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…

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

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)

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

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 $\{a_0, a_1, a_2, \ldots a_n\}$

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 $\leq a_n$

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

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**:

Prime Number Theorem

- **Prime Number Theorem**:
  - Let $\pi(x)$ be the number of primes less than x

Prime Number Theorem

- **Prime Number Theorem**:
  - Let $\pi(x)$ be the number of primes less than x
  - Then

$$\pi(x) \approx \frac{x}{\ln x}$$

Prime Number Theorem

- **Prime Number Theorem**:
  - Let $\pi(x)$ 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 $x \to \infty$

Prime Number Theorem

- **Prime Number Theorem**:
  - Let $\pi(x)$ 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 $x \geq 17$, $\pi(x) \leq 1.10555 \frac{x}{\ln x}$

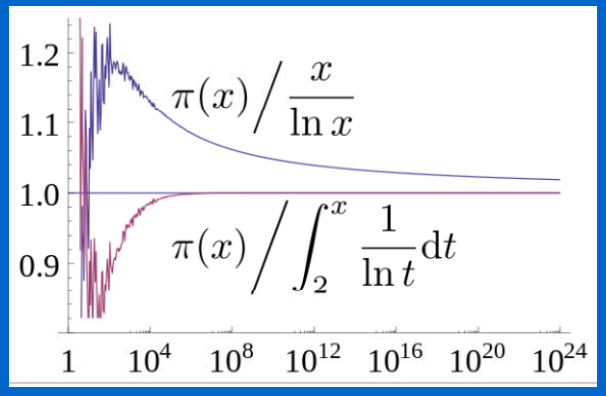
Prime Number Theorem

- **Prime Number Theorem**:
  - Let $\pi(x)$ 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 $x \geq 17$, $\pi(x) \leq 1.10555 \frac{x}{\ln x}$



Prime Number Theorem

- **Prime Number Theorem**:
  - Let $\pi(x)$ 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

$$\pi(10^{100}) - \pi(10^{99}) \approx \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}} \approx 3.9 \times 10^{97}$$

Factors

- Every composite number can be expressible as a product $a \cdot b$ of integers with $1 < a, b < n$

Factors

- Every composite number can be expressible as a product $a \cdot b$ of integers with $1 < a, b < n$
- Every positive integer has a unique representation as a product of prime numbers raised to different powers.

Factors

- Every composite number can be expressible as a product $a \cdot b$ 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 | a·b $\Rightarrow$ p | a or p | b,
  more generally, p is a prime number and p | a·b·…·z
  $\Rightarrow$ p must divide one of a, b, …, z

Factors

- Lemma: p is a prime number and p | a·b $\Rightarrow$ p | a or p | b,
  more generally, p is a prime number and p | a·b·…·z
  $\Rightarrow$ p must divide one of a, b, …, z
  - proof:
    - case 1: p | a

Factors

- Lemma: p is a prime number and p | a·b $\Longrightarrow$ p | a or p | b,
  more generally, p is a prime number and p | a·b·…·z
  $\Longrightarrow$ p must divide one of a, b, …, z
  - proof:
    - case 1: p | a
    - case 2: p $\nmid$ a,

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 $\Rightarrow \gcd(p, a) = 1 \Rightarrow 1 = a\,x + p\,y$

Factors

- Lemma: p is a prime number and $p \mid a \cdot b \Rightarrow p \mid a$ or $p \mid b$,
  more generally, p is a prime number and $p \mid a \cdot b \cdot \ldots \cdot z$
  $\Rightarrow$ 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, $b = \underline{b\,a}\,x + b\,\underline{p}\,y$

Factors

- Lemma: p is a prime number and $p \mid a \cdot b \Rightarrow p \mid a$ or $p \mid b$,
  more generally, p is a prime number and $p \mid a \cdot b \cdot \ldots \cdot z$
  $\Rightarrow$ 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, $b = \underline{b\,a}\,x + b\,\underline{p}\,y$
      - $p \mid a\,b \Rightarrow p \mid b$

Factors

- Lemma: p is a prime number and $p \mid a \cdot b \Rightarrow p \mid a$ or $p \mid b$,
  more generally, p is a prime number and $p \mid a \cdot b \cdot \ldots \cdot z$
  $\Rightarrow$ 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

Factorization into primes

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

Factorization into primes

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

Factorization into primes

- Theorem: Every positive integer is a product of primes. This factorization into primes is unique, up to reordering of the factors.
  - Proof: product of primes
    - assume there exist positive integers that are not product of primes

Factorization into primes

- Theorem: Every positive integer is a product of primes. This factorization into primes is unique, up to reordering of the factors.
  - Proof: product of primes
    - assume there exist positive integers that are not product of primes
    - let n be the smallest such integer

Factorization into primes

- Theorem: Every positive integer is a product of primes. This factorization into primes is unique, up to reordering of the factors.
  - 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. $n = a \cdot b$

Factorization into primes

- Theorem: Every positive integer is a product of primes. This factorization into primes is unique, up to reordering of the factors.
  - 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. $n = a \cdot b$

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

Factorization into primes

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

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

Factorization into primes

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

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

Factorization into primes

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

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

Factorization into primes

- Theorem: Every positive integer is a product of primes. This factorization into primes is unique, up to reordering of the factors.
  - 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 $n = r_1^{c1} r_2^{c2} \cdots r_k^{ck} p_1^{a1} p_2^{a2} \cdots p_s^{as} = r_1^{c1} r_2^{c2} \cdots r_k^{ck} q_1^{b1} q_2^{b2} \cdots q_t^{bt}$ where p_i, q_j are all distinct primes.

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

Factorization into primes

- Theorem: Every positive integer is a product of primes. This factorization into primes is unique, up to reordering of the factors.
  - 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 $n = r_1^{c1} r_2^{c2} \cdots r_k^{ck} p_1^{a1} p_2^{a2} \cdots p_s^{as} = r_1^{c1} r_2^{c2} \cdots r_k^{ck} q_1^{b1} q_2^{b2} \cdots q_t^{bt}$ where p_i, q_j are all distinct primes.
    - let $m = n / (r_1^{c1} r_2^{c2} \cdots r_k^{ck})$

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

Factorization into primes

- Theorem: Every positive integer is a product of primes. This factorization into primes is unique, up to reordering of the factors.
  - 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 $n = r_1^{c1} r_2^{c2} \cdots r_k^{ck} p_1^{a1} p_2^{a2} \cdots p_s^{as} = r_1^{c1} r_2^{c2} \cdots r_k^{ck} q_1^{b1} q_2^{b2} \cdots q_t^{bt}$ where p_i, q_j are all distinct primes.
    - let $m = n / (r_1^{c1} r_2^{c2} \cdots r_k^{ck})$
    - consider p_1 for example, since p_1 divide $m = q_1 q_1 .. q_1 q_2 \cdots q_t$, p_1 must divide one of the factors q_j, contradict the fact that "p_i, q_j are distinct primes"

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

Fermat's Little Theorem

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

("Fair-MAH")

Fermat's Little Theorem

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

Fermat's Little Theorem

✧ If p is a prime, p ∤ 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 $\psi: S \rightarrow Z$

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. $\psi: S \to S$

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

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 $\psi(x) \neq \psi(y)$

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 $\gcd(a, p) = 1$

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

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

✡ $1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv \psi(1) \cdot \psi(2) \cdot \ldots \cdot \psi(p-1) \equiv (a \cdot 1) \cdot (a \cdot 2) \cdot \ldots \cdot (a \cdot (p-1))$

$\equiv a^{p-1} (1 \cdot 2 \cdot \ldots \cdot (p-1)) \pmod{p}$

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

Fermat's Little Theorem

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

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

Fermat's Little Theorem

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

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

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

Fermat's Little Theorem

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

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

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

- 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 $\leftarrow$(*)

  usually, if $2^{n-1} \equiv 1 \pmod{n}$, then n is prime

Fermat's Little Theorem

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

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

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

- if n is prime, then $2^{n-1} \equiv 1 \pmod{n}$

  i.e. if $2^{n-1} \not\equiv 1 \pmod{n}$ 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 $1729 = 7 \cdot 13 \cdot 19$

Fermat's Little Theorem

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

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

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

- if n is prime, then $2^{n-1} \equiv 1 \pmod{n}$

  i.e. if $2^{n-1} \not\equiv 1 \pmod{n}$ then n is not prime $\leftarrow$(*)

  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. $\gcd(a,n) = 1$

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 $Z_{10}^* = \{1,3,7,9\}$

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 $\phi(\bullet)$

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

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

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

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 $\gcd(n,m)=d_1$, $\gcd(n/d_1,d_1)=d_2$, $\gcd(m/d_1,d_1)=d_3$

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 $\gcd(n,m)=d_1$, $\gcd(n/d_1,d_1)=d_2$, $\gcd(m/d_1,d_1)=d_3$
  - $\phi(n) = n \prod_{\forall p \mid n} (1-1/p)$

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 $\gcd(n,m)=d_1$, $\gcd(n/d_1,d_1)=d_2$, $\gcd(m/d_1,d_1)=d_3$
  - $\phi(n) = n \prod_{\forall p \mid n} (1-1/p)$

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

How large is $\phi(n)$?

- $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large
- Probability that a prime number p is a factor of a random number r ?

How large is $\phi(n)$?

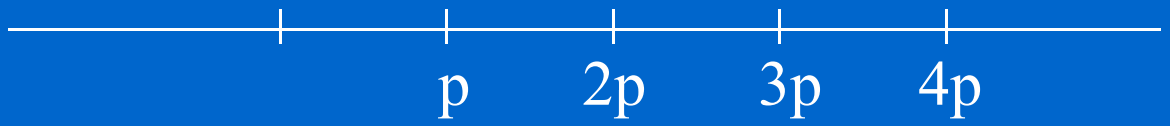
- $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large
- Probability that a prime number p is a factor of a random number r ?

r must be of the form **kp**

How large is $\phi(n)$?

- $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large
- Probability that a prime number p is a factor of a random number r ? $1/p$

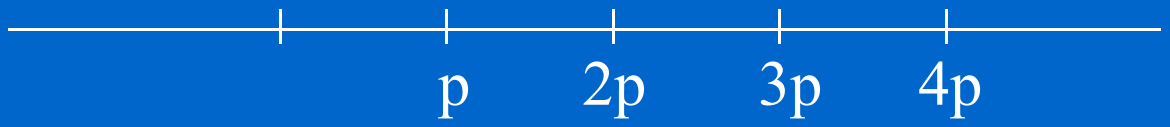
r must be of the form **kp**



How large is $\phi(n)$?

- $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large
- Probability that a prime number p is a factor of a random number r ? $1/p$

r must be of the form **kp**

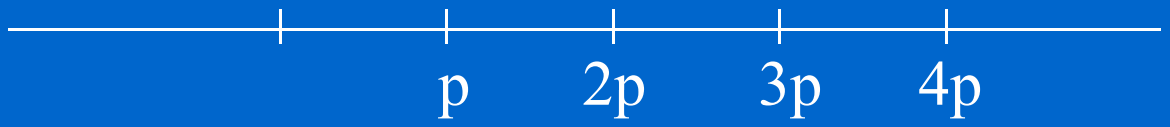


- Probability that two independent random numbers r_1 and r_2 both have a given prime number p as a factor?

How large is $\phi(n)$?

- $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large
- Probability that a prime number p is a factor of a random number r ? $1/p$

r must be of the form **kp**

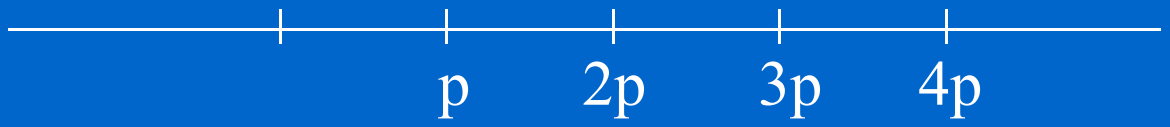


- Probability that two independent random numbers r_1 and r_2 both have a given prime number p as a factor? $1/p^2$

How large is $\phi(n)$?

- $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large
- Probability that a prime number p is a factor of a random number r ? $1/p$

r must be of the form **kp**

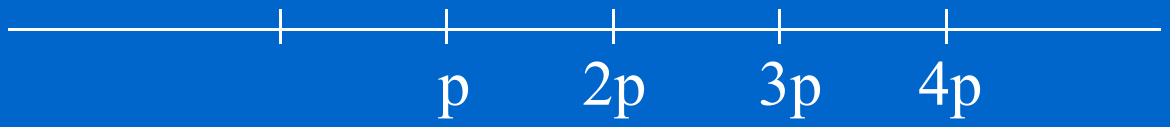


- Probability that two independent random numbers r_1 and r_2 both have a given prime number p as a factor? $1/p^2$
- The probability that they do not have p as a common factor is thus $1 - 1/p^2$

How large is $\phi(n)$?

- $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large
- Probability that a prime number p is a factor of a random number r ? $1/p$

r must be of the form **kp**

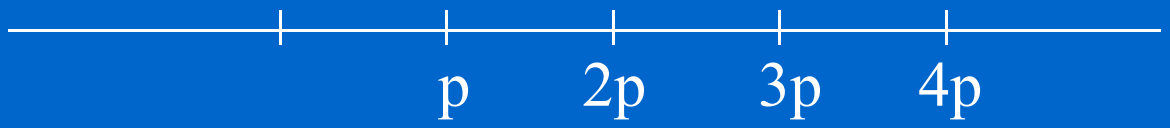


- Probability that two independent random numbers r_1 and r_2 both have a given prime number p as a factor? $1/p^2$
- The probability that they do not have p as a common factor is thus $1 - 1/p^2$
- The probability that two numbers r_1 and r_2 have no common prime factor?

How large is $\phi(n)$?

- $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large
- Probability that a prime number p is a factor of a random number r ? $1/p$

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:

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

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

Pr{ r_1 and r_2 relatively prime }

- Equalities:

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

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

- $P = (1-1/2^2)(1-1/3^2)(1-1/5^2)(1-1/7^2) \cdot \ldots$

Pr{ r_1 and r_2 relatively prime }

- Equalities:

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

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

- $P = (1-1/2^2)(1-1/3^2)(1-1/5^2)(1-1/7^2) \cdot \ldots$

$$= ((1+1/2^2+1/2^4+\ldots)(1+1/3^2+1/3^4+\ldots) \cdot \ldots)^{-1}$$

Pr{ r_1 and r_2 relatively prime }

- Equalities:

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

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

- $P = (1-1/2^2)(1-1/3^2)(1-1/5^2)(1-1/7^2) \cdot \ldots$

$$= ((1+1/2^2+1/2^4+\ldots)(1+1/3^2+1/3^4+\ldots) \cdot \ldots)^{-1}$$

$$= (1+1/2^2+1/3^2+1/4^2+1/5^2+1/6^2+\ldots)^{-1}$$

each positive number has a unique prime number factorization

ex. $45^2 = 3^4 \cdot 5^2$

$\Pr\{ r_1 \text{ and } r_2 \text{ relatively prime} \}$

- Equalities:

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

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

- $P = (1-1/2^2)(1-1/3^2)(1-1/5^2)(1-1/7^2) \cdot \ldots$

$= ((1+1/2^2+1/2^4+\ldots)(1+1/3^2+1/3^4+\ldots) \cdot \ldots)^{-1}$

$= (1+1/2^2+1/3^2+1/4^2+1/5^2+1/6^2+\ldots)^{-1}$

$= 6/\pi^2$

each positive number has a unique prime number factorization

ex. $45^2 = 3^4 \cdot 5^2$

$\Pr\{ r_1 \text{ and } r_2 \text{ relatively prime} \}$

- 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

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

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, $\phi(n) \approx n \cdot 6/\pi^2$

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 }

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 $1/p^n$

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 $1 - 1/p^n$

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

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

- If gcd(a,n)_1 then $a^{\phi(n)} \equiv 1 \pmod{n}$

Euler's Theorem

true when n is prime

- If gcd(a,n)_1 then $a^{\phi(n)} \equiv 1 \pmod{n}$

Euler's Theorem

true when n is prime

- 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

Euler's Theorem

true when n is prime

- 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 $\psi: S \to Z$

Euler's Theorem

true when n is prime

- 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 $\psi: S \rightarrow Z$
- $\forall x \in S$ and gcd(a, n) = 1,

Euler's Theorem

true when n is prime

- 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, $\psi(x) \neq 0 \pmod{n}$

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

Euler's Theorem

true when n is prime

- 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,
  $\psi(x) \neq 0 \pmod{n}$
  $\gcd(\psi(x), n) = 1$

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

Euler's Theorem

true when n is prime

- 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,

$$\left.\begin{array}{l} \psi(x) \neq 0 \pmod{n} \\ \gcd(\psi(x), n) = 1 \end{array}\right\} \Rightarrow \forall x \in S, \psi(x) \in S, \text{ i.e. } \psi: S \to S$$

Euler's Theorem

true when n is prime

- 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,

$$\left.\begin{array}{l} \psi(x) \neq 0 \pmod{n} \\ \gcd(\psi(x), n) = 1 \end{array}\right\} \Rightarrow \forall x \in S, \psi(x) \in S, \text{ i.e. } \psi: S \to S$$

- $\forall$ 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

Euler's Theorem

true when n is prime

- 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. $\psi: S \to S$
- $\forall x, y \in S$, '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)

Euler's Theorem

true when n is prime

✧ 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,

$\left.\begin{array}{l} \psi(x) \neq 0 \pmod{n} \\ \gcd(\psi(x), n) = 1 \end{array}\right\} \Rightarrow \forall x \in S, \psi(x) \in S$, i.e. $\psi: S \to S$

✡ $\forall$ 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)

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

Euler's Theorem

true when n is prime

- 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. $\psi: S \to S$
- $\forall x, y \in S$, '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

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 $\gcd(a, n) = 1$,

  $\left.\begin{array}{l}\psi(x) \neq 0 \pmod{n} \\ \gcd(\psi(x), n) = 1\end{array}\right\} \Rightarrow \forall x \in S, \psi(x) \in S$, i.e. $\psi: S \to S$
- $\forall\ x, y \in S$, '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 $7^{803} \pmod{1000}$

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

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

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

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.

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

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

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

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

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

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

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

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

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. $\forall a \in Z_n^*$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

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. $\forall a \in Z_n^*$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

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

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. $\forall a \in Z_n^*$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

  - 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 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. $\forall a \in Z_n^*$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

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

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

$$a^{\phi(n)} = (1+\lambda p)^{p^{r-1}} = 1 + \mathbf{C}_1^{p^{r-1}} \lambda p + \mathbf{C}_2^{p^{r-1}} (\lambda p)^2 + \ldots$$

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

A 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. $\forall a \in Z_n^*$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod n$
  - consider $n = p^r$, $\phi(n) = p^{r-1}(p-1)$

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

    $a^{\phi(n)} = (1+\lambda p)^{p^{r-1}} = 1 + \mathbf{C}_1^{p^{r-1}} \lambda p + \mathbf{C}_2^{p^{r-1}} (\lambda p)^2 + \ldots$

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

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

A second proof (cont'd)

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

A second proof (cont'd)

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

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

A second proof (cont'd)

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

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

A second proof (cont'd)

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

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

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

A second proof (cont'd)

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

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

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

A second proof (cont'd)

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

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

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

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

A second proof (cont'd)

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

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

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

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

A second proof (cont'd)

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

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

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

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

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

A second proof (cont'd)

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

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

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

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

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

A second proof (cont'd)

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

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

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

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

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

$\gcd(p^r, q^s)=1$

A second proof (cont'd)

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

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

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

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

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

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

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. $\forall a \in Z^*_n$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

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. $\forall a \in Z^*_n$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

- 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

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. $\forall a \in Z^*_n$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

- 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

$\forall a \in Z^*_{p_i^{r_i}}$, $a^{p_i-1} \equiv 1 \pmod{p_i}$

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. $\forall a \in Z^*_n$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

- 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

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

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. $\forall a \in Z^*_n$ ($p \nmid a$ 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

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

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

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. $\forall a \in Z^*_n$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

- 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

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

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

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. $\forall a \in Z^*_n$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

- 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

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. $\forall a \in Z_n^*$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

- 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 $\Rightarrow \prod_{i=1}^{k} p_i^{r_i} \mid a^{\phi(n)}-1$

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. $\forall a \in Z^*_n$ ($p \nmid a$ and $q \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

- 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. $\forall a \in Z^*_n$ ($\forall i, p_i \nmid a$), $a^{\phi(n)} \equiv 1 \pmod{n}$

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 $n=p \cdot q$, $p \neq q$, $\lambda(n) = \text{lcm}(p-1, q-1)$, $\lambda(n) \mid \phi(n)$

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 $n=p \cdot q$, $p \neq q$, $\lambda(n) = \text{lcm}(p-1, q-1)$, $\lambda(n) \mid \phi(n)$

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

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 $n=p \cdot q$, $p \neq q$, $\lambda(n) = \text{lcm}(p-1, q-1)$, $\lambda(n) \mid \phi(n)$

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

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

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 $n=p \cdot q$, $p \neq q$, $\lambda(n) = \text{lcm}(p-1, q-1)$, $\lambda(n) \mid \phi(n)$

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

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

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

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 $n=p \cdot q$, $p \neq q$, $\lambda(n) = \text{lcm}(p-1, q-1)$, $\lambda(n) \mid \phi(n)$

- 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. $p \nmid a \wedge q \nmid a$), $a^{\lambda(n)} \equiv 1 \pmod{n}$

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 $n = p \cdot q$, $p \neq q$, $\lambda(n) = \text{lcm}(p-1, q-1)$, $\lambda(n) \mid \phi(n)$

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

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 $n = p \cdot q$, $p \neq q$, $\lambda(n) = \text{lcm}(p-1, q-1)$, $\lambda(n) \mid \phi(n)$

- 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 $a^{n \cdot \lambda(n)} = (1 + k \cdot n)^n$,

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 $n = p \cdot q$, $p \neq q$, $\lambda(n) = \text{lcm}(p-1, q-1)$, $\lambda(n) \mid \phi(n)$

- 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 Principle to do 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 $a^x \equiv a^y \pmod{n}$.

Basic Principle to do 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)

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

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

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 $\phi(p-1)$

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?

Primitive Testing Procedure

- How do we test whether h is a primitive root modulo p?
  - naïve method:

    go through all powers h^2, h^3, …, h^{p-2}, and make sure they all $\neq 1$ modulo p

Primitive Testing Procedure

- How do we test whether h is a primitive root modulo p?
  - naïve method:

    go through all powers h^2, h^3, …, h^{p-2}, and make sure they all ≠ 1 modulo p
  - faster method:

    assume p-1 has prime factors q_1, q_2, …, q_n,
    for all q_i, make sure $h^{(p-1)/q_i}$ modulo p is not 1,
    then h is a primitive root

Primitive Testing Procedure

- How do we test whether h is a primitive root modulo p?
  - naïve method:

    go through all powers h^2, h^3, …, h^{p-2}, and make sure they all $\neq 1$ modulo p
  - faster method:

    assume p-1 has prime factors q_1, q_2, …, 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 $h \equiv g^a \pmod p$, if gcd(a, p-1)=d (i.e. g^a is not a primitive root), $(g^a)^{(p-1)/q_i} \equiv (g^{a/q_i})^{(p-1)} \equiv 1 \pmod p$ for some $q_i \mid d$

Primitive Testing Procedure

- How do we test whether h is a primitive root modulo p?
  - naïve method:

    go through all powers h^2, h^3, …, h^{p-2}, and make sure they all $\neq 1$ modulo p
  - faster method:

    assume p-1 has prime factors q_1, q_2, …, 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 $h \equiv g^a \pmod p$, if gcd(a, p-1)=d (i.e. g^a is not a primitive root), $(g^a)^{(p-1)/q_i} \equiv (g^{a/q_i})^{(p-1)} \equiv 1 \pmod p$ for some $q_i \mid d$

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

Primitive Testing Procedure

- How do we test whether h is a primitive root modulo p?
  - naïve method:

    go through all powers h^2, h^3, …, h^{p-2}, and make sure they all $\neq 1$ modulo p
  - faster method:

    assume p-1 has prime factors q_1, q_2, …, 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 $h \equiv g^a \pmod p$, if gcd(a, p-1)=d (i.e. g^a is not a primitive root), $(g^a)^{(p-1)/q_i} \equiv (g^{a/q_i})^{(p-1)} \equiv 1 \pmod p$ for some $q_i \mid d$

ex. p=29, p-1=2·2·7, 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 a primitive g:

Primitive Testing Procedure (cont'd)

- Procedure to test a primitive g:

let p-1 has prime factors $q_1, q_2, \ldots, q_n$, (i.e. $\phi(p)=p-1=q_1^{r_1}...q_n^{r_n}$)

for all q_i, $g^{(p-1)/q_i} \pmod p$ is not $1 \Rightarrow$ g is a primitive

Primitive Testing Procedure (cont'd)

- Procedure to test a primitive g:

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

Proof:

Primitive Testing Procedure (cont'd)

- Procedure to test a primitive g:

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

Proof:

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

Primitive Testing Procedure (cont'd)

- Procedure to test a primitive g:

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

Proof:

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

Fermat Theorem: $g^{\phi(p)} \equiv 1 \pmod p$ therefore implies $ord_p(g) \leq \phi(p)$

Primitive Testing Procedure (cont'd)

- Procedure to test a primitive g:

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

Proof:

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

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

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

Primitive Testing Procedure (cont'd)

- Procedure to test a primitive g:

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

Proof:

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

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

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

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

Primitive Testing Procedure (cont'd)

- Procedure to test a primitive g:

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

Proof:

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

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

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

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

(b) assume g is not a primitive root i.e $ord_p(g) < \phi(p)=p-1$

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

Primitive Testing Procedure (cont'd)

- Procedure to test a primitive g:

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

Proof:

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

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

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

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

(b) assume g is not a primitive root i.e $ord_p(g) < \phi(p)=p-1$

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

(c) if for all q_i, $g^{(p-1)/qi} \neq 1 \pmod p$

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

Lucas Primality Test

- An integer n is **prime** iff

  $\exists a$, s.t. { **1.** $a^{n-1} \equiv 1 \pmod{n}$
  2. $\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod{n}$

Lucas Primality Test

- An integer n is **prime** iff

  $\exists a$, s.t. { **1.** $a^{n-1} \equiv 1 \pmod{n}$

  2. $\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod{n}$

the converse of Fermat Little Theorem

Lucas Primality Test

- An integer n is **prime** iff

  ∃a, s.t. { **1.** $a^{n-1} \equiv 1 \pmod{n}$

  2. ∀prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod{n}$

the converse of Fermat Little Theorem

catch: inefficient, factors of n-1 are required

Lucas Primality Test

✧ An integer n is **prime** iff

$\exists a$, s.t. { **1.** $a^{n-1} \equiv 1 \pmod{n}$
2. $\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod{n}$

the converse of Fermat Little Theorem

Proof:

($\Rightarrow$) if n is prime,

catch: inefficient, factors of n-1 are required

Lucas Primality Test

✧ An integer n is **prime** iff

$\exists a$, s.t. { **1.** $a^{n-1} \equiv 1 \pmod{n}$; **2.** $\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod{n}$ }

the converse of Fermat Little Theorem

Proof:

($\Rightarrow$) if n is prime,

catch: inefficient, factors of n-1 are required

Fermat's little theorem ensures that "$\forall a \neq kn$, $a^{n-1} \equiv 1 \pmod{n}$"

Lucas Primality Test

✧ An integer n is **prime** iff

the converse of Fermat Little Theorem

$\exists a$, s.t. { **1.** $a^{n-1} \equiv 1 \pmod{n}$
2. $\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod{n}$

Proof:

($\Rightarrow$) if n is prime,

catch: inefficient, factors of n-1 are required

Fermat's little theorem ensures that "$\forall a \neq kn$, $a^{n-1} \equiv 1 \pmod{n}$"

a primitive a ensures "$\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod{n}$"

Lucas Primality Test

✧ An integer n is **prime** iff

$\exists a$, s.t. { **1.** $a^{n-1} \equiv 1 \pmod{n}$
2. $\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod{n}$

the converse of Fermat Little Theorem

Proof:

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

Fermat's little theorem ensures that "$\forall a \neq kn$, $a^{n-1} \equiv 1 \pmod{n}$"

a primitive a ensures "$\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod{n}$"

($\Leftarrow$) if $\exists a$, s.t. 1. $a^{n-1} \equiv 1 \pmod{n}$ and

2. $\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod{n}$

Lucas Primality Test

✧ An integer n is **prime** iff

$\exists a$, s.t. { **1.** $a^{n-1} \equiv 1 \pmod n$
2. $\forall$prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$

the converse of Fermat Little Theorem

Proof:

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

Fermat's little theorem ensures that "$\forall a \neq kn$, $a^{n-1} \equiv 1 \pmod n$"

a primitive a ensures "$\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$"

($\Leftarrow$) if $\exists$a, s.t. 1. $a^{n-1} \equiv 1 \pmod n$ and

2. $\forall$prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$

By definition, $ord_n(a)$ is the smallest positive x s.t. $a^x \equiv 1 \pmod n$

Lucas Primality Test

✧ An integer n is **prime** iff

$\exists a$, s.t. { **1.** $a^{n-1} \equiv 1 \pmod n$
2. $\forall$prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$

the converse of Fermat Little Theorem

Proof:

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

Fermat's little theorem ensures that "$\forall a \neq kn$, $a^{n-1} \equiv 1 \pmod n$"

a primitive a ensures "$\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$"

($\Leftarrow$) if $\exists$a, s.t. 1. $a^{n-1} \equiv 1 \pmod n$ and

2. $\forall$prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$

By definition, $ord_n(a)$ is the smallest positive x s.t. $a^x \equiv 1 \pmod n$

the first condition implies that $ord_n(a) \leq n-1$, also, $ord_n(a) \mid n-1$

Lucas Primality Test

✧ An integer n is **prime** iff

$\exists a$, s.t. { **1.** $a^{n-1} \equiv 1 \pmod n$

2. $\forall$prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$

the converse of Fermat Little Theorem

Proof:

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

Fermat's little theorem ensures that "$\forall a \neq kn$, $a^{n-1} \equiv 1 \pmod n$"

a primitive a ensures "$\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$"

($\Leftarrow$) if $\exists$a, s.t. 1. $a^{n-1} \equiv 1 \pmod n$ and

2. $\forall$prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$

By definition, $ord_n(a)$ is the smallest positive x s.t. $a^x \equiv 1 \pmod n$

the first condition implies that $ord_n(a) \leq n-1$, also, $ord_n(a) \mid n-1$

the second condition then implies that $ord_n(a) = n-1$ (*)

Lucas Primality Test

✧ An integer n is **prime** iff

the converse of Fermat Little Theorem

$\exists a$, s.t. { **1.** $a^{n-1} \equiv 1 \pmod n$

2. $\forall$prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$

Proof:

($\Rightarrow$) if n is prime,

catch: inefficient, factors of n-1 are required

Fermat's little theorem ensures that "$\forall a \neq kn$, $a^{n-1} \equiv 1 \pmod n$"

a primitive a ensures "$\forall$ prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$"

($\Leftarrow$) if $\exists a$, s.t. 1. $a^{n-1} \equiv 1 \pmod n$ and

2. $\forall$prime factor q of n-1, $a^{n-1/q} \neq 1 \pmod n$

By definition, $ord_n(a)$ is the smallest positive x s.t. $a^x \equiv 1 \pmod n$

the first condition implies that $ord_n(a) \leq n-1$, also, $ord_n(a) \mid n-1$

the second condition then implies that $ord_n(a) = n-1$ (*)

Euler thm says that $a^{\phi(n)} \equiv 1 \pmod n$, by definition $\phi(n)<n-1$ if n is a composite number, i.e. $ord_n(a) < n-1$, contradict with (*).

Pratt's Primality Certificate

- Pratt's proved in 1975 that this polynomial-size structure can **prove that a number is prime** and is verifiable in polynomial time

Pratt's Primality Certificate

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

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 6$, $229 - 1 = 2^2 \times 3 \times 19$)

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 6$, $229 - 1 = 2^2 \times 3 \times 19$)

verification

$6^{229-1} \equiv 1 \pmod{229}$

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 6$, $229 - 1 = 2^2 \times 3 \times 19$)

verification

$6^{229-1} \equiv 1 \pmod{229}$

$6^{228/2} \equiv 228 \pmod{229}$

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 6$, $229 - 1 = 2^2 \times 3 \times 19$)

verification

$6^{229-1} \equiv 1 \pmod{229}$

$6^{228/2} \equiv 228 \pmod{229}$

$6^{228/3} \equiv 134 \pmod{229}$

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 6$, $229 - 1 = 2^2 \times 3 \times 19$)

verification

$6^{229-1} \equiv 1 \pmod{229}$

$6^{228/2} \equiv 228 \pmod{229}$

$6^{228/3} \equiv 134 \pmod{229}$

$6^{228/19} \equiv 165 \pmod{229}$

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 6, 229 - 1 = 2^2 \times 3 \times 19$)

verification

$6^{229-1} \equiv 1 \pmod{229}$

$6^{228/2} \equiv 228 \pmod{229}$

$6^{228/3} \equiv 134 \pmod{229}$

$6^{228/19} \equiv 165 \pmod{229}$

By LPT, if 2, 3, 19 are primes, then 229 is also a prime

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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

verification

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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)

verification

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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

verification

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 3 - 1 = 2$)

verification

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 3 - 1 = 2$)

verification

$2^{3-1} \equiv 1 \pmod 3$

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 3 - 1 = 2$)

verification

$2^{3-1} \equiv 1 \pmod 3$

$2^{2/2} \equiv 2 \pmod 3$

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 3 - 1 = 2$)

verification

$2^{3-1} \equiv 1 \pmod 3$

$2^{2/2} \equiv 2 \pmod 3$

By LPT, 2 is a prime, then 3 is also a prime

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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)

verification

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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

verification

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 19 - 1 = 2 \times 3^2$)

verification

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 19 - 1 = 2 \times 3^2$)

verification

$2^{19-1} \equiv 1 \pmod{19}$

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 19 - 1 = 2 \times 3^2$)

verification

$2^{19-1} \equiv 1 \pmod{19}$

$2^{18/2} \equiv 18 \pmod{19}$

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 19 - 1 = 2 \times 3^2$)

verification

$2^{19-1} \equiv 1 \pmod{19}$

$2^{18/2} \equiv 18 \pmod{19}$

$2^{18/3} \equiv 7 \pmod{19}$

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 19 - 1 = 2 \times 3^2$)

verification

$2^{19-1} \equiv 1 \pmod{19}$

$2^{18/2} \equiv 18 \pmod{19}$

$2^{18/3} \equiv 7 \pmod{19}$

By LPT, if 2 and 3 are primes, then 19 is also a prime

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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)

verification

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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

verification

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 6, 229 - 1 = 2^2 \times 3 \times 19$)

verification

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 ($a = 2, 3 - 1 = 2$)

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 3 - 1 = 2$)

verification

$2^{3-1} \equiv 1 \pmod 3$

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 3 - 1 = 2$)

verification

$2^{3-1} \equiv 1 \pmod 3$

$2^{2/2} \equiv 2 \pmod 3$

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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 ($a = 2, 3 - 1 = 2$)

verification

$2^{3-1} \equiv 1 \pmod 3$

$2^{2/2} \equiv 2 \pmod 3$

By LPT, 2 is a prime, then 3 is also a prime

Pratt's Primality Certificate

- Pratt's proved in 1975 that this 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)

Number of Primitive Root in Z_p^*

- Why are there $\phi(p-1)$ primitive roots?

Number of Primitive Root in Z_p^*

- Why are there $\phi(p-1)$ primitive roots?
  - let g be a primitive root (the order of g is p-1)

Number of Primitive Root in Z_p^*

- Why are there $\phi(p-1)$ primitive roots?
  - let g be a primitive root (the order of g is p-1)
  - $g, g^2, g^3, \ldots, g^{p-1}$ is a permutation of 1,2,…p-1

Number of Primitive Root in Z_p^*

- Why are there $\phi(p-1)$ primitive roots?
  - let g be a primitive root (the order of g is p-1)
  - $g, g^2, g^3, \ldots, g^{p-1}$ is a permutation of 1,2,…p-1
  - if gcd(a, p-1)=d, then $(g^a)^{(p-1)/d} \equiv (g^{a/d})^{(p-1)} \equiv 1 \pmod p$ which says that the order of g^a is at most (p-1)/d, therefore, g^a is not a primitive root $\Rightarrow$ There are at most $\phi(p-1)$ primitive roots in Z_p^*

an integer less than p-1

Number of Primitive Root in Z_p^*

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

an integer less than p-1

Number of Primitive Root in Z_p^*

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

    assume that for a certain q_i, $(g^a)^{(p-1)/q_i} \equiv 1 \pmod p$

an integer less than p-1

Number of Primitive Root in Z_p^*

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

    assume that for a certain q_i, $(g^a)^{(p-1)/q_i} \equiv 1 \pmod p$

    $\Rightarrow p-1 \mid a \cdot (p-1) / q_i$

an integer less than p-1

Number of Primitive Root in Z_p^*

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

    assume that for a certain q_i, $(g^a)^{(p-1)/q_i} \equiv 1 \pmod p$

    $\Rightarrow$ p-1 | a · (p-1) / q_i

    $\Rightarrow \exists$ integer k, a · (p-1) / q_i = k · (p-1) i.e. a = k · q_i

an integer less than p-1

Number of Primitive Root in Z_p^*

- Why are there $\phi(p-1)$ primitive roots?
  - let g be a primitive root (the order of g is p-1)
  - $g, g^2, g^3, \ldots, g^{p-1}$ is a permutation of 1,2,…p-1

    an integer less than p-1
  - if gcd(a, p-1)=d, then $(g^a)^{(p-1)/d} \equiv (g^{a/d})^{(p-1)} \equiv 1 \pmod p$ which says that the order of g^a is at most (p-1)/d, therefore, g^a is not a primitive root $\Rightarrow$ There are at most $\phi(p-1)$ primitive roots in Z_p^*
  - For an element g^a in Z_p^* where gcd(a, p-1) = 1, it is guaranteed that $(g^a)^{(p-1)/q_i} \neq 1 \pmod p$ for all q_i (q_i is factors or p-1)

    assume that for a certain q_i, $(g^a)^{(p-1)/q_i} \equiv 1 \pmod p$

    $\Rightarrow p-1 \mid a \cdot (p-1) / q_i$

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

    $\Rightarrow q_i \mid a$

Number of Primitive Root in Z_p^*

- Why are there $\phi(p-1)$ primitive roots?
  - let g be a primitive root (the order of g is p-1)
  - $g, g^2, g^3, \ldots, g^{p-1}$ is a permutation of 1,2,…p-1

    an integer less than p-1
  - if gcd(a, p-1)=d, then $(g^a)^{(p-1)/d} \equiv (g^{a/d})^{(p-1)} \equiv 1 \pmod p$ which says that the order of g^a is at most (p-1)/d, therefore, g^a is not a primitive root $\Rightarrow$ There are at most $\phi(p-1)$ primitive roots in Z_p^*
  - For an element g^a in Z_p^* where gcd(a, p-1) = 1, it is guaranteed that $(g^a)^{(p-1)/q_i} \neq 1 \pmod p$ for all q_i (q_i is factors or p-1)

    assume that for a certain q_i, $(g^a)^{(p-1)/q_i} \equiv 1 \pmod p$

    $\Rightarrow p-1 \mid a \cdot (p-1) / q_i$

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

    $\Rightarrow q_i \mid a$

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

Multiplicative Generators in Z_n^*

- How do we define a multiplicative generator in Z_n^* if n is a composite number?

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^*?

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 $n = p \cdot q$, 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, $\lambda(n) = \text{lcm}(p-1, q-1)$ is at most $\phi(n) / 2$. The size of a maximal possible multiplicative subgroup in Z_n^* is therefore no larger than $\lambda(n)$.

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 $n = p \cdot q$, 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, $\lambda(n) = \text{lcm}(p-1, q-1)$ 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

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 $n = p \cdot q$, 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, $\lambda(n) = \text{lcm}(p-1, q-1)$ 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

Finding Square Roots mod n

- For example: find x such that $x^2 \equiv 71 \pmod{77}$

Finding Square Roots mod n

- For example: find x such that $x^2 \equiv 71 \pmod{77}$
  - Is there any solution?

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?

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?

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

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, $b \in QR_p$

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

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

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

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?)

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 $y^{\frac{p-1}{2}} \stackrel{?}{\equiv} 1 \pmod{p}$

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 $\quad y^{\frac{p-1}{2}} \stackrel{?}{\equiv} 1 \pmod{p}$

- $p \equiv 3 \pmod 4$

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 $\quad y^{\frac{p-1}{2}} \stackrel{?}{\equiv} 1 \pmod{p}$

- $p \equiv 3 \pmod 4$

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

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 $\quad y^{\frac{p-1}{2}} \stackrel{?}{\equiv} 1 \pmod{p}$

- $p \equiv 3 \pmod 4$

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

  - $(p+1)/4 = (4k+3+1)/4 = k+1$ is an integer

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?)

$$\text{check} \quad y^{\frac{p-1}{2}} \stackrel{?}{\equiv} 1 \pmod{p}$$

- $p \equiv 3 \pmod 4$

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

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

Finding Square Root mod p

- $p \equiv 1 \pmod 4$

Finding Square Root mod p

- $p \equiv 1 \pmod 4$
  - Peralta, Eurocrypt'86, $p = 2^s q + 1$, both p, q are prime

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

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 $z = r$

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 $(r + x)^{(p-1)/2} \equiv u + v\,x \pmod{f(x)}$, $f(x) = x^2 - y$

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

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: $(b+cx)(d+ex) \equiv (bd+ce\,x^2) + (be+cd)\,x$

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: $(b+cx)(d+ex) \equiv (bd+ce\,x^2) + (be+cd)\,x$

$\equiv (bd+ce\,y) + (be+cd)\,x \pmod{x^2-y}$

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

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 $(r + x)^{(p-1)/2}$

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 $z^2 \equiv 12 \pmod{13}$

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

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 $r = 3$, $3^2 = 9 \neq 12$

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 $r = 3$, $3^2 = 9 \neq 12$
  - $(3 + x)^{(13-1)/2} = (3 + x)^6 \equiv 12 + 0\,x \pmod{x^2-12}$

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 $r = 7$, $7^2 \equiv 10 \neq 12$

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 $r = 7$, $7^2 \equiv 10 \neq 12$
  - $(7 + x)^{(13-1)/2} = (7 + x)^6 \equiv 0 + 8\,x \pmod{x^2-12}$

    $\Rightarrow z = 8^{-1} = 5 \pmod{13}$

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???

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.

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 $x^2 \equiv y \pmod{n}$

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.

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 $n = p \cdot q$

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 $x^2 \equiv y \pmod{q}$"???

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

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 ($\Rightarrow$)

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 ($\Rightarrow$) $x^2-y=kn=kpq$

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 $q \mid x^2-y$ □

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 $q \mid x^2-y$ □

  ($\Leftarrow$)

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 $q \mid x^2-y$ □

  ($\Leftarrow$) $p \mid x^2-y$ and $q \mid x^2-y$

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 $q \mid x^2-y$ □

  ($\Leftarrow$) $p \mid x^2-y$ and $q \mid x^2-y \Rightarrow pq \mid x^2-y$ i.e. $x^2-y=kpq=kn$ □

Finding Square Roots mod p·q

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

Finding Square Roots mod p·q

- find x such that $x^2 \equiv 71 \pmod{77}$
  - $77 = 7 \cdot 11$

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 $f(x^*) \equiv 5 \pmod{11}$"

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 $x^2 \equiv 71 \pmod{77}$

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: $x \equiv \pm 1 \pmod{7}$

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: $x \equiv \pm 4 \pmod{11}$

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

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

    $x \equiv 1 \pmod{7} \equiv 4 \pmod{11} \Rightarrow x \equiv 15 \pmod{77}$

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
    - $x \equiv 1 \pmod{7} \equiv 4 \pmod{11} \Rightarrow x \equiv 15 \pmod{77}$
    - $x \equiv 1 \pmod{7} \equiv 7 \pmod{11} \Rightarrow x \equiv 29 \pmod{77}$

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

    $x \equiv 1 \pmod{7} \equiv 4 \pmod{11} \Rightarrow x \equiv 15 \pmod{77}$

    $x \equiv 1 \pmod{7} \equiv 7 \pmod{11} \Rightarrow x \equiv 29 \pmod{77}$

    $x \equiv 6 \pmod{7} \equiv 4 \pmod{11} \Rightarrow x \equiv 48 \pmod{77}$

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

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

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.

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

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

$$x \equiv c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv a \pmod{p.q}$$

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

$$x \equiv c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv a \pmod{p.q}$$
$$x \equiv c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv b \pmod{p.q}$$

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

$$x \equiv c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv a \pmod{p.q}$$
$$x \equiv c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv b \pmod{p.q}$$
$$x \equiv -c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv -b \pmod{p.q}$$

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

$$x \equiv c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv a \pmod{p.q}$$
$$x \equiv c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv b \pmod{p.q}$$
$$x \equiv -c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv -b \pmod{p.q}$$
$$x \equiv -c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv -a \pmod{p.q}$$

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

$$x \equiv c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv a \pmod{p.q}$$
$$x \equiv c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv b \pmod{p.q}$$
$$x \equiv -c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv -b \pmod{p.q}$$
$$x \equiv -c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv -a \pmod{p.q}$$

we can find out $a \equiv b \pmod{p}$ and $a \equiv -b \pmod{q}$

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

$$x \equiv c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv a \pmod{p.q}$$
$$x \equiv c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv b \pmod{p.q}$$
$$x \equiv -c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv -b \pmod{p.q}$$
$$x \equiv -c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv -a \pmod{p.q}$$

we can find out $a \equiv b \pmod{p}$ and $a \equiv -b \pmod{q}$

(or equivalently $a \equiv -b \pmod{p}$ and $a \equiv b \pmod{q}$)

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

$$x \equiv c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv a \pmod{p.q}$$
$$x \equiv c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv b \pmod{p.q}$$
$$x \equiv -c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv -b \pmod{p.q}$$
$$x \equiv -c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv -a \pmod{p.q}$$

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. $\gcd(15-29, 77)=7$)

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

$$x \equiv c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv a \pmod{p.q}$$
$$x \equiv c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv b \pmod{p.q}$$
$$x \equiv -c \pmod{p} \equiv d \pmod{q} \Rightarrow x \equiv -b \pmod{p.q}$$
$$x \equiv -c \pmod{p} \equiv -d \pmod{q} \Rightarrow x \equiv -a \pmod{p.q}$$

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. $y \in QR_n$

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^*

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 $\{1,2,\ldots p-1\}$

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)

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 $p-x$ are both square roots of a certain $y \in Z_p^*$,

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 $p-x$ are both square roots of a certain $y \in Z_p^*$,
- Because there are only $p-1$ elements in Z_p^*, we know that $|QR_p| \leq (p-1)/2$

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 $p-x$ 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)

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

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, $g \in QNR_p$

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, $g \in QNR_p$
- ✶ If $g^{2k+1} \equiv g^{2k} \cdot g \in QR_p$, $\exists\, x \in Z_p^*$ such that $x^2 \equiv g^{2k} \cdot g \pmod{p}$

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, $g \in QNR_p$
- ✶ If $g^{2k+1} \equiv g^{2k} \cdot g \in QR_p$, $\exists\, x \in Z_p^*$ such that $x^2 \equiv g^{2k} \cdot g \pmod p$

  Since $\gcd(g^{2k}, p)=1$, g $(g^{2k})^{-1} \cdot x^2$ $((g^{-1})^k \cdot x)^2 \in QR_p$ contradiction

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, $g \in QNR_p$
- ✶ If $g^{2k+1} \equiv g^{2k} \cdot g \in QR_p$, $\exists\, x \in Z_p^*$ such that $x^2 \equiv g^{2k} \cdot g \pmod p$

  Since $\gcd(g^{2k}, p)=1$, g $(g^{2k})^{-1} \cdot x^2$ $((g^{-1})^k \cdot x)^2 \in QR_p$ contradiction

$(g^{2k})^{-1}(g^{2k}) \equiv (g^{2k})^{-1} g \cdot g \cdot \ldots \cdot g \equiv 1 \pmod p$

$\Rightarrow (g^{2k})^{-1} \equiv g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1} \equiv (g^{-1})^{2k} \equiv ((g^{-1})^k)^2$

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, $g \in QNR_p$
- ✶ If $g^{2k+1} \equiv g^{2k} \cdot g \in QR_p$, $\exists\, x \in Z_p^*$ such that $x^2 \equiv g^{2k} \cdot g \pmod p$

  Since $\gcd(g^{2k}, p)=1$, g $(g^{2k})^{-1} \cdot x^2$ $((g^{-1})^k \cdot x)^2 \in QR_p$ contradiction

  Thus, $g^{2k+1} \in QNR_p$

$(g^{2k})^{-1}(g^{2k}) \equiv (g^{2k})^{-1} g \cdot g \cdot \ldots \cdot g \equiv 1 \pmod p$

$\Rightarrow (g^{2k})^{-1} \equiv g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1} \equiv (g^{-1})^{2k} \equiv ((g^{-1})^k)^2$

Quadratic Residues in Z_p^*

- ex. p=143537, p-1=143536=$2^4 \cdot 8971$,

  $\phi(p\text{-}1)=2^4 \cdot 8971 \cdot (1\text{-}1/2) \cdot (1\text{-}1/8971)=71760$ primitives,

  $(p\text{-}1)/2=71768$ QR_p's and 71768 QNR_p's

Quadratic Residues in Z_p^*

- ex. p=143537, p-1=143536=$2^4 \cdot 8971$,

  $\phi(p\text{-}1)=2^4 \cdot 8971 \cdot (1\text{-}1/2) \cdot (1\text{-}1/8971)=71760$ primitives,

  $(p\text{-}1)/2=71768$ 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}, $g^{8971 \cdot 3}$,..., $g^{8971 \cdot 15}$

Quadratic Residues in Z_p^*

- ex. p=143537, p-1=143536=$2^4 \cdot 8971$,

  $\phi(p\text{-}1)=2^4 \cdot 8971 \cdot (1\text{-}1/2) \cdot (1\text{-}1/8971)=71760$ primitives,

  $(p\text{-}1)/2=71768$ 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}, $g^{8971 \cdot 3}$,..., $g^{8971 \cdot 15}$

  - Elements in Z_p^* can be grouped further according to their order

Quadratic Residues in Z_p^*

- ex. p=143537, p-1=143536=$2^4 \cdot 8971$,

  $\phi(p\text{-}1)=2^4 \cdot 8971 \cdot (1\text{-}1/2) \cdot (1\text{-}1/8971)=71760$ primitives,

  $(p\text{-}1)/2=71768$ 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}, $g^{8971 \cdot 3}$,..., $g^{8971 \cdot 15}$

  - Elements in Z_p^* can be grouped further according to their order

    since $\forall x \in Z_p^*$, $ord_p(x) \mid p\text{-}1$, we can list all possible orders

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

$\mathbf{QR}_n$ for Composite Modulus n

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

$\mathbf{QR}_n$ 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. $x^2 \equiv y \pmod{n} \Leftrightarrow x^2 = k \cdot n + y = k \cdot p \cdot q + y$

$\mathbf{QR}_n$ for Composite Modulus n

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

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

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

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.

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

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

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

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.

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

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

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

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

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

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

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.

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

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

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

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

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

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

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

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.

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

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

- 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, $y \equiv r^2 \pmod{p} \equiv r^2 \pmod{q}$

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.

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

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

- 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

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 $p \mid a$

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

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

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)

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)
  - $(a/p) = a^{(p-1)/2} \pmod{p}$

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 $L(a \cdot b, p) = L(a, p) \cdot L(b, p)$

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 $a = 1$, $L(a, p) = 1$

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, $L(a, p) = L(a/2, p) \cdot (-1)^{(p^2-1)/8}$

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

- 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

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

Legendre Symbol

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

($\Rightarrow$)

- If $y \in \mathrm{QR}_p$

Legendre Symbol

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

($\Rightarrow$)

- If $y \in \mathrm{QR}_p$
- Then $\exists x \in Z_p^*$ such that $y \equiv x^2 \pmod{p}$

Legendre Symbol

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

($\Rightarrow$)

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

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. $y \in QNR_p$

Legendre Symbol

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

($\Rightarrow$)

- If $y \in \mathrm{QR}_p$
- 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 $y \notin \mathrm{QR}_p$ i.e. $y \in \mathrm{QNR}_p$
- Then $y \equiv g^{2k+1} \pmod{p}$

Legendre Symbol

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

($\Rightarrow$)

- If $y \in \mathrm{QR}_p$
- Then $\exists x \in \mathrm{Z}_p^*$ 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 $y \notin \mathrm{QR}_p$ i.e. $y \in \mathrm{QNR}_p$
- Then $y \equiv g^{2k+1} \pmod{p}$
- Therefore, $y^{(p-1)/2} \equiv (g^{2k} \cdot g)^{(p-1)/2} \equiv g^{k(p-1)} g^{(p-1)/2} \equiv g^{(p-1)/2} \not\equiv 1 \pmod{p}$

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, $y^{(p-1)/2} \equiv (g^{2k} \cdot g)^{(p-1)/2} \equiv g^{k(p-1)} g^{(p-1)/2} \equiv g^{(p-1)/2} \not\equiv 1 \pmod{p}$

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

Jacobi Symbol

- Jacobi symbol J(a, n) is a generalization of the Legendre symbol to a composite modulus n

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. $J(a, n) \equiv a^{(n-1)/2} (\text{mod } n)$

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. $J(a, n) \equiv a^{(n-1)/2} (\text{mod } n)$
- Jacobi symbol cannot be used to determine whether a is a quadratic residue mod n (unless n is a prime)

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:

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 $n|a$

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 $a \notin QR_n$

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, $J(a, n) = J(a, p_1 \cdot p_2 \ldots \cdot p_m) = J(a,p_1) \cdot J(a,p_2) \ldots \cdot J(a,p_m)$

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, $J(a, n) = J(a, p_1 \cdot p_2 \ldots \cdot p_m) = J(a,p_1) \cdot J(a,p_2) \ldots \cdot J(a,p_m)$
  - Rule 1: $J(1, n) = 1$

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, $J(a, n) = J(a, p_1 \cdot p_2 \ldots \cdot p_m) = J(a,p_1) \cdot J(a,p_2) \ldots \cdot J(a,p_m)$
  - Rule 1: $J(1, n) = 1$
  - Rule 2: $J(a \cdot b, n) = J(a, n) \cdot J(b, n)$

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, $J(a, n) = J(a, p_1 \cdot p_2 \ldots \cdot p_m) = J(a,p_1) \cdot J(a,p_2) \ldots \cdot J(a,p_m)$
  - Rule 1: $J(1, n) = 1$
  - Rule 2: $J(a \cdot b, n) = J(a, n) \cdot J(b, n)$
  - Rule 3: $J(2, n) = 1$ if $(n^2-1)/8$ is even and $J(2, n) = -1$ otherwise

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, $J(a, n) = J(a, p_1 \cdot p_2 \ldots \cdot p_m) = J(a,p_1) \cdot J(a,p_2) \ldots \cdot J(a,p_m)$
  - Rule 1: $J(1, n) = 1$
  - Rule 2: $J(a \cdot b, n) = J(a, n) \cdot J(b, n)$
  - Rule 3: $J(2, n) = 1$ if $(n^2-1)/8$ is even and $J(2, n) = -1$ otherwise
  - Rule 4: $J(a, n) = J(a \bmod n, n)$

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, $J(a, n) = J(a, p_1 \cdot p_2 \ldots \cdot p_m) = J(a,p_1) \cdot J(a,p_2) \ldots \cdot J(a,p_m)$
  - Rule 1: $J(1, n) = 1$
  - Rule 2: $J(a \cdot b, n) = J(a, n) \cdot J(b, n)$
  - Rule 3: $J(2, n) = 1$ if $(n^2-1)/8$ is even and $J(2, n) = -1$ otherwise
  - Rule 4: $J(a, n) = J(a \bmod n, n)$
  - 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

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, $J(a, n) = J(a, p_1 \cdot p_2 \ldots \cdot p_m) = J(a,p_1) \cdot J(a,p_2) \ldots \cdot J(a,p_m)$
  - Rule 1: $J(1, n) = 1$
  - Rule 2: $J(a \cdot b, n) = J(a, n) \cdot J(b, n)$
  - Rule 3: $J(2, n) = 1$ if $(n^2-1)/8$ is even and $J(2, n) = -1$ otherwise
  - Rule 4: $J(a, n) = J(a \bmod n, n)$
  - 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: $J(a, b_1 \cdot b_2) = J(a, b_1) \cdot J(a, b_2)$

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, $J(a, n) = J(a, p_1 \cdot p_2 \ldots \cdot p_m) = J(a,p_1) \cdot J(a,p_2) \ldots \cdot J(a,p_m)$
  - Rule 1: $J(1, n) = 1$
  - Rule 2: $J(a \cdot b, n) = J(a, n) \cdot J(b, n)$
  - Rule 3: $J(2, n) = 1$ if $(n^2-1)/8$ is even and $J(2, n) = -1$ otherwise
  - Rule 4: $J(a, n) = J(a \bmod n, n)$
  - 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: $J(a, b_1 \cdot b_2) = J(a, b_1) \cdot J(a, b_2)$
  - Rule 7: if $\gcd(a, b)=1$, a and b are odd

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, $J(a, n) = J(a, p_1 \cdot p_2 \ldots \cdot p_m) = J(a,p_1) \cdot J(a,p_2) \ldots \cdot J(a,p_m)$
  - Rule 1: J(1, n) = 1
  - Rule 2: $J(a \cdot b, n) = J(a, n) \cdot J(b, n)$
  - 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: $J(a, b_1 \cdot b_2) = J(a, b_1) \cdot J(a, b_2)$
  - 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

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, $J(a, n) = J(a, p_1 \cdot p_2 \ldots \cdot p_m) = J(a,p_1) \cdot J(a,p_2) \ldots \cdot J(a,p_m)$
  - Rule 1: J(1, n) = 1
  - Rule 2: $J(a \cdot b, n) = J(a, n) \cdot J(b, n)$
  - 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: $J(a, b_1 \cdot b_2) = J(a, b_1) \cdot J(a, b_2)$
  - 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

QR_n and Jacobi Symbol

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

  $x \in QR_n$

QR_n and Jacobi Symbol

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

$$x \in QR_n$$

$$\Leftrightarrow x \in QR_p \text{ and } x \in QR_q$$

QR_n and Jacobi Symbol

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

$$x \in QR_n$$

$$\Leftrightarrow x \in QR_p \text{ and } x \in QR_q$$

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

QR_n and Jacobi Symbol

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

$$x \in QR_n$$

$$\Leftrightarrow x \in QR_p \text{ and } x \in QR_q$$

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

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

QR_n and Jacobi Symbol

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

$$x \in QR_n$$

$$\Leftrightarrow x \in QR_p \text{ and } x \in QR_q$$

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

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

	$J(x, p)$	$J(x, q)$	$J(x, n)$	

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

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

	$J(x, p)$	$J(x, q)$	$J(x, n)$	
Q_{00}				

QR_n and Jacobi Symbol

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

$$x \in QR_n$$
$$\Leftrightarrow x \in QR_p \text{ and } x \in QR_q$$
$$\Leftrightarrow J(x, p) = x^{(p-1)/2} \equiv 1 \pmod{p} \text{ and } J(x, q) = x^{(q-1)/2} \equiv 1 \pmod{q}$$
$$\Rightarrow J(x, n) = J(x, p) \cdot J(x, q) = 1$$

	$J(x, p)$	$J(x, q)$	$J(x, n)$	
Q_{00}	1	1	1	$x \in QR_n$

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

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

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

QR_n and Jacobi Symbol

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

$$x \in QR_n$$
$$\Leftrightarrow x \in QR_p \text{ and } x \in QR_q$$
$$\Leftrightarrow J(x, p) = x^{(p-1)/2} \equiv 1 \pmod{p} \text{ and } J(x, q) = x^{(q-1)/2} \equiv 1 \pmod{q}$$
$$\Rightarrow J(x, n) = J(x, p) \cdot J(x, q) = 1$$

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

QR_n and Jacobi Symbol

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

$$x \in QR_n$$
$$\Leftrightarrow x \in QR_p \text{ and } x \in QR_q$$
$$\Leftrightarrow J(x, p) = x^{(p-1)/2} \equiv 1 \pmod{p} \text{ and } J(x, q) = x^{(q-1)/2} \equiv 1 \pmod{q}$$
$$\Rightarrow J(x, n) = J(x, p) \cdot J(x, q) = 1$$

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

QR_n and Jacobi Symbol

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

$$x \in QR_n$$
$$\Leftrightarrow x \in QR_p \text{ and } x \in QR_q$$
$$\Leftrightarrow J(x, p) = x^{(p-1)/2} \equiv 1 \pmod{p} \text{ and } J(x, q) = x^{(q-1)/2} \equiv 1 \pmod{q}$$
$$\Rightarrow J(x, n) = J(x, p) \cdot J(x, q) = 1$$

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

QR_n and Jacobi Symbol

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

$$x \in QR_n$$
$$\Leftrightarrow x \in QR_p \text{ and } x \in QR_q$$
$$\Leftrightarrow J(x, p) = x^{(p-1)/2} \equiv 1 \pmod{p} \text{ and } J(x, q) = x^{(q-1)/2} \equiv 1 \pmod{q}$$
$$\Rightarrow J(x, n) = J(x, p) \cdot J(x, q) = 1$$

	$J(x, p)$	$J(x, q)$	$J(x, n)$	
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}				

QR_n and Jacobi Symbol

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

$$x \in QR_n$$
$$\Leftrightarrow x \in QR_p \text{ and } x \in QR_q$$
$$\Leftrightarrow J(x, p) = x^{(p-1)/2} \equiv 1 \pmod{p} \text{ and } J(x, q) = x^{(q-1)/2} \equiv 1 \pmod{q}$$
$$\Rightarrow J(x, n) = J(x, p) \cdot J(x, q) = 1$$

	$J(x, p)$	$J(x, q)$	$J(x, n)$	
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	$x \in QNR_n$

Wilson's Theorem

$$(p\text{-}1)! \equiv -1 \pmod{p}$$

Wilson's Theorem

$$(p\text{-}1)! \quad -1 \pmod{p}$$

Proof:

Goal: $(p\text{-}1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p\text{-}1) \equiv -1 \equiv (p\text{-}1) \pmod{p}$

Wilson's Theorem

$$(p\text{-}1)! \quad -1 \pmod{p}$$

Proof:

Goal: $(p\text{-}1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p\text{-}1) \equiv -1 \equiv (p\text{-}1) \pmod{p}$

★ Since $\gcd(p\text{-}1, p) = 1$, the above is equivalent to $(p\text{-}2)! \equiv 1 \pmod{p}$

Wilson's Theorem

$$(p\text{-}1)! \quad -1 \pmod{p}$$

Proof:

Goal: $(p\text{-}1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p\text{-}1) \equiv -1 \equiv (p\text{-}1) \pmod{p}$

★ Since $\gcd(p\text{-}1, p) = 1$, the above is equivalent to $(p\text{-}2)! \equiv 1 \pmod{p}$

★ e.g. $p = 5$, $3 \cdot 2 \cdot 1 \equiv 1 \pmod{5}$

Wilson's Theorem

$$(p\text{-}1)! \quad -1 \pmod{p}$$

Proof:

Goal: $(p\text{-}1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p\text{-}1) \equiv -1 \equiv (p\text{-}1) \pmod{p}$

★ Since $\gcd(p\text{-}1, p) = 1$, the above is equivalent to $(p\text{-}2)! \equiv 1 \pmod{p}$

★ e.g. $p = 5$, $3 \cdot 2 \cdot 1 \equiv 1 \pmod{5}$

$p = 7$, $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \quad 1 \pmod{7}$

Wilson's Theorem

$$(p\text{-}1)! \quad -1 \pmod{p}$$

Proof:

Goal: $(p\text{-}1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p\text{-}1) \equiv -1 \equiv (p\text{-}1) \pmod{p}$

★ Since $\gcd(p\text{-}1, p) = 1$, the above is equivalent to $(p\text{-}2)! \equiv 1 \pmod{p}$

★ e.g. $p = 5$, $3 \cdot 2 \cdot 1 \equiv 1 \pmod{5}$

$p = 7$, $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \quad 1 \pmod{7}$

★ We know that $1^{-1} \equiv 1 \pmod{p}$ and $(-1)^{-1} \equiv -1 \pmod{p}$

Wilson's Theorem

$$(p\text{-}1)! \quad -1 \pmod{p}$$

Proof:

Goal: $(p\text{-}1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p\text{-}1) \equiv -1 \equiv (p\text{-}1) \pmod{p}$

- ✶ Since $\gcd(p\text{-}1, p) = 1$, the above is equivalent to $(p\text{-}2)! \equiv 1 \pmod{p}$
- ✶ e.g. $p = 5$, $3 \cdot 2 \cdot 1 \equiv 1 \pmod 5$

  $p = 7$, $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \quad 1 \pmod 7$
- ✶ We know that $1^{-1} \equiv 1 \pmod{p}$ and $(-1)^{-1} \equiv -1 \pmod{p}$
- ✶ Claim: $\forall i \in Z_p^* \setminus \{1,-1\}$, $i^{-1} \neq i$ (pf: if $i^{-1} \equiv i$ then $i^2 \equiv 1$, $i \in \{1,-1\}$)

Wilson's Theorem

$(p\text{-}1)! \quad -1 \pmod p$

Proof:

Goal: $(p\text{-}1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p\text{-}1) \equiv -1 \equiv (p\text{-}1) \pmod p$

- ✶ Since $\gcd(p\text{-}1, p) = 1$, the above is equivalent to $(p\text{-}2)! \equiv 1 \pmod p$
- ✶ e.g. $p = 5$, $3 \cdot 2 \cdot 1 \equiv 1 \pmod 5$

  $p = 7$, $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \quad 1 \pmod 7$
- ✶ We know that $1^{-1} \equiv 1 \pmod p$ and $(-1)^{-1} \equiv -1 \pmod p$
- ✶ Claim: $\forall i \in Z_p^* \setminus \{1,-1\}$, $i^{-1} \neq i$ (pf: if $i^{-1} \equiv i$ then $i^2 \equiv 1$, $i \in \{1,-1\}$)
- ✶ Claim: $\forall i_1 \neq i_2 \in Z_p^* \setminus \{1,-1\}$, $i_1^{-1} \neq i_2^{-1}$ (pf: if $i_1^{-1} \equiv i_2^{-1}$ then $i_1 \cdot i_2^{-1} \equiv 1$ then $i_1 \equiv i_2$, contradiction)

Wilson's Theorem

$(p\text{-}1)!$ $\quad$ $-1 \pmod p$

Proof:

Goal: $(p\text{-}1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p\text{-}1) \equiv -1 \equiv (p\text{-}1) \pmod p$

- ✶ Since $\gcd(p\text{-}1, p) = 1$, the above is equivalent to $(p\text{-}2)! \equiv 1 \pmod p$
- ✶ e.g. $p = 5$, $\quad 3 \cdot 2 \cdot 1 \equiv 1 \pmod 5$

  $p = 7$, $\quad 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \quad 1 \pmod 7$
- ✶ We know that $1^{-1} \equiv 1 \pmod p$ and $(-1)^{-1} \equiv -1 \pmod p$
- ✶ Claim: $\forall i \in Z_p^* \setminus \{1,-1\}$, $i^{-1} \neq i$ (pf: if $i^{-1} \equiv i$ then $i^2 \equiv 1$, $i \in \{1,-1\}$)
- ✶ Claim: $\forall i_1 \neq i_2 \in Z_p^* \setminus \{1,-1\}$, $i_1^{-1} \neq i_2^{-1}$ (pf: if $i_1^{-1} \equiv i_2^{-1}$ then $i_1 \cdot i_2^{-1} \equiv 1$ then $i_1 \equiv i_2$, contradiction)
- ✶ Out of the set $\{2, 3, \ldots p\text{-}2\}$, we can form $(p\text{-}3)/2$ pairs such that $i \cdot j \equiv 1 \pmod p$, multiply them together, we obtain $(p\text{-}2)! \equiv 1$

Another Proof of QR_p test

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

Another Proof of QR_p test

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

($\Rightarrow$) ★ If $y \in QR_p$

Another Proof of QR_p test

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

($\Rightarrow$)
- If $y \in QR_p$
- Then $\exists x \in Z_p^*$ such that $y \equiv x^2 \pmod{p}$

Another Proof of QR_p test

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

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

Another Proof of QR_p test

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

($\Rightarrow$) ★ If $y \in QR_p$

★ Then $\exists x \in Z_p^*$ such that $y \equiv x^2 \pmod{p}$

★ Therefore, $y^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{(p-1)} \equiv 1 \pmod{p}$

($\Leftarrow$) ★ $\forall i, y \in Z_p^*$, $\gcd(i, p)=1$, $\exists j$ such that $i \cdot j \equiv y \pmod{p}$

Another Proof of QR_p test

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

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

($\Leftarrow$)
- $\forall i, y \in Z_p^*$, $\gcd(i, p)=1$, $\exists j$ such that $i \cdot j \equiv y \pmod{p}$
- If $y \notin QR_p$, the congruence $x^2 \equiv y \pmod{p}$ has no solution, therefore, $j \neq i \pmod{p}$

Another Proof of QR_p test

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

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

($\Leftarrow$)
- $\forall i, y \in Z_p^*$, $\gcd(i, p)=1$, $\exists j$ such that $i \cdot j \equiv y \pmod{p}$
- If $y \notin QR_p$, the congruence $x^2 \equiv y \pmod{p}$ has no solution, therefore, $j \neq i \pmod{p}$
- We can group the integers 1, 2, …, p-1 into $(p-1)/2$ pairs (i, j), each satisfying $i \cdot j \equiv y \pmod{p}$

Another Proof of QR_p test

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

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

($\Leftarrow$)
- $\forall i, y \in Z_p^*$, $\gcd(i, p)=1$, $\exists j$ such that $i \cdot j \equiv y \pmod{p}$
- If $y \notin QR_p$, the congruence $x^2 \equiv y \pmod{p}$ has no solution, therefore, $j \neq i \pmod{p}$
- We can group the integers 1, 2, …, p-1 into $(p-1)/2$ pairs (i, j), each satisfying $i \cdot j \equiv y \pmod{p}$
- Multiply them together, we have $(p-1)! \equiv y^{(p-1)/2} \pmod{p}$

Another Proof of QR_p test

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

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

($\Leftarrow$)
- $\forall i, y \in Z_p^*$, $\gcd(i, p)=1$, $\exists j$ such that $i \cdot j \equiv y \pmod{p}$
- If $y \notin QR_p$, the congruence $x^2 \equiv y \pmod{p}$ has no solution, therefore, $j \neq i \pmod{p}$
- We can group the integers 1, 2, …, p-1 into $(p-1)/2$ pairs (i, j), each satisfying $i \cdot j \equiv y \pmod{p}$
- Multiply them together, we have $(p-1)! \equiv y^{(p-1)/2} \pmod{p}$
- From Wilson's theorem, $y^{(p-1)/2} \equiv -1 \pmod{p}$

Exactly Two Square Roots

Every $y \in QR_p$ has exactly two square roots

i.e. x and $p-x$ such that $x^2 \equiv (p-x)^2 \equiv y \pmod{p}$

Exactly Two Square Roots

Every $y \in QR_p$ has exactly two square roots

i.e. x and $p-x$ such that $x^2 \equiv (p-x)^2 \equiv y \pmod{p}$

Exactly Two Square Roots

Every $y \in QR_p$ has exactly two square roots

i.e. x and p-x such that $x^2 \equiv (p-x)^2 \equiv y \pmod{p}$

pf: ⋆ $QR_p = \{g^2, g^4, \ldots, g^{p-1}\}$, $|Z_p^*| = p-1$, and $|QR_p| = (p-1)/2$

Exactly Two Square Roots

Every $y \in QR_p$ has exactly two square roots

i.e. x and $p-x$ such that $x^2 \equiv (p-x)^2 \equiv y \pmod{p}$

pf:

- ★ $QR_p = \{g^2, g^4, \ldots, g^{p-1}\}$, $|Z_p^*| = p-1$, and $|QR_p| = (p-1)/2$
- ★ For each $y \equiv g^{2k}$ in QR_p, there are at least two distinct $x \in Z_p^*$ s.t. $x^2 \equiv y \pmod{p}$, i.e., g^k and $p-g^k$ (if one is even, the other is odd)

Exactly Two Square Roots

Every $y \in QR_p$ has exactly two square roots

i.e. x and $p-x$ such that $x^2 \equiv (p-x)^2 \equiv y \pmod{p}$

pf:

- ★ $QR_p = \{g^2, g^4, \ldots, g^{p-1}\}$, $|Z_p^*| = p-1$, and $|QR_p| = (p-1)/2$
- ★ For each $y \equiv g^{2k}$ in QR_p, there are at least two distinct $x \in Z_p^*$ s.t. $x^2 \equiv y \pmod{p}$, i.e., g^k and $p-g^k$ (if one is even, the other is odd)
- ★ Since $|QR_p| = (p-1)/2$, we can obtain a set of $p-1$ square roots $S = \{g, p-g, g^2, p-g^2, \ldots, g^{(p-1)/2}, p-g^{(p-1)/2}\}$

Exactly Two Square Roots

Every $y \in QR_p$ has exactly two square roots

i.e. x and $p-x$ such that $x^2 \equiv (p-x)^2 \equiv y \pmod{p}$

pf:

- ★ $QR_p = \{g^2, g^4, \ldots, g^{p-1}\}$, $|Z_p^*| = p-1$, and $|QR_p| = (p-1)/2$
- ★ For each $y \equiv g^{2k}$ in QR_p, there are at least two distinct $x \in Z_p^*$ s.t. $x^2 \equiv y \pmod{p}$, i.e., g^k and $p-g^k$ (if one is even, the other is odd)
- ★ Since $|QR_p| = (p-1)/2$, we can obtain a set of $p-1$ square roots $S = \{g, p-g, g^2, p-g^2, \ldots, g^{(p-1)/2}, p-g^{(p-1)/2}\}$
- ★ **Claim**: the elements of S are all distinct (1. $g^i \neq g^j \pmod{p}$ when $i \neq j$ since g is a primitive, 2. $g^i \neq -g^j \pmod{p}$ when $i \neq j$, otherwise $(g^i+g^j)(g^i-g^j) \equiv g^{2i}-g^{2j} \equiv 0 \pmod{p}$ implies $i \neq j \pmod{(p-1)/2}$, 3. $g^i \neq -g^i \pmod{p}$ since if one is even, the other is odd)

Exactly Two Square Roots

Every $y \in QR_p$ has exactly two square roots

i.e. x and $p-x$ such that $x^2 \equiv (p-x)^2 \equiv y \pmod p$

pf:

- ★ $QR_p = \{g^2, g^4, \ldots, g^{p-1}\}$, $|Z_p^*| = p-1$, and $|QR_p| = (p-1)/2$
- ★ For each $y \equiv g^{2k}$ in QR_p, there are at least two distinct $x \in Z_p^*$ s.t. $x^2 \equiv y \pmod p$, i.e., g^k and $p-g^k$ (if one is even, the other is odd)
- ★ Since $|QR_p| = (p-1)/2$, we can obtain a set of $p-1$ square roots $S = \{g, p-g, g^2, p-g^2, \ldots, g^{(p-1)/2}, p-g^{(p-1)/2}\}$
- ★ **Claim**: the elements of S are all distinct (1. $g^i \neq g^j \pmod p$ when $i \neq j$ since g is a primitive, 2. $g^i \neq -g^j \pmod p$ when $i \neq j$, otherwise $(g^i+g^j)(g^i-g^j) \equiv g^{2i}-g^{2j} \equiv 0 \pmod p$ implies $i \neq j \pmod{(p-1)/2}$, 3. $g^i \neq -g^i \pmod p$ since if one is even, the other is odd)
- ★ If there is one more square root z of $y \equiv g^{2k}$ which is not g^k and $-g^k$, it must belong to S (which is Z_p^*), say g^j, $j \neq k$, which would imply that $g^{2j} \equiv g^{2k} \pmod p$, and leads to contradiction

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*
- Let $p = k \cdot q + 1$ i.e. $q \mid p\text{-}1$ where q is also a prime number

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*
- Let $p = k \cdot q + 1$ i.e. $q \mid p\text{-}1$ where q is also a prime number
- Let $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*
- Let $p = k \cdot q + 1$ i.e. $q \mid p\text{-}1$ where q is also a prime number
- Let $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$
- Is G_q a subgroup in Z_p^*? YES

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*
- Let $p = k \cdot q + 1$ i.e. $q \mid p\text{-}1$ where q is also a prime number
- Let $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$
- Is G_q a subgroup in Z_p^*? YES

  $\forall\ x, y$ G_q, it is clear that z $g^{i \cdot k}$ $x \cdot y$ $g^{(i1+i2) \cdot k} \pmod p$

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*
- Let $p = k \cdot q + 1$ i.e. $q \mid p\text{-}1$ where q is also a prime number
- Let $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$
- Is G_q a subgroup in Z_p^*? YES

  $\forall\, x, y$ G_q, it is clear that z $g^{i \cdot k}$ $x \cdot y$ $g^{(i1+i2) \cdot k} \pmod p$

  is also in G_q, where $i \equiv i_1 + i_2 \pmod q$

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*
- Let $p = k \cdot q + 1$ i.e. $q \mid p\text{-}1$ where q is also a prime number
- Let $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$
- Is G_q a subgroup in Z_p^*? YES

  $\forall\, x, y$ G_q, it is clear that z $g^{i \cdot k}$ $x \cdot y$ $g^{(i1+i2) \cdot k} \pmod p$

  is also in G_q, where $i \equiv i_1 + i_2 \pmod q$
- Is the order of the subgroup G_q q? YES

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*
- Let $p = k \cdot q + 1$ i.e. $q \mid p\text{-}1$ where q is also a prime number
- Let $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$
- Is G_q a subgroup in Z_p^*? YES

  $\forall\ x, y$ G_q, it is clear that z $g^{i \cdot k}$ $x \cdot y$ $g^{(i1+i2) \cdot k} \pmod p$

  is also in G_q, where $i \equiv i_1 + i_2 \pmod q$
- Is the order of the subgroup G_q q? YES

  $\forall\ i_1, i_2$ Z_q, i_1 i_2, $g^{i1 \cdot k}$ $g^{i2 \cdot k} \pmod p$ otherwise g is not a

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*
- Let $p = k \cdot q + 1$ i.e. $q \mid p\text{-}1$ where q is also a prime number
- Let $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$
- Is G_q a subgroup in Z_p^*? YES

  $\forall\ x, y$ G_q, it is clear that z $g^{i \cdot k}$ $x \cdot y$ $g^{(i1+i2) \cdot k} \pmod p$ is also in G_q, where $i \equiv i_1 + i_2 \pmod q$
- Is the order of the subgroup G_q q? YES

  $\forall\ i_1, i_2$ Z_q, i_1 i_2, $g^{i1 \cdot k}$ $g^{i2 \cdot k} \pmod p$ otherwise g is not a primitive in Z_p^*, also $g^{q \cdot k} \equiv 1 \pmod p$

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*
- Let $p = k \cdot q + 1$ i.e. $q \mid p\text{-}1$ where q is also a prime number
- Let $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$
- Is G_q a subgroup in Z_p^*? YES

  $\forall\ x, y$ G_q, it is clear that z $g^{i \cdot k}$ $x \cdot y$ $g^{(i1+i2) \cdot k} \pmod p$ is also in G_q, where $i \equiv i_1 + i_2 \pmod q$
- Is the order of the subgroup G_q q? YES

  $\forall\ i_1, i_2$ Z_q, i_1 i_2, $g^{i1 \cdot k}$ $g^{i2 \cdot k} \pmod p$ otherwise g is not a primitive in Z_p^*, also $g^{q \cdot k} \equiv 1 \pmod p$
- How many generators are there in G_q? $\phi(q)=q\text{-}1$

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*
- Let $p = k \cdot q + 1$ i.e. $q \mid p\text{-}1$ where q is also a prime number
- Let $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$
- Is G_q a subgroup in Z_p^*? YES

  $\forall\ x, y$ G_q, it is clear that z $g^{i \cdot k}$ $x \cdot y$ $g^{(i1+i2) \cdot k} \pmod p$ is also in G_q, where $i \equiv i_1 + i_2 \pmod q$
- Is the order of the subgroup G_q q? YES

  $\forall\ i_1, i_2$ Z_q, i_1 i_2, $g^{i1 \cdot k}$ $g^{i2 \cdot k} \pmod p$ otherwise g is not a primitive in Z_p^*, also $g^{q \cdot k} \equiv 1 \pmod p$
- How many generators are there in G_q? $\phi(q)=q\text{-}1$

  a. there are $\phi(p\text{-}1)$ generators in $Z_p^* = \{g^1, g^2, \ldots, g^x, \ldots, g^{p-1}\}$, since

Order q Subgroup G_q of Z_p^*

- Let p be a prime number, g be a primitive in Z_p^*
- Let $p = k \cdot q + 1$ i.e. $q \mid p\text{-}1$ where q is also a prime number
- Let $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$
- Is G_q a subgroup in Z_p^*? YES

  $\forall\ x, y$ G_q, it is clear that z $g^{i \cdot k}$ $x \cdot y$ $g^{(i1+i2) \cdot k} \pmod p$ is also in G_q, where $i \equiv i_1 + i_2 \pmod q$
- Is the order of the subgroup G_q q? YES

  $\forall\ i_1, i_2$ Z_q, i_1 i_2, $g^{i1 \cdot k}$ $g^{i2 \cdot k} \pmod p$ otherwise g is not a primitive in Z_p^*, also $g^{q \cdot k} \equiv 1 \pmod p$
- How many generators are there in G_q? $\phi(q)=q\text{-}1$

  a. there are $\phi(p\text{-}1)$ generators in $Z_p^* = \{g^1, g^2, \ldots, g^x, \ldots, g^{p-1}\}$, since $\gcd(p\text{-}1, x) = d > 1$ implies that $\text{ord}_p(g^x) = (p\text{-}1)/d$

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

therefore, $\text{ord}_p(g^x) = p\text{-}1$

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

therefore, $\text{ord}_p(g^x) = p\text{-}1$

b. there are $\phi(q)$ primitives in $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$ since

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

therefore, $\text{ord}_p(g^x) = p\text{-}1$

b. there are $\phi(q)$ primitives in $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$ since q is also a prime number

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

therefore, $\text{ord}_p(g^x) = p\text{-}1$

b. there are $\phi(q)$ primitives in $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$ since q is also a prime number

- **Is G_q a unique order q subgroup in Z_p^* ?** YES

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

therefore, $\text{ord}_p(g^x) = p\text{-}1$

b. there are $\phi(q)$ primitives in $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$ since q is also a prime number

- **Is G_q a unique order q subgroup in Z_p^* ?** YES

  Let S be an order-q cyclic subgroup, $S = \{g, g^2, \ldots, g^q \equiv 1\}$. Since

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

therefore, $\text{ord}_p(g^x) = p\text{-}1$

b. there are $\phi(q)$ primitives in $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$ since q is also a prime number

- **Is G_q a unique order q subgroup in Z_p^* ?** YES

  Let S be an order-q cyclic subgroup, $S = \{g, g^2, \ldots, g^q \equiv 1\}$. Since p is prime, $\exists$ a unique k-th root $g_1 \in Z_p^*$, s.t. $g \equiv g_1^k \pmod{p}$

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

therefore, $\text{ord}_p(g^x) = p\text{-}1$

b. there are $\phi(q)$ primitives in $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$ since q is also a prime number

- **Is G_q a unique order q subgroup in Z_p^* ?** YES

Let S be an order-q cyclic subgroup, $S = \{g, g^2, \ldots, g^q \equiv 1\}$. Since p is prime, $\exists$ a unique k-th root $g_1 \in Z_p^*$, s.t. $g \equiv g_1^k \pmod{p}$

Let $g_1 \neq g$ be another primitive, clearly $g_1 \neq g^s \pmod{p}$,

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

therefore, $\text{ord}_p(g^x) = p\text{-}1$

b. there are $\phi(q)$ primitives in $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$ since q is also a prime number

- **Is G_q a unique order q subgroup in Z_p^* ?** YES

Let S be an order-q cyclic subgroup, $S = \{g, g^2, \ldots, g^q \equiv 1\}$. Since p is prime, $\exists$ a unique k-th root $g_1 \in Z_p^*$, s.t. $g \equiv g_1^k \pmod{p}$

Let $g_1 \neq g$ be another primitive, clearly $g_1 \neq g^s \pmod{p}$,

Is the set $S = \{g_1^k, g_1^{2k}, \ldots, g_1^{q \cdot k} \equiv 1\}$ different from G_q?

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

therefore, $\text{ord}_p(g^x) = p\text{-}1$

b. there are $\phi(q)$ primitives in $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$ since q is also a prime number

- **Is G_q a unique order q subgroup in Z_p^* ?** YES

Let S be an order-q cyclic subgroup, $S = \{g, g^2, \ldots, g^q \equiv 1\}$. Since p is prime, $\exists$ a unique k-th root $g_1 \in Z_p^*$, s.t. $g \equiv g_1^k \pmod{p}$

Let $g_1 \neq g$ be another primitive, clearly $g_1 \neq g^s \pmod{p}$,

Is the set $S = \{g_1^k, g_1^{2k}, \ldots, g_1^{q \cdot k} \equiv 1\}$ different from G_q?

let $x \in S$, i.e. $x \equiv g_1^{i1 \cdot k} \pmod{p}$, $i_1 \in Z_q$

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

therefore, $\text{ord}_p(g^x) = p\text{-}1$

b. there are $\phi(q)$ primitives in $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$ since q is also a prime number

- **Is G_q a unique order q subgroup in Z_p^* ?** YES

Let S be an order-q cyclic subgroup, $S = \{g, g^2, \ldots, g^q \equiv 1\}$. Since p is prime, $\exists$ a unique k-th root $g_1 \in Z_p^*$, s.t. $g \equiv g_1^k \pmod{p}$

Let $g_1 \neq g$ be another primitive, clearly $g_1 \equiv g^s \pmod{p}$,

Is the set $S = \{g_1^k, g_1^{2k}, \ldots, g_1^{q \cdot k} \equiv 1\}$ different from G_q?

let $x \in S$, i.e. $x \equiv g_1^{i_1 \cdot k} \pmod{p}$, $i_1 \in Z_q$

$x \equiv g_1^{i_1 \cdot k} \equiv g^{s \cdot i_1 \cdot k} \equiv g^{i \cdot k} \pmod{p}$ where $i \equiv s \cdot i_1 \pmod{q}$, i.e. $S \subseteq G_q$

Order q Subgroup G_q (cont'd)

also $(g^x)^y \equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$ implies that either $x \cdot y \mid p\text{-}1$ or $p\text{-}1 \mid x \cdot y$, $\gcd(x, p\text{-}1) = 1$ implies that $p\text{-}1 \mid y$

therefore, $\text{ord}_p(g^x) = p\text{-}1$

b. there are $\phi(q)$ primitives in $G_q = \{g^k, g^{2k}, \ldots, g^{q \cdot k} \equiv 1\}$ since q is also a prime number

- **Is G_q a unique order q subgroup in Z_p^* ?** YES

Let S be an order-q cyclic subgroup, $S = \{g, g^2, \ldots, g^q \equiv 1\}$. Since p is prime, $\exists$ a unique k-th root $g_1 \in Z_p^*$, s.t. $g \equiv g_1^k \pmod{p}$

Let $g_1 \neq g$ be another primitive, clearly $g_1 \neq g^s \pmod{p}$,

Is the set $S = \{g_1^k, g_1^{2k}, \ldots, g_1^{q \cdot k} \equiv 1\}$ different from G_q?

let $x \in S$, i.e. $x \equiv g_1^{i_1 \cdot k} \pmod{p}$, $i_1 \in Z_q$

$x \equiv g_1^{i_1 \cdot k} \equiv g^{s \cdot i_1 \cdot k} \equiv g^{i \cdot k} \pmod{p}$ where $i \equiv s \cdot i_1 \pmod{q}$, i.e. $S \subseteq G_q$

The proof is similar for $G_q \subseteq S$. Therefore, $S = G_q$

Gauss' Lemma

Lemma: let p be a prime, a is an integer s.t. gcd(a, p)=1,

define $\{\alpha_j \equiv j \cdot a \pmod p\}_{j=1,\ldots,(p-1)/2}$,

let n be the number of α_j's s.t. $\alpha_j > p/2$ then $L(a, p) = (-1)^n$

pf.

- ✶ $\alpha_j \in \{r_1, \ldots, r_n\}$ if $\alpha_j > p/2$ and $\alpha_j \in \{s_1, \ldots, s_{(p-1)/2-n}\}$ if $\alpha_j < p/2$
- ✶ Since gcd(a, p)=1, r_i and s_i are all distinct and non-zero
- ✶ Clearly, $0 < p-r_i < p/2$ for i=1,…,n
- ✶ no $p-r_i$ is an s_j: if $p-r_i=s_j$ then $s_j \equiv -r_i \pmod p$

rewrite in terms of a: $u\,a \equiv -v\,a \pmod p$ where $1 \le u, v \le (p-1)/2$

$\Rightarrow u \equiv -v \pmod p$ where $1 \le u, v \le (p-1)/2 \Rightarrow$ impossible

$\Rightarrow \{s_1, \ldots, s_{(p-1)/2-n}, p-r_1, \ldots, p-r_n\}$ is a reordering of $\{1, 2, \ldots, (p-1)/2\}$

- ✶ Thus, $((p-1)/2)! \equiv s_1 \cdots s_{(p-1)/2-n} \cdot (-r_1) \cdots (-r_n) \equiv (-1)^n\, s_1 \cdots s_{(p-1)/2-n} \cdot r_1 \cdots r_n$

$\equiv (-1)^n\, ((p-1)/2)!\, a^{(p-1)/2} \pmod p \Rightarrow L(a, p) = (-1)^n$

Theorem: $J(2, p) = (-1)^{(p^2-1)/8}$

Theorem: let p be a prime, gcd(a, p) = 1 then $L(a, p) = (-1)^t$

where $t = \sum_{j=1}^{(p-1)/2} \lfloor j \cdot a/p \rfloor$. Also $L(2, p) = (-1)^{(p^2-1)/8}$

pf.

- ✶ $\alpha_j \in \{r_1, \ldots, r_n\}$ if $\alpha_j > p/2$ and $\alpha_j \in \{s_1, \ldots, s_{(p-1)/2-n}\}$ if $\alpha_j < p/2$
- ✶ $j\, a = p \lfloor j \cdot a/p \rfloor + \alpha_j$ for $j=1, \ldots, (p-1)/2$

$$\Rightarrow \sum_{j=1}^{(p-1)/2} j\, a = \sum_{j=1}^{(p-1)/2} p \lfloor j \cdot a/p \rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{(p-1)/2-n} s_j$$

- ✶ $\{s_1, \ldots, s_{(p-1)/2-n}, p-r_1, \ldots, p-r_n\}$ is a reordering of $\{1, 2, \ldots, (p-1)/2\}$

$$\Rightarrow \sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{n} (p-r_j) + \sum_{j=1}^{(p-1)/2-n} s_j = np - \sum_{j=1}^{n} r_j + \sum_{j=1}^{(p-1)/2-n} s_j$$

- ✶ Subtracting the above two equations, we have

$$(a-1) \sum_{j=1}^{(p-1)/2} j = p \left(\sum_{j=1}^{(p-1)/2} \lfloor j \cdot a/p \rfloor - n \right) + 2 \sum_{j=1}^{n} r_j$$

$J(2, p) = (-1)^{(p^2-1)/8}$ (cont'd)

- $\sum_{j=1}^{(p-1)/2} j = 1 + \ldots + (p-1)/2 = (p-1)/2\,(1 + (p-1)/2) / 2 = (p^2-1)/8$
- Thus, we have $(a-1)\,(p^2-1)/8 \equiv \sum_{j=1}^{(p-1)/2} \lfloor j \cdot a/p \rfloor - n \pmod 2$

- If a is odd, $n \equiv \sum_{j=1}^{(p-1)/2} \lfloor j \cdot a/p \rfloor$
- If $a = 2$, $\lfloor j \cdot 2/p \rfloor = 0$ for $j=1, \ldots, (p-1)/2$, $n \equiv (p^2-1)/8 \pmod 2$

therefore, $J(2, p) = (-1)^{(p^2-1)/8}$

Lemma. ord-k elements in $Z_p^* \leq \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

Lemma. ord-k elements in $Z_p^* \leq \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k - 1 \equiv 0 \pmod{p}$ has at most k roots

Lemma. ord-k elements in $Z_p^* \leq \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

e.g. p = 13

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if a is a nontrivial root ($a \neq 1$), then $\{a^0, a^1, a^2, \ldots, a^{k-1}\}$ is the set of the k distinct roots.

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1}

k=6, {4, 3, 12, 9, 10, 1}

$(2^{(p-1)/k})^j = (2^2)^j$

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1}

k=6, {4, 3, 12, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1}

k=6, {4, 3, 12, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1}

k=6, {4, 3, 12, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, 12, 11, 9, 5, 10, 7, 1}

k=6, {4, 3, 12, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1}

k=6, {4, 3, 12, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if a is a nontrivial root ($a \neq 1$), then $\{a^0, a^1, a^2, \ldots, a^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, 5, 10, 7, 1}

k=6, {4, 3, 12, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, 10, 7, 1}

k=6, {4, 3, 12, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^{ℓ} with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, 1}

k=6, {4, 3, 12, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {4, 3, 12, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {4, 3, 12, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {4, ~~8~~, 12, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {4, ~~8~~, ~~12~~, 9, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {4, ~~8~~, ~~12~~, ~~9~~, 10, 1}

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {~~4~~, ~~3~~, ~~12~~, ~~9~~, 10, ~~1~~}, $\phi(6)$

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {~~4~~, ~~8~~, ~~12~~, ~~3~~, 10, ~~1~~}, $\phi(6)$

k=4, {8, 12, 5, 1}, $\phi(4)$

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {~~4~~, ~~8~~, ~~12~~, ~~9~~, 10, ~~1~~}, $\phi(6)$

k=4, {~~8~~, ~~12~~, 5, 1}, $\phi(4)$

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {~~4~~, ~~8~~, ~~12~~, ~~3~~, 10, ~~1~~}, $\phi(6)$

k=4, {~~8~~, ~~12~~, 5, ~~1~~}, $\phi(4)$

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {4, ~~8~~, ~~12~~, ~~9~~, 10, ~~1~~}, $\phi(6)$ k=3, {3, 9, 1}, $\phi(3)$

k=4, {8, ~~12~~, 5, ~~1~~}, $\phi(4)$

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {4, ~~8~~, ~~12~~, ~~9~~, 10, ~~1~~}, $\phi(6)$ k=3, {3, 9, ~~1~~}, $\phi(3)$

k=4, {8, ~~12~~, 5, ~~1~~}, $\phi(4)$

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if a is a nontrivial root ($a \neq 1$), then $\{a^0, a^1, a^2, \ldots, a^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1}, $\phi(12)$

k=6, {4, 3, 12, 9, 10, 1}, $\phi(6)$ k=3, {3, 9, 1}, $\phi(3)$

k=4, {8, 12, 5, 1}, $\phi(4)$ k=2, {12, 1}, $\phi(2)$

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {4, ~~8~~, ~~12~~, ~~9~~, 10, ~~1~~}, $\phi(6)$ k=3, {3, 9, ~~1~~}, $\phi(3)$

k=4, {8, ~~12~~, 5, ~~1~~}, $\phi(4)$ k=2, {12, ~~1~~}, $\phi(2)$

Lemma. ord-k elements in $Z_p^* \le \phi(k)$

Lemma. There are at most $\phi(k)$ ord-k elements in Z_p^*, $k \mid p-1$

pf. ✧ Z_p^* is a field $\Rightarrow$ $x^k-1 \equiv 0 \pmod p$ has at most k roots

✧ if $\boldsymbol{a}$ is a nontrivial root ($\boldsymbol{a} \neq 1$), then $\{\boldsymbol{a}^0, \boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}\}$ is the set of the k distinct roots.

✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most **k/d**

✧ Only those a^ℓ with $\gcd(\ell, k) = 1$ might have order k

✧ Hence, there are at most $\phi(k)$ order k elements

e.g. p = 13 $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

2 is a generator in $Z_{13}^* = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\}$

k=12, {2, ~~4~~, ~~8~~, ~~3~~, 6, ~~12~~, 11, ~~9~~, ~~5~~, ~~10~~, 7, ~~1~~}, $\phi(12)$

k=6, {4, ~~8~~, ~~12~~, ~~9~~, 10, ~~1~~}, $\phi(6)$ k=3, {3, 9, ~~1~~}, $\phi(3)$

k=4, {8, ~~12~~, 5, ~~1~~}, $\phi(4)$ k=2, {12, ~~1~~}, $\phi(2)$ k=1, {1}, $\phi(1)$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$p-1 = \Sigma_{k|p-1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$p-1 = \Sigma_{k|p-1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

let p=13, $a \in Z_p^*$

gcd(a, p-1)=k $\Rightarrow$ k | p-1

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$p-1 = \Sigma_{k|p-1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

let p=13, $a \in Z_p^*$

gcd(a, p-1)=k $\Rightarrow$ k | p-1

k=1, {1,5,7,11}, $\phi(12/1)$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$p-1 = \Sigma_{k|p-1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

let p=13, $a \in Z_p^*$

gcd(a, p-1)=k $\Rightarrow$ k | p-1

k=1, {1,5,7,11}, $\phi(12/1)$

k=2, {2,10}, $\phi(12/2)$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$p-1 = \Sigma_{k|p-1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

let p=13, $a \in Z_p^*$

gcd(a, p-1)=k $\Rightarrow$ k | p-1

k=1, {1,5,7,11}, $\phi(12/1)$

k=2, {2,10}, $\phi(12/2)$

k=3, {3,9}, $\phi(12/3)$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$p-1 = \Sigma_{k|p-1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

let p=13, $a \in Z_p^*$

gcd(a, p-1)=k $\Rightarrow$ k | p-1

k=1, {1,5,7,11}, $\phi(12/1)$

k=2, {2,10}, $\phi(12/2)$

k=3, {3,9}, $\phi(12/3)$

k=4, {4,8}, $\phi(12/4)$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$p-1 = \Sigma_{k|p-1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

let p=13, $a \in Z_p^*$

gcd(a, p-1)=k $\Rightarrow$ k | p-1

k=1, {1,5,7,11}, $\phi(12/1)$

k=2, {2,10}, $\phi(12/2)$

k=3, {3,9}, $\phi(12/3)$

k=4, {4,8}, $\phi(12/4)$

k=6, {6}, $\phi(12/6)$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$p-1 = \Sigma_{k|p-1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

let p=13, $a \in Z_p^*$

gcd(a, p-1)=k $\Rightarrow$ k | p-1

k=1, {1,5,7,11}, ϕ(12/1)

k=2, {2,10}, ϕ(12/2)

k=3, {3,9}, ϕ(12/3)

k=4, {4,8}, ϕ(12/4)

k=6, {6}, ϕ(12/6)

k=12, {12}, ϕ(12/12)

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$$p-1 = \Sigma_{k|p-1}\ (\#\ a \text{ in } Z_p^*\ \text{s.t. } \gcd(a, p-1) = k)$$

$$= \Sigma_{k|p-1}\ (\#\ b \text{ in } \{1,\ldots,(p-1)/k\}\ \text{s.t. } \gcd(b, (p-1)/k) = 1)$$

a/k

let p=13, $a \in Z_p^*$

$\gcd(a, p-1)=k \Rightarrow k \mid p-1$

k=1, {1,5,7,11}, $\phi(12/1)$

k=2, {2,10}, $\phi(12/2)$

k=3, {3,9}, $\phi(12/3)$

k=4, {4,8}, $\phi(12/4)$

k=6, {6}, $\phi(12/6)$

k=12, {12}, $\phi(12/12)$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$$p-1 = \Sigma_{k|p-1}\ (\#\ a \text{ in } Z_p^*\ \text{s.t. } \gcd(a, p-1) = k)$$

$$= \Sigma_{k|p-1}\ (\#\ b \text{ in } \{1,\ldots,(p-1)/k\}\ \text{s.t. } \gcd(b, (p-1)/k) = 1)$$

$$= \Sigma_{k|p-1}\ \phi((p-1)/k)$$

a/k

let p=13, $a \in Z_p^*$

$\gcd(a, p-1)=k \Rightarrow k \mid p-1$

k=1, {1,5,7,11}, $\phi(12/1)$

k=2, {2,10}, $\phi(12/2)$

k=3, {3,9}, $\phi(12/3)$

k=4, {4,8}, $\phi(12/4)$

k=6, {6}, $\phi(12/6)$

k=12, {12}, $\phi(12/12)$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$$p-1 = \Sigma_{k|p-1}\ (\#\ a \text{ in } Z_p^*\ \text{s.t. } \gcd(a, p-1) = k)$$

$$= \Sigma_{k|p-1}\ (\#\ b \text{ in } \{1,\ldots,(p-1)/k\}\ \text{s.t. } \gcd(b, (p-1)/k) = 1)$$

$$= \Sigma_{k|p-1}\ \phi((p-1)/k)$$

a/k

let p=13, $a \in Z_p^*$

$\gcd(a, p-1)=k \Rightarrow k \mid p-1$

k=1, {1,5,7,11}, $\phi(12/1)$

k=2, {2,10}, $\phi(12/2)$

k=3, {3,9}, $\phi(12/3)$

k=4, {4,8}, $\phi(12/4)$

k=6, {6}, $\phi(12/6)$

k=12, {12}, $\phi(12/12)$

$\{\phi(1\}, \phi(2), \phi(3), \phi(4), \phi(6), \phi(12)\}$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

$$p-1 = \Sigma_{k|p-1}\ (\#\ a \text{ in } Z_p^*\ \text{s.t. } \gcd(a, p-1) = k)$$

$$= \Sigma_{k|p-1}\ (\#\ b \text{ in } \{1,\ldots,(p-1)/k\}\ \text{s.t. } \gcd(b, (p-1)/k) = 1)$$

$$= \Sigma_{k|p-1}\ \phi((p-1)/k)$$

a/k

let p=13, $a \in Z_p^*$

$\gcd(a, p-1)=k \Rightarrow k \mid p-1$

k=1, {1,5,7,11}, $\phi(12/1)$

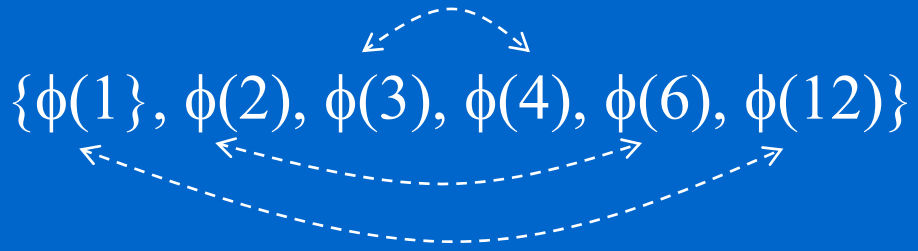
k=2, {2,10}, $\phi(12/2)$

k=3, {3,9}, $\phi(12/3)$

k=4, {4,8}, $\phi(12/4)$

k=6, {6}, $\phi(12/6)$

k=12, {12}, $\phi(12/12)$



Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$

Lemma. $\Sigma_{k|p-1}\ \phi(k) = p-1$ let $\phi(1)=1$

pf.

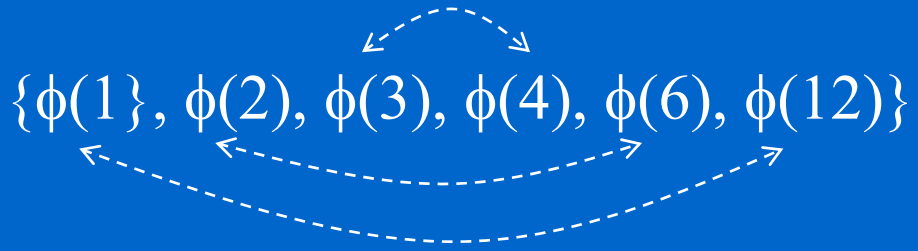
$$p-1 = \Sigma_{k|p-1}\ (\#\ a \text{ in } Z_p^*\ \text{s.t. } \gcd(a, p-1) = k)$$

$$= \Sigma_{k|p-1}\ (\#\ b \text{ in } \{1,\ldots,(p-1)/k\}\ \text{s.t. } \gcd(b, (p-1)/k) = 1)$$

$$= \Sigma_{k|p-1}\ \phi((p-1)/k)$$

$$= \Sigma_{k|p-1}\ \phi(k)$$

a/k



let p=13, $a \in Z_p^*$

$\gcd(a, p-1)=k \Rightarrow k \mid p-1$

k=1, {1,5,7,11}, ϕ(12/1)

k=2, {2,10}, ϕ(12/2)

k=3, {3,9}, ϕ(12/3)

k=4, {4,8}, ϕ(12/4)

k=6, {6}, ϕ(12/6)

k=12, {12}, ϕ(12/12)

Z_p^* is a *cyclic* group

Theorem: Z_p^* is a *cyclic* group for a prime number p

Z_p^* is a *cyclic* group

Theorem: Z_p^* is a *cyclic* group for a prime number p

pf. Lemma 1: # of ord-k elements in $Z_p^* \leq \phi(k)$, where $k \mid p-1$

Lemma 2: $\Sigma_{k|p-1}\ \phi(k) = p-1$

Z_p^* is a *cyclic* group

Theorem: Z_p^* is a *cyclic* group for a prime number p

pf. Lemma 1: # of ord-k elements in $Z_p^* \leq \phi(k)$, where $k \mid p-1$

Lemma 2: $\Sigma_{k|p-1}\ \phi(k) = p-1$

The order k of every element in Z_p^* divides p-1

Z_p^* is a *cyclic* group

Theorem: Z_p^* is a *cyclic* group for a prime number p

pf. Lemma 1: # of ord-k elements in $Z_p^* \le \phi(k)$, where $k \mid p-1$

Lemma 2: $\Sigma_{k|p-1}\ \phi(k) = p-1$

The order k of every element in Z_p^* divides p-1

$\Rightarrow \Sigma_{k|p-1}$ (# of elements in Z_p^* with order k) = p-1

Z_p^* is a *cyclic* group

Theorem: Z_p^* is a *cyclic* group for a prime number p

pf. Lemma 1: # of ord-k elements in $Z_p^* \le \phi(k)$, where $k \mid p-1$

Lemma 2: $\Sigma_{k|p-1}\ \phi(k) = p-1$

The order k of every element in Z_p^* divides p-1

$\Rightarrow \Sigma_{k|p-1}$ (# of elements in Z_p^* with order k) = p-1

(Lemma 1) $\Rightarrow p-1 \le \Sigma_{k|p-1}\ \phi(k)$, combined with lemma 2,

we know that # of ord-k elements in $Z_p^* = \phi(k)$

Z_p^* is a *cyclic* group

Theorem: Z_p^* is a *cyclic* group for a prime number p

pf. Lemma 1: # of ord-k elements in $Z_p^* \le \phi(k)$, where $k \mid p-1$

Lemma 2: $\Sigma_{k|p-1}\ \phi(k) = p-1$

The order k of every element in Z_p^* divides p-1

$\Rightarrow \Sigma_{k|p-1}$ (# of elements in Z_p^* with order k) = p-1

(Lemma 1) $\Rightarrow p-1 \le \Sigma_{k|p-1}\ \phi(k)$, combined with lemma 2,

we know that # of ord-k elements in $Z_p^* = \phi(k)$

$\Rightarrow$ # of ord-(p-1) elements in $Z_p^* = \phi(p-1) > 1$

Z_p^* is a *cyclic* group

Theorem: Z_p^* is a *cyclic* group for a prime number p

pf. Lemma 1: # of ord-k elements in $Z_p^* \le \phi(k)$, where $k \mid p-1$

Lemma 2: $\Sigma_{k|p-1}\ \phi(k) = p-1$

The order k of every element in Z_p^* divides p-1

$\Rightarrow \Sigma_{k|p-1}$ (# of elements in Z_p^* with order k) = p-1

(Lemma 1) $\Rightarrow p-1 \le \Sigma_{k|p-1}\ \phi(k)$, combined with lemma 2,

we know that # of ord-k elements in $Z_p^* = \phi(k)$

$\Rightarrow$ # of ord-(p-1) elements in $Z_p^* = \phi(p-1) > 1$

$\Rightarrow$ There is at least one generator in Z_p^*, i.e. Z_p^* is cyclic

Z_p^* is a *cyclic* group

Theorem: Z_p^* is a *cyclic* group for a prime number p

pf. Lemma 1: # of ord-k elements in $Z_p^* \le \phi(k)$, where $k \mid p-1$

Lemma 2: $\Sigma_{k|p-1}\ \phi(k) = p-1$

The order k of every element in Z_p^* divides p-1

$\Rightarrow \Sigma_{k|p-1}$ (# of elements in Z_p^* with order k) = p-1

(Lemma 1) $\Rightarrow p-1 \le \Sigma_{k|p-1}\ \phi(k)$, combined with lemma 2,

we know that # of ord-k elements in $Z_p^* = \phi(k)$

$\Rightarrow$ # of ord-(p-1) elements in $Z_p^* = \phi(p-1) > 1$

$\Rightarrow$ There is at least one generator in Z_p^*, i.e. Z_p^* is cyclic

Ex. p=13, p-1 = |{2,6,11,7}| + |{4,10}| + |{8,5}| + |{3,9}| + |{12}| + |{1}|
k=12 k=6 k=4 k=3 k=2 k=1

Generators in QR_n

- Number of generators in Z_p^*: $\phi(p-1)$

  Let g be a primitive, $Z_p^* = \langle g \rangle = \{g, g^2, g^3, \ldots, g^k, \ldots, g^{p-1}\}$

  if $\gcd(k, p-1) = d \neq 1$ then g^k is not a primitive

  since $(g^k)^{(p-1)/d} = (g^{k/d})^{p-1} = 1$, i.e. $ord_p(g^k) \leq (p-1)/d$

  if $\gcd(k, p-1) = 1$ and g^k is not a primitive, then $d = ord_p(g^k) < p-1$, i.e.

  $(g^k)^d = 1$; g is a primitive $\Rightarrow p-1 \mid k\,d \Rightarrow p-1 \mid d$ contradiction.

- Z_n^* is not a cyclic group ($n = p\,q$, $p=2p'+1$, $q=2q'+1$, $\lambda(n)=2p'q'$)

  Since $x^{\lambda(n)} \equiv 1 \pmod n$, there is no generator that can generate all members in Z_n^*

- QR_n is a cyclic group of order $\lambda(n)/2 = \text{lcm}(p-1, q-1)/2 = p'\,q'$

  $\forall\, x \in Z_n^*$, $x^{\lambda(n)} \equiv 1 \pmod n$ Carmichael's Theorem

  clearly, $(x^2)^{\lambda(n)/2} \equiv 1 \pmod n$, $QR_n = \{x^2 \mid \forall\, x \in Z_n^*\}$

  i.e. $\forall\, y \in QR_n$, $ord_n(y) \mid p'\,q'$ $(ord_n(y) \in \{1, p', q', p'q'\})$

Generators in QR_n (cont'd)

cyclic? $\exists\, x^* \in Z_n^*\ ord_n(x^*) = \lambda(n) = 2\,p'\,q' \Rightarrow$

$\exists\, y^*\ (=(x^*)^2) \in QR_n$ s.t. $ord_n(y^*) = \lambda(n)/2 = p'\,q'$

- Let y be a random element in QR_n, the probability that y is a generator is close to 1

Let y^* be a generator of QR_n,

$$QR_n = \langle y^* \rangle = \{y^*, (y^*)^2, (y^*)^3, \ldots, (y^*)^k, \ldots, (y^*)^{p'q'}\}$$

if $\gcd(k, p'q') = d \neq 1$ then $(y^*)^k$ is not a generator

since $((y^*)^k)^{p'q'/d} = ((y^*)^{k/d})^{p'q'} = 1$, i.e. $ord_p((y^*)^k) \leq (p'q')/d$

$\phi(p'q') = \phi(p')\,\phi(q') = (p'-1)(q'-1) = p'q' - p' - q' + 1$

$= p'q' - (p'-1) - (q'-1) - 1$

$\forall\, x \in \{(y^*)^{q'}, (y^*)^{2q'}, \ldots, (y^*)^{(p'-1)q'}\}\ ord_n(x) = p'$

$\forall\, x \in \{(y^*)^{p'}, (y^*)^{2p'}, \ldots, (y^*)^{(q'-1)p'}\}\ ord_n(x) = q'$

$ord_n(1) = 1$

$Pr\{x \text{ is a generator} \mid x \in_R QR_n\} = \phi(p'q') / (p'q')$ is close to 1

Subgroups in Z_n^*

Consider $n = p\,q$, $p=2p'+1$, $q=2q'+1$, $m=p'q'$, $\lambda(n) = \text{lcm}(p-1, q-1)=2m$,

$\phi(n) = (p-1)(q-1) = 4m$

- **Z_n^*** is not a cyclic group
  - Carmichael's theorem asserts that no element in Z_n^* can generate all elements in Z_n^*. (maximum order is 2m instead of 4m)
  - However, Z_n^* is still a group over modulo n multiplication.
- **QR_n** is a cyclic subgroup of order $m = \lambda(n)/2$, $QR_n = \{x^2 \mid \forall\ x \in Z_n^*\}$
  - $J_{00} = \{x \in Z_n^* \mid J(x,p)=1 \text{ and } J(x,q)=1\}$
  - If there exists an element in Z_n^* whose order is 2m, then QR_n is clearly a cyclic group. (Will the precondition be true?)
  - $\forall\ x \in Z_n^*\ x^{2m} \equiv 1 \pmod n$ implies that $\forall\ y \in QR_n\ \text{ord}_n(y) \mid p'q'$ i.e. $\text{ord}_n(y)$ is either 1, p', q', or p'q' (if there is one y s.t. $\text{ord}_n(y)=m$ then y is a generator and QR_n is cyclic). Let's construct one.

Subgroups in Z_n^* (cont'd)

Let g_1 be a generator in Z_p^*, and g_2 be a generator in Z_q^*

Let **$g \equiv g_1 \pmod p \equiv g_2 \pmod q$**, (note that $J(g, n) = 1$, $g \in J_{11}$)

$g^{p-1} \equiv g^{2p'} \equiv {g_1}^{2p'} \equiv 1 \pmod p$, $g^{q-1} \equiv g^{2q'} \equiv {g_2}^{2q'} \equiv 1 \pmod q$

$\Rightarrow$ $g^{2p'q'} \equiv 1 \pmod p$ and $g^{2q'p'} \equiv 1 \pmod q$ i.e. $g^{2p'q'} \equiv 1 \pmod n$

if there exists a $k \in \{1, 2, p', q', 2p', 2q', p'q'\}$ s.t. $g^k \equiv 1 \pmod n$

then $\text{ord}_n(g)$ is not $2p'q'$

1. $k=1$: $\Rightarrow g_1 \equiv 1 \pmod p$ contradict with $\text{ord}_p(g_1) = p-1$
2. $k=p'$: $\Rightarrow g^{p'} \equiv {g_1}^{p'} \equiv 1 \pmod p$ contradict with $\text{ord}_p(g_1) = 2p'$
3. $k=q'$: $\Rightarrow g^{q'} \equiv {g_2}^{q'} \equiv 1 \pmod q$ contradict with $\text{ord}_q(g_2) = 2q'$
4. $k=2$: $\Rightarrow {g_1}^2 \equiv 1 \pmod p$ contradict with $\text{ord}_p(g_1) = p-1$
5. $k=2p'$: $\Rightarrow g^{2p'} \equiv {g_2}^{2p'} \equiv 1 \pmod q$ contradict with $\text{ord}_q(g_2) = 2q'$
6. $k=2q'$: $\Rightarrow g^{2q'} \equiv {g_1}^{2q'} \equiv 1 \pmod p$ contradict with $\text{ord}_p(g_1) = 2p'$

Subgroups in Z_n^* (cont'd)

7. $k=p'q'$: $\Rightarrow g^{p'q'} \equiv g_1^{p'q'} \equiv 1 \pmod p$

since $g_1^{2p'} \equiv 1 \pmod p$ and

$\gcd(q', 2) = 1 \Rightarrow \exists\ a, b$ s.t. $a\,q' + b\,2 = 1$

$\Rightarrow g_1^{p'} \equiv g_1^{p'(a\,q' + b\,2)} \equiv (g_1^{p'\,q'})^a (g_1^{2\,p'})^b \equiv 1 \pmod p$

contradict with $\mathrm{ord}_p(g_1) = 2p'$

1~7 implies that $\mathrm{ord}_n(g) = 2p'q'$, i.e. $QR_o = \{g^2, g^4, \ldots, g^{p'q'}\}$ and QR_n is a cyclic group.

- ★ Pr{Elements in QR_n being a generator} = $\phi(p'q') / (p'q')$

✧ **J_n** is a cyclic subgroup of order $2m = \lambda(n)$, $J_n = \{x \in Z_n^* \mid J(x,n)=1\}$

- ★ $J_{11} = \{x \in Z_n^* \mid J(x,p)=-1 \text{ and } J(x,q)=-1\}$
- ★ The above proof also shows that $J_n = \{g, g^2, \ldots, g^{2p'q'}\}$ is cyclic
- ★ Pr{Elements in J_n being a generator} = $\phi(p'q') / (2p'q')$

✧ **$J_{01} \cup J_{10}$** $= Z_n^* \setminus \{J_{00} \cup J_{11}\}$ is not a subgroup in Z_n^*

- ★ if $x \in J_{01}$ then $x * x \in J_{00}$

Generator in QR_n

- $n = p\,q$, $p=2p'+1$, $q=2q'+1$
- Find a generator in QR_n

1. Find a generator g_1 of Z_p^* (i.e. $Z_p^* = \langle g_1 \rangle$) and g_2 of Z_q^* (i.e. $Z_q^* = \langle g_2 \rangle$)
2. Calculate the generator $h_1 \equiv g_1^2 \pmod p$ of QR_p and $h_2 \equiv g_2^2 \pmod 1$ of QR_q
3. Let $h \equiv h_1 \pmod p \equiv h_2 \pmod q$.

It is clear that $h \equiv g^2 \pmod n$, i.e. $h \in QR_n$, where $g \equiv g_1 \pmod p \equiv g_2 \pmod q$.

Claim: h is a generator of QR_n

pf.

$y \in QR_n \Rightarrow y \in QR_p$ and $y \in QR_q$

i.e. $\exists\, x_1 \in Z_{p'}$ and $x_2 \in Z_{q'}$, $y \equiv h_1^{x_1} \pmod p \equiv h_2^{x_2} \pmod q$

$\Rightarrow y \equiv g_1^{2x_1} \pmod p \equiv g_2^{2x_2} \pmod q$

$\Rightarrow y \equiv g^{2x} \pmod n$ if $2x \equiv 2x_1 \pmod{p-1} \equiv 2x_2 \pmod{q-1}$

a unique $x \in Z_{p'q'}$ exists by CRT since $\gcd(p-1, q-1) = \gcd(2p', 2q') = 2$

$\Rightarrow y \equiv h^x \pmod n$

Generate Elements in Z_n^*

- Z_n^* is NOT a cyclic group ($n = p\,q$, $p=2p'+1$, $q=2q'+1$, $m=p'\,q'$)
- How do we generate random elements in Z_n^*?

  $Z_n^* = \{ g^a u^{-e\,b_1} (-1)^{b_2} \mid g$ is a generator in QR_n, $\gcd(e, \phi(n)) = 1$,
  $u \in_R Z_n^*$ and $J(u,n) = -1$,
  $a \in \{0,\ldots,m-1\}$, $b_1 \in \{0,1\}$, and $b_2 \in \{0,1\}$ $\}$

  Note: 1. $J(-1, n) = 1$ and $-1 \in J_n \backslash QR_n$ since $(-1)^{(p-1)/2} \equiv (-1)^{p'} \equiv -1 \pmod p$
  2. e is odd, $\phi(n)-e$ is also odd, $J(u^{-e}, n) = J(u, n) = -1$

- We can view the above as 4 parts

  1. J_{00} (QR_n): $b_1 = b_2 = 0$, $J_{00} = \{g^a \mid a \in \{0,\ldots,m-1\}\}$
  2. J_{11} ($J_n \backslash QR_n$): $b_1 = 0$, $b_2 = 1$, $J_{11} = \{-g^a \mid a \in \{0,\ldots,m-1\}\}$

  Assume that $J(u, p) = -1$ and $J(u, q) = 1$

  3. J_{01}: $b_1 = 1$, $b_2 = 0$, $J_{01} = \{g^a u^{-e} \mid a \in \{0,\ldots,m-1\}\}$
  4. J_{10}: $b_1 = 1$, $b_2 = 1$, $J_{01} = \{-g^a u^{-e} \mid a \in \{0,\ldots,m-1\}\}$

Lagrange's Theorem

- Theorem: for any finite group G, the order (number of elements) of every subgroup H of G divides the order of G.
  - proof sketch: divide G into left cosets H – equivalence classes, and show that they have the same size.

Lagrange's Theorem

- Theorem: for any finite group G, the order (number of elements) of every subgroup H of G divides the order of G.
  - proof sketch: divide G into left cosets H – equivalence classes, and show that they have the same size.
- It implies that: the order of any element a of a finite group (i.e. the smallest positive integer number k with $a^k = 1$) divides the order of the group. Since the order of a is equal to the order of the cyclic subgroup generated by a. Also, $a^{|G|} = 1$ since order of a divides $|G|$.

Lagrange's Theorem

- Theorem: for any finite group G, the order (number of elements) of every subgroup H of G divides the order of G.
  - proof sketch: divide G into left cosets H – equivalence classes, and show that they have the same size.
- It implies that: the order of any element a of a finite group (i.e. the smallest positive integer number k with $a^k = 1$) divides the order of the group. Since the order of a is equal to the order of the cyclic subgroup generated by a. Also, $a^{|G|} = 1$ since order of a divides $|G|$.
- Any prime order group is cyclic.