmod{p_i^{r_i}}$

$\Rightarrow (a^{(p_i-1)p_i^{r_i-1}})^{\prod_{\forall j \neq i} (p_j-1)p_j^{r_j-1}} \equiv a^{\phi(n)} \equiv 1 \pmod{p_i^{r_i}} \Rightarrow p_i^{r_i} \mid a^{\phi(n)}-1$

all $p_i^{r_i}$ are relatively prime $\Rightarrow \prod_{i=1}^{k} p_i^{r_i} \mid a^{\phi(n)}-1$, i.e. $\forall a \in Z_n^* (\forall i, p_i \nmid a)$, $\underline{a^{\phi(n)} \equiv 1 \pmod n}$

Carmichael Theorem

Theorem:

$\forall a \in Z_n^*$, $a^{\lambda(n)} \equiv 1 \pmod{n}$ and $a^{n\cdot\lambda(n)} \equiv 1 \pmod{n^2}$
where $n=p\cdot q$, $p \neq q$, $\lambda(n) = \mathrm{lcm}(p-1, q-1)$, $\lambda(n) \mid \phi(n)$

✧ like Euler's Theorem, we can prove it through Fermat's Little Theorem, consider $n = p \cdot q$, where $p\neq q$,

$\forall a\in Z_p^*$, $a^{p-1} \equiv 1 \pmod{p} \Rightarrow (a^{p-1})^{(q-1)/\gcd(p-1,q-1)} \equiv a^{\lambda(n)} \equiv 1 \pmod{p}$

$\forall a\in Z_q^*$, $a^{q-1} \equiv 1 \pmod{q} \Rightarrow (a^{q-1})^{(p-1)/\gcd(p-1,q-1)} \equiv a^{\lambda(n)} \equiv 1 \pmod{q}$

$\gcd(p,q)=1 \Rightarrow pq \mid a^{\lambda(n)}-1$, $\forall a\in Z_n^*$ (i.e. $p\nmid a \wedge q\nmid a$), $a^{\lambda(n)} \equiv 1 \pmod{n}$

therefore, $\forall a\in Z_n^*$, $a^{\lambda(n)} = 1 + k \cdot n$

raise both side to the n-th power, we get $a^{n\cdot\lambda(n)} = (1 + k \cdot n)^n$,

$\Rightarrow a^{n\cdot\lambda(n)} = 1 + n\cdot k\cdot n + \ldots \Rightarrow \forall a \in Z_n^*$ (or $Z_{n^2}^*$), $a^{n\cdot\lambda(n)} \equiv 1 \pmod{n^2}$

Basic Speedup in Exponentiation

✧ Let a, n, x, y be integers with $n\geq 1$, and $\gcd(a,n)=1$ if $x \equiv y \pmod{\phi(n)}$, then $a^x \equiv a^y \pmod{n}$.

✧ If you want to work mod n, you should work mod $\phi(n)$ or $\lambda(n)$ in the exponent.

Primitive Roots modulo p

✧ When p is a prime number, a primitive root modulo p is a number whose powers yield every nonzero element mod p. (equivalently, the order of a primitive root is p-1)

✧ ex: $3^1\equiv 3$, $3^2\equiv 2$, $3^3\equiv 6$, $3^4\equiv 4$, $3^5\equiv 5$, $3^6\equiv 1 \pmod{7}$
3 is a primitive root mod 7

✧ sometimes called a multiplicative generator

✧ there are plenty of primitive roots, actually $\phi(p-1)$

- ex. $p=101$, $\phi(p-1)=100\cdot(1-1/2)\cdot(1-1/5)=40$
  $p=143537$, $\phi(p-1)=143536\cdot(1-1/2)\cdot(1-1/8971)=71760$

Primitive Testing Procedure

✧ How do we test whether h is a primitive root modulo p?

- naïve inefficient method:
  go through all powers $h^2, h^3, \ldots, h^{p-2}$, and make sure they all $\neq 1$ modulo p
- fast method:
  let p-1 has prime factors $q_1, q_2, \ldots, q_n$,
  for all q_i, make sure $h^{(p-1)/q_i}$ modulo p is not 1,
  then h is a primitive root

Intuition: let $h \equiv g^a \pmod{p}$, $\gcd(a, p-1)=d \Rightarrow$ h is not a primitive root

$(g^a)^{(p-1)/d} \equiv (g^{a/d})^{(p-1)} \equiv 1 \pmod{p}$

$\Rightarrow \forall$ prime $q_i \mid d$, $h^{(p-1)/q_i} \equiv (g^a)^{(p-1)/q_i} \equiv (g^{a/q_i})^{(p-1)} \equiv 1 \pmod{p}$

ex. $p=29$, $p-1=2\cdot 2\cdot 7$, $h=5$, $h^{28/2}=1$, $h^{28/7}=16$, 5 is not a primitive
$h=11$, $h^{28/2}=28$, $h^{28/7}=25$, 11 is a primitive

Primitive Testing Procedure (cont'd)

- Procedure to test if h is a primitive root :

> let p-1 has prime factors $q_1, q_2, \ldots, q_n$, (i.e. $\phi(p)=p-1=q_1^{r_1}\ldots q_n^{r_n}$)
> for all q_i, $h^{(p-1)/q_i}$ (mod p) is not 1 $\Rightarrow$ h is a primitive

pf:

(a) by definition, $ord_p(h)$ is the smallest positive x s.t. $h^x \equiv 1$ (mod p)

Fermat Theorem: $h^{\phi(p)} \equiv 1$ (mod p) therefore implies $ord_p(h) \le \phi(p)$

if $\phi(p) = ord_p(h) * k + s$ with $0 \le s < ord_p(h)$

$h^{\phi(p)} \equiv h^{ord_p(h) * k}\, h^s \equiv h^s \equiv 1$ (mod p), but $s < ord_p(h) \Rightarrow s = 0$, i.e. $ord_p(h) \mid \phi(p)$

(b) assume h is not a primitive root i.e $ord_p(h) < \phi(p)=p-1$ ($q_1^{r_1}\ldots q_n^{r_n}$)

then $\exists$ i such that $ord_p(h) \mid (p-1)/q_i$ i.e. $h^{(p-1)/q_i} \equiv 1$ (mod p) for some q_i

(c) if for all q_i, $h^{(p-1)/q_i} \ne 1$ (mod p)

then $ord_p(h) = \phi(p)$ and h is a primitive root modulo p

Number of Primitive Roots in Z_p^*

- Why are there $\phi(p-1)$ primitive roots?
  - let h be a primitive root (the order of h is p-1)
  - $h, h^2, h^3, \ldots, h^{p-1}$ is a permutation of 1,2,…p-1 (an integer less than p-1)
  - if gcd(a, p-1)=d, then $(h^a)^{(p-1)/d} \equiv (h^{a/d})^{(p-1)} \equiv 1$ (mod p) which says that the order of h^a is at most (p-1)/d, therefore, h^a is not a primitive root $\Rightarrow$ There are **at most** $\phi(p-1)$ primitive roots in Z_p^*
  - For any element h^a in Z_p^* where gcd(a, p-1) = 1, it is guaranteed that $(h^a)^{(p-1)/q_i} \ne 1$ (mod p) for all q_i (q_i is prime factors of p-1)

pf. assume that for a certain q_i, $(h^a)^{(p-1)/q_i} \equiv 1$ (mod p)

h is a primitive root $\Rightarrow$ $p-1 \mid a \cdot (p-1) / q_i$

$\Rightarrow \exists$ integer k s.t. $a \cdot (p-1) / q_i = k \cdot (p-1)$ i.e. $a = k \cdot q_i$

$\Rightarrow q_i \mid a$

$\Rightarrow q_i \mid \gcd(a, p-1)$ contradiction

Lucas Primality Test

- An integer n is **prime** iff *__the converse of Fermat Little Theorem__*

$\exists$a, s.t. **1.** $a^{n-1} \equiv 1$ (mod n)
2. $\forall$prime factor q of n-1, $a^{n-1/q} \ne 1$ (mod n)

Proof:

($\Rightarrow$) if n is prime, *__catch: inefficient, factors of n-1 are required__*

Fermat's little theorem ensures that "$\forall a \ne kn$, $a^{n-1} \equiv 1$ (mod n)"
a primitive a ensures "$\forall$ prime factor q of n-1, $a^{n-1/q} \ne 1$ (mod n)"

($\Leftarrow$) if $\exists$a, s.t. 1. $a^{n-1} \equiv 1$ (mod n) and
2. $\forall$prime factor q of n-1, $a^{n-1/q} \ne 1$ (mod n)

By definition, $ord_n(a)$ is the smallest positive x s.t. $a^x \equiv 1$ (mod n)
the first condition implies that $ord_n(a) \le n-1$ and $ord_n(a) \mid n-1$
the second condition then implies that $ord_n(a) = n-1$ (*)
Euler thm says that $a^{\phi(n)} \equiv 1$ (mod n), by definition $\phi(n)<n-1$ if n is a composite number, i.e. $ord_n(a) \mid \phi(n) < n-1$, contradict with (*).

Pratt's Primality Certificate

- Pratt's proved in 1975 that the following polynomial-size structure can **prove that a number is prime** and is verifiable in polynomial time
- based on the **Lucas Primality Test (LPT)**
- example:

229 ($a = 6$, $229 - 1 = 2^2 \times 3 \times 19$)
- 2 (known prime)
- 3 ($a = 2$, $3 - 1 = 2$)
  - 2 (known prime)
- 19 ($a = 2$, $19 - 1 = 2 \times 3^2$)
  - 2 (known prime)
  - 3 ($a = 2$, $3 - 1 = 2$)
    - 2 (known prime)

verification

$2^{3-1} \equiv 1$ (mod 3)
$2^{2/2} \equiv 2$ (mod 3)
By LPT, 2 is a prime, then 3 is also a prime

$2^{19-1} \equiv 1$ (mod 19)
$2^{18/2} \equiv 18$ (mod 19)
$2^{18/3} \equiv 7$ (mod 19)
By LPT, if 2 and 3 are primes, then 19 is also a prime

$6^{229-1} \equiv 1$ (mod 229)
$6^{228/2} \equiv 228$ (mod 229)
$6^{228/3} \equiv 134$ (mod 229)
$6^{228/19} \equiv 165$ (mod 229)
By LPT, if 2, 3, 19 are primes, then 229 is also a prime

Multiplicative Generators in Z_n^*

- How do we define a multiplicative generator in Z_n^* if n is a composite number?
  - Is there an element in Z_n^* that can generate all elements of Z_n^*?
  - If n = p · q, the answer is negative. From Carmichael theorem, $\forall a \in Z_n^*$, $a^{\lambda(n)} \equiv 1 \pmod{n}$, gcd(p-1, q-1) is at least 2, $\lambda(n)$ = lcm(p-1, q-1) is at most $\phi(n) / 2$. The size of a maximal possible multiplicative subgroup in Z_n^* is therefore no larger than $\lambda(n)$.
  - If $n = p^k$, the answer is yes
  - How many elements in Z_n^* can generate the maximal possible subgroup of Z_n^*?

Finding Square Roots mod n

- For example: find x such that $x^2 \equiv 71 \pmod{77}$
  - Is there any solution?
  - How many solutions are there?
  - How do we solve the above equation systematically?
- In general: find x s.t. $x^2 \equiv b \pmod{n}$,

  where $b \in QR_n$, $n = p \cdot q$, and p, q are prime numbers
- Easier case: find x s.t. $x^2 \equiv b \pmod{p}$,

  where p is a prime number, $b \in QR_p$

Note: QR_n is "Quadratic Residue in Z_n^*" to be defined later

Finding Square Root mod p

- Given $y \in Z_p^*$, find x, s.t. $x^2 \equiv y \pmod{p}$, p is prime

Two cases:
- $p \equiv 1 \pmod 4$ (i.e. $p = 4k + 1$) : probabilistic algorithm
- $p \equiv 3 \pmod 4$ (i.e. $p = 4k + 3$) : deterministic algorithm

- Is there any solution? (Is y a QR_p?)

  check $y^{\frac{p-1}{2}} \overset{?}{\equiv} 1 \pmod{p}$ ***Euler's Criterion***
- $p \equiv 3 \pmod 4$

$$x \equiv \pm y^{\frac{p+1}{4}} \pmod{p}$$

  - $(p+1)/4 = (4k+3+1)/4 = k+1$ is an integer
  - $x^2 = y^{(p+1)/2} = y^{(p-1)/2} \cdot y \equiv y \pmod{p}$

Finding Square Root mod p

- $p \equiv 1 \pmod 4$
  - Peralta, Eurocrypt'86, $p = 2^s q + 1$, both p, q are prime
  - 3-step probabilistic procedure
    1. Choose a random number r, if $r^2 \equiv y \pmod{p}$, output $z = r$
    2. Calculate $(r + x)^{(p-1)/2} \equiv u + v\,x \pmod{f(x)}$, $f(x) = x^2 - y$
    3. If $u = 0$ then output $z \equiv v^{-1} \pmod{p}$, else goto step 1

    note: $(b+cx)(d+ex) \equiv (bd+ce\,x^2) + (be+cd)\,x$
    $\equiv (bd+ce\,y) + (be+cd)\,x \pmod{x^2-y}$
    use *square-multiply* algorithm to calculate the polynomial $(r + x)^{(p-1)/2}$
  - the probability to successfully find z for each $r \geq 1/2$

Finding Square Root mod p

✧ ex: find z such that $z^2 \equiv 12 \pmod{13}$

solution:

- ✡ $13 \equiv 1 \pmod 4$ ie. 4k+1
- ✡ choose $r = 3$, $3^2 = 9 \neq 12$
- ✡ $(3 + x)^{(13-1)/2} = (3 + x)^6 \equiv 12 + 0\,x \pmod{x^2-12}$
- ✡ choose $r = 7$, $7^2 \equiv 10 \neq 12$
- ✡ $(7 + x)^{(13-1)/2} = (7 + x)^6 \equiv 0 + 8\,x \pmod{x^2-12}$
  $\Rightarrow z = 8^{-1} = 5 \pmod{13}$

Why does it work???

Why is the success probability > ½ ???

Finding Square Roots mod n

✧ Now let's return to the question of solving square roots in Z_n^*, i.e.

for an integer $y \in QR_n$,

find $x \in Z_n^*$ such that $x^2 \equiv y \pmod n$

✧ We would like to transform the problem into solving square roots mod p.

✧ Question: for $n=p\cdot q$

Is solving "$x^2 \equiv y \pmod n$" equivalent to solving

"$x^2 \equiv y \pmod p$ and $x^2 \equiv y \pmod q$"??? **yes**

($\Rightarrow$) $x^2-y=kn=kpq \Rightarrow p \mid x^2-y$ and $q \mid x^2-y$ □

($\Leftarrow$) $p|x^2-y$, $q|x^2-y$, i.e. $x^2-y=kp=k'q$, $q \nmid p \Rightarrow q|k$, i.e. $x^2-y=k''pq$ □

Finding Square Roots mod p·q

✧ find x such that $x^2 \equiv 71 \pmod{77}$

- ✶ $77 = 7 \cdot 11$
- ✶ "x^* satisfies $f(x^*) \equiv 71 \pmod{77}$" $\Leftrightarrow$
  "x^* satisfies both $f(x^*) \equiv 1 \pmod 7$ and $f(x^*) \equiv 5 \pmod{11}$"
- ✶ since 7 and 11 are prime numbers, we can solve $x^2 \equiv 1 \pmod 7$ and $x^2 \equiv 5 \pmod{11}$ far more easily than $x^2 \equiv 71 \pmod{77}$
  - $x^2 \equiv 1 \pmod 7$ has two solutions: $x \equiv \pm 1 \pmod 7$
  - $x^2 \equiv 5 \pmod{11}$ has two solutions: $x \equiv \pm 4 \pmod{11}$
- ✶ put them together and use CRT to calculate the four solutions
  - $x \equiv 1 \pmod 7 \equiv 4 \pmod{11} \Rightarrow x \equiv 15 \pmod{77}$
  - $x \equiv 1 \pmod 7 \equiv 7 \pmod{11} \Rightarrow x \equiv 29 \pmod{77}$
  - $x \equiv 6 \pmod 7 \equiv 4 \pmod{11} \Rightarrow x \equiv 48 \pmod{77}$
  - $x \equiv 6 \pmod 7 \equiv 7 \pmod{11} \Rightarrow x \equiv 62 \pmod{77}$

Computational Equivalence to Factoring

✧ Previous slides show that once you know the factors of n are p and q, you can easily solve the square roots of n

✧ Indeed, if you can solve the square roots for one single quadratic residue mod n, you can factor n.

- ✶ from the four solutions $\pm a$, $\pm b$ on the previous slide
  - $x \equiv c \pmod p \equiv d \pmod q \Rightarrow x \equiv a \pmod{p\cdot q}$
  - $x \equiv c \pmod p \equiv -d \pmod q \Rightarrow x \equiv b \pmod{p\cdot q}$
  - $x \equiv -c \pmod p \equiv d \pmod q \Rightarrow x \equiv -b \pmod{p\cdot q}$
  - $x \equiv -c \pmod p \equiv -d \pmod q \Rightarrow x \equiv -a \pmod{p\cdot q}$

  we can find out $a \equiv b \pmod p$ and $a \equiv -b \pmod q$
  (or equivalently $a \equiv -b \pmod p$ and $a \equiv b \pmod q$)
- ✶ therefore, $p \mid (a-b)$ i.e. $\gcd(a-b, n) = p$ (ex. gcd(15-29, 77)=7)
  $q \mid (a+b)$ i.e. $\gcd(a+b, n) = q$ (ex. gcd(15+29, 77)=11)

Quadratic Residues

- Consider $y \in Z_n^*$, if $\exists\, x \in Z_n^*$, such that $x^2 \equiv y \pmod{n}$, then y is called a quadratic residue mod n, i.e. $y \in QR_n$
- If the modulus p is prime, there are $(p-1)/2$ quadratic residues in Z_p^*
  - let g be a primitive root in Z_p^*, $\{g, g^2, g^3, \ldots, g^{p-1}\}$ is a permutation of $\{1,2,\ldots p-1\}$
  - in the above set, $\{g^2, g^4, \ldots, g^{p-1}\}$ are quadratic residues (QR_p)
  - $\{g, g^3, \ldots, g^{p-2}\}$ are quadratic non-residues (QNR_p), out of which there are $\phi(p-1)$ primitive roots

Quadratic Residues in Z_p^*

1st proof:

- For each $x \in Z_p^*$, $p-x \neq x \pmod{p}$ (since if x is odd, $p-x$ is even), it's clear that x and $p-x$ ($-x$) are both square roots of a certain $y \in Z_p^*$
- Because there are only $p-1$ elements in Z_p^*, we know that $|QR_p| \leq (p-1)/2$
- Because $|\{g^2, g^4, \ldots, g^{p-1}\}| = (p-1)/2$, there can be no more quadratic residues outside this set. Therefore, the set $\{g, g^3, \ldots, g^{p-2}\}$ contains only quadratic non-residues

Quadratic Residues in Z_p^*

2nd proof:

- Because the squares of x and $p-x$ are the same, the number of quadratic residues must be less than $p-1$ (i.e. some element in Z_p^* must be quadratic non-residue)
- Let g is a primitive, consider this set $\{g, g^3, \ldots, g^{p-2}\}$ directly
- If $g \in QR_p$, then g cannot be a primitive (because g^k must all be quadratic residues). Thus, if g is a primitive then $g \in QNR_p$
- If $g^{2k+1} \equiv g^{2k} \cdot g \in QR_p$, $\exists\, x \in Z_p^*$ such that $x^2 \equiv g^k \cdot g^k \cdot g \pmod{p}$
  Since $\gcd(g^k, p)=1$, $g \equiv ((g^k)^{-1})^2 \cdot x^2 \equiv ((g^k)^{-1} \cdot x)^2 \in QR_p$ contradiction
- Thus, $g^{2k+1} \in QNR_p$

Quadratic Residues in Z_p^*

- ex. p=143537, $p-1=143536=2^4 \cdot 8971$,
  $\phi(p-1)=2^4 \cdot 8971 \cdot (1-1/2) \cdot (1-1/8971)=71760$ primitives,
  $(p-1)/2=71768$ QR_p's and 71768 QNR_p's
  - Note: if g is a primitive, then g^3, g^5 … are also primitives
    except the following 8 numbers $g^{8971}, g^{8971\cdot 3}, \ldots, g^{8971\cdot 15}$
  - Elements in Z_p^* can be grouped further according to their order
    since $\forall x \in Z_p^*$, $ord_p(x) \mid p-1$, we can list all possible orders

$ord_p(x)$	$p-1$	$\frac{p-1}{2}$	$\frac{p-1}{4}$	$\frac{p-1}{8}$	8971 $\frac{p-1}{16}$	16 $\frac{p-1}{8971}$	8 $\frac{p-1}{8971\cdot 2}$	4 $\frac{p-1}{8971\cdot 4}$	2 $\frac{p-1}{8971\cdot 8}$	1 $\frac{p-1}{8971\cdot 16}$
	QNR_p	QR_p	QR_p	QR_p	QR_p	QNR_p	QR_p	QR_p	QR_p	QR_p
#	$\phi(p-1)$					8			2	1

QR_n for Composite Modulus n

- ✧ If y is a quadratic residue modulo n, it must be a quadratic residue modulo all prime factors of n.

  $\exists\, x \in Z_n^*$ s.t. $x^2 \equiv y \pmod n \Leftrightarrow x^2 = k \cdot n + y = k \cdot p \cdot q + y$

  $\Rightarrow x^2 \equiv y \pmod p$ and $x^2 \equiv y \pmod q$

- ✧ If y is a quadratic residue modulo p and also a quadratic residue modulo q, then y is a quadratic residue modulo n.

  $\exists\, r_1 \in Z_p^*$ and $r_2 \in Z_q^*$ such that

  $y \equiv r_1^2 \pmod p \equiv (r_1 \bmod p)^2 \pmod p$

  $\equiv r_2^2 \pmod q \equiv (r_2 \bmod q)^2 \pmod q$

  from CRT, $\exists!\, r \in Z_n^*$ such that $r \equiv r_1 \pmod p \equiv r_2 \pmod q$

  therefore, $y \equiv r^2 \pmod p \equiv r^2 \pmod q$

  again from CRT, $y \equiv r^2 \pmod{p \cdot q}$

Legendre Symbol

- ✧ Legendre symbol $L(a, p)$ is defined when a is any integer, p is a prime number greater than 2
  - ✶ $L(a, p) = 0$ if $p \mid a$
  - ✶ $L(a, p) = 1$ if a is a quadratic residue mod p
  - ✶ $L(a, p) = -1$ if a is a quadratic non-residue mod p
- ✧ Two methods to compute (a/p)
  - ✶ $(a/p) = a^{(p-1)/2} \pmod p$
  - ✶ recursively calculate by $L(a \cdot b, p) = L(a, p) \cdot L(b, p)$
    1. If $a = 1$, $L(a, p) = 1$
    2. If a is even, $L(a, p) = L(a/2, p) \cdot (-1)^{(p^2-1)/8}$
    3. If a is odd prime, $L(a, p) = L((p \bmod a), a) \cdot (-1)^{(a-1)(p-1)/4}$
- ✧ Legendre symbol $L(a, p) = -1$ if $a \in QNR_p$

  $L(a, p) = 1$ if $a \in QR_p$

Legendre Symbol

$$y \in QR_p \Leftrightarrow y^{(p-1)/2} \equiv 1 \pmod p$$

($\Rightarrow$)

- ✶ If $y \in QR_p$
- ✶ Then $\exists x \in Z_p^*$ such that $y \equiv x^2 \pmod p$
- ✶ Therefore, $y^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{(p-1)} \equiv 1 \pmod p$

($\Leftarrow$)

- ✶ If $y \notin QR_p$ i.e. $y \in QNR_p$
- ✶ Then $y \equiv g^{2k+1} \pmod p$
- ✶ Therefore, $y^{(p-1)/2} \equiv (g^{2k} \cdot g)^{(p-1)/2} \equiv g^{k(p-1)}\, g^{(p-1)/2} \equiv g^{(p-1)/2} \not\equiv 1 \pmod p$

$\mathrm{ord}_p(g) = p-1$

Jacobi Symbol

- ✧ Jacobi symbol $J(a, n)$ is a generalization of the Legendre symbol to a composite modulus n
- ✧ If n is a prime, $J(a, n)$ is equal to the Legendre symbol i.e. $J(a, n) \equiv a^{(n-1)/2} \pmod n$
- ✧ Jacobi symbol cannot be used to determine whether a is a quadratic residue mod n (unless n is a prime)

  ex. $J(7, 143) = J(7, 11) \cdot J(7, 13) = (-1) \cdot (-1) = 1$

  however, there is no integer x such that

  $x^2 \equiv 7 \pmod{143}$

Calculation of Jacobi Symbol

- The following algorithm computes the Jacobi symbol J(a, n), for any integer a and odd integer n, recursively:
  - Def 1: J(0, n) = 0 also If n is prime, J(a, n) = 0 if $n|a$
  - Def 2: If n is prime, J(a, n) = 1 if $a \in QR_n$ and J(a, n) = -1 if $a \notin QR_n$
  - Def 3: If n is a composite, J(a, n) = J(a, $p_1 \cdot p_2 \cdots p_m$) = J(a,p_1)·J(a,p_2)…·J(a,p_m)
  - Rule 1: J(1, n) = 1
  - Rule 2: J($a \cdot b$, n) = J(a, n) · J(b, n)
  - Rule 3: J(2, n) = 1 if (n^2-1)/8 is even and J(2, n) = -1 otherwise
  - Rule 4: J(a, n) = J(a mod n, n)
  - Rule 5: J(a, b) = J(-a, b) if a <0 and (b-1)/2 is even,
    J(a, b) = -J(-a, b) if a<0 and (b-1)/2 is odd
  - Rule 6: J(a, $b_1 \cdot b_2$) = J(a, b_1) · J(a, b_2)
  - Rule 7: if gcd(a, b)=1, a and b are odd
    - 7a: J(a, b) = J(b, a) if (a-1)·(b-1)/4 is even
    - 7b: J(a, b) = -J(b, a) if (a-1)·(b-1)/4 is odd

QR_n and Jacobi Symbol

- Consider $n = p \cdot q$, where p and q are prime numbers

$x \in QR_n$

$\Leftrightarrow x \in QR_p$ and $x \in QR_q$

$\Leftrightarrow$ J(x, p) = $x^{(p-1)/2} \equiv 1 \pmod{p}$ and J(x, q) = $x^{(q-1)/2} \equiv 1 \pmod{q}$

$\Rightarrow$ J(x, n) = J(x, p) · J(x, q) = 1

	J(x, p)	J(x, q)	J(x, n)	
Q_{00}	1	1	1	$x \in QR_n$
Q_{01}	1	-1	-1	$x \in QNR_n$
Q_{10}	-1	1	-1	$x \in QNR_n$
Q_{11}	-1	-1	1	$x \in QNR_n$