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

- $\phi(n)$: the number of integers $1 \leq a < n$ 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 $\{1,3,7,9\}$

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

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

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 $\{1,3,7,9\}$
- properties of $\phi(\bullet)$
  - $\phi(p) = p-1$, if p is prime
  - $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$, if p is prime
  - $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $\gcd(n,m)=1$ multiplicative property
  - $\phi(n \cdot m) = \phi((d_1/d_2/d_3)^2) \cdot \phi(d_2^3) \cdot \phi(d_3^3) \cdot \phi(n/d_1/d_2) \cdot \phi(m/d_1/d_3)$

    if $\gcd(n,m)=d_1$, $\gcd(n/d_1,d_1)=d_2$, $\gcd(m/d_1,d_1)=d_3$
  - $\phi(n) = n \prod_{\forall p|n} (1-1/p)$
- ex. $\phi(10)=(2-1)\cdot(5-1)=4$ $\phi(120)=120(1-1/2)(1-1/3)(1-1/5)=32$

$\forall$ prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

- $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$

$\forall$prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

- $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$

$\forall$prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

✧ $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $gcd(x, p^r)=1$

$\forall$prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

- $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$

$\forall$prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

✧ $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$

$\forall$ prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

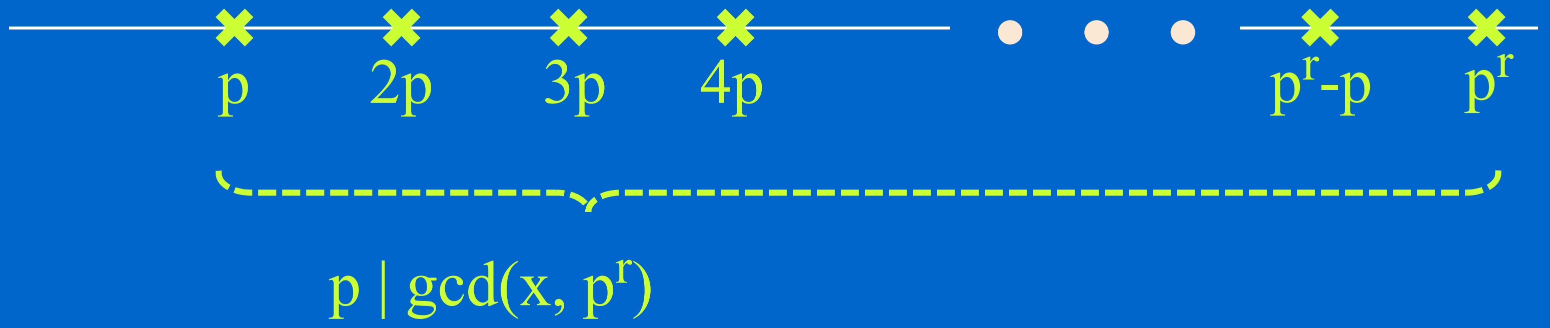
- $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$

$\forall$prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

- $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$

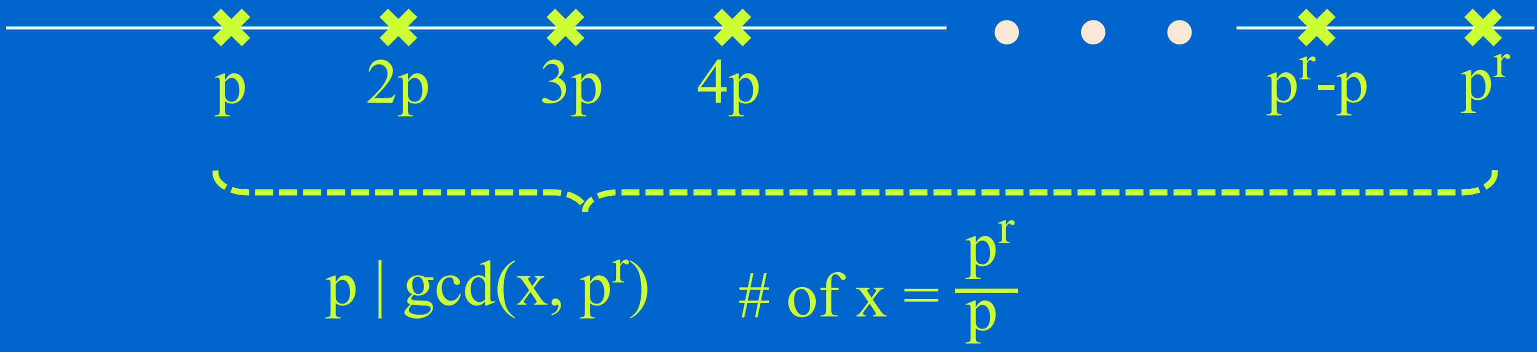
$\forall$prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

- $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$



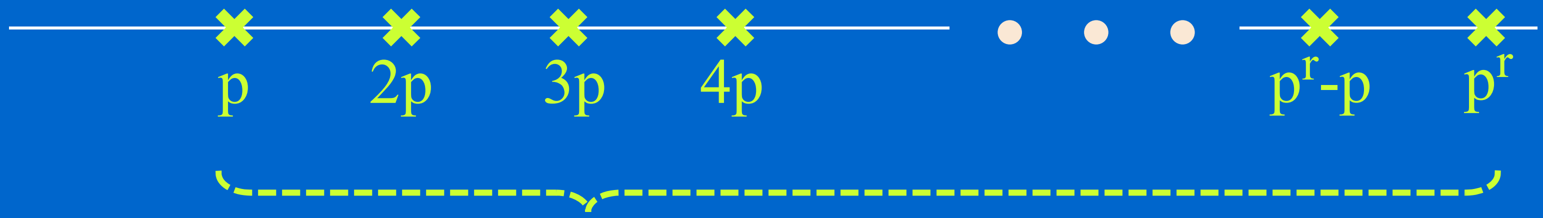
$\forall$ prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

✧ $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$



$\forall$ prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

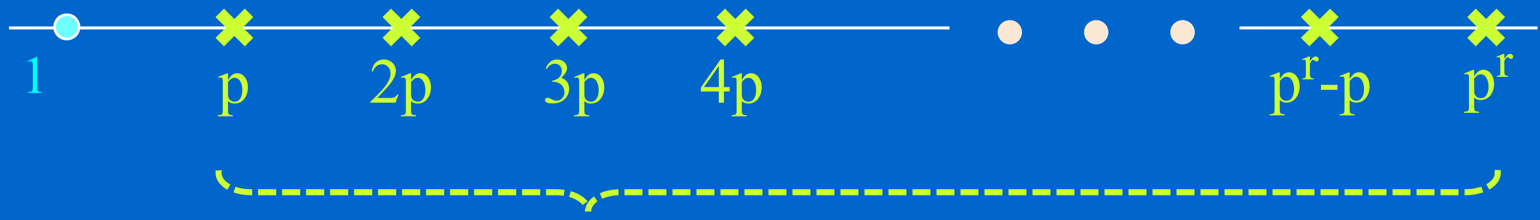
- $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$



$p \mid \gcd(x, p^r)$ $\quad$ $\# \text{ of } x = \frac{p^r}{p} = p^{r-1}$

$\forall$prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

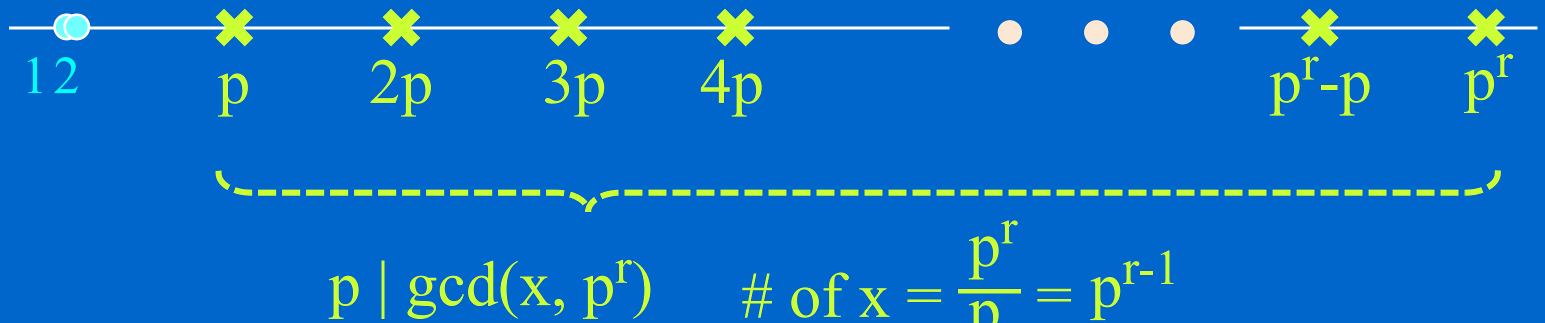
- $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$



$p \mid \gcd(x, p^r)$ # of x = $\frac{p^r}{p} = p^{r-1}$

$\forall$ prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

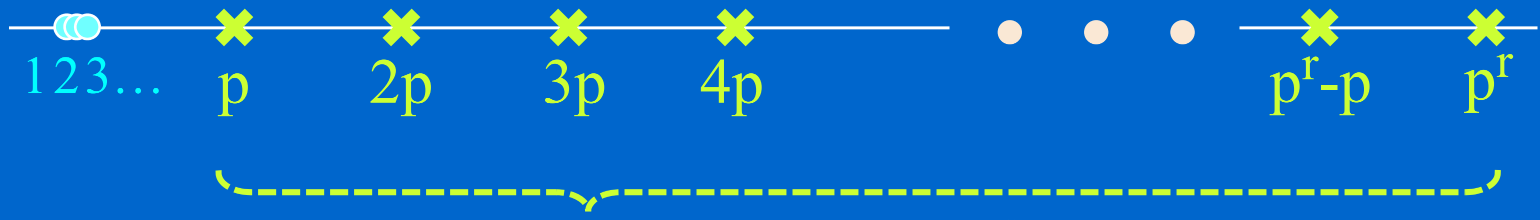
✧ $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$



# of x = $\frac{p^r}{p} = p^{r-1}$

$\forall$ prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

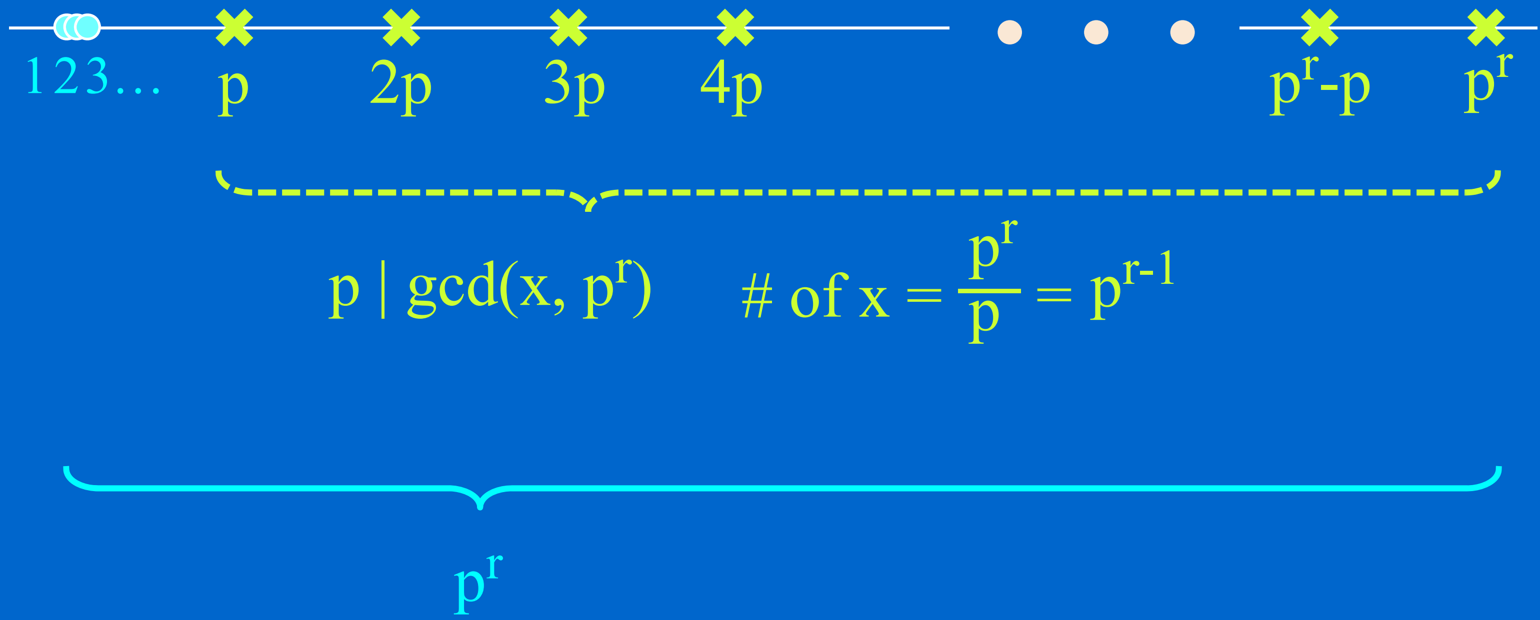
- $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$



$p \mid \gcd(x, p^r)$ $\quad$ $\#\text{ of } x = \dfrac{p^r}{p} = p^{r-1}$

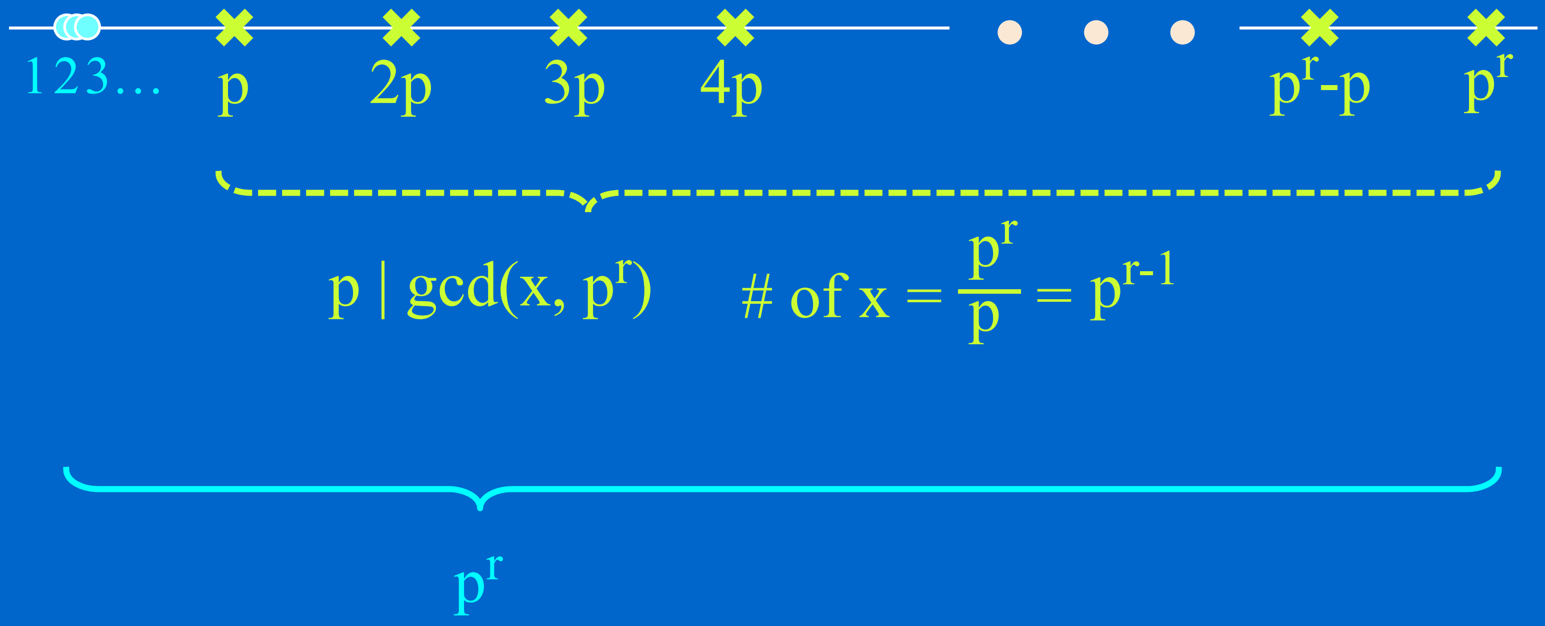
$\forall$prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

✧ $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$



$\forall$prime p, $\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$

- $\phi(p^r)$: the number of integers $1 \le x < p^r$ s.t. $\gcd(x, p^r)=1$



$$\phi(p^r) = p^r - p^{r-1} = p^r \cdot (1-1/p)$$

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $\gcd(n,m)=1$

$\gcd(n, m) = 1$

$$Z_{nm}^{*} = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a \in Z_n^{*}, b \in Z_m^{*}\}$$

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $\gcd(n,m)=1$

$\gcd(n, m) = 1$

$$Z_{nm}^{*} = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a \in Z_n^{*}, b \in Z_m^{*}\}$$

$\gcd(a,n) = 1$, $\gcd(b,m) = 1$, $\gcd(x, n\, m) = 1$

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $\gcd(n,m)=1$

$\gcd(n, m) = 1$

$Z_{nm}^{*} = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a \in Z_n^{*}, b \in Z_m^{*}\}$

$\gcd(a,n) = 1$, $\gcd(b,m) = 1$, $\gcd(x, n\,m) = 1$

$n\, n^{-1} \equiv 1 \pmod{m}$

$\phi(n\cdot m) = \phi(n)\cdot\phi(m)$ if $\gcd(n,m)=1$

$\gcd(n, m) = 1$

$$Z_{nm}^* = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a\in Z_n^*, b\in Z_m^*\}$$

$\gcd(a,n) = 1$, $\gcd(b,m) = 1$, $\gcd(x, n\, m) = 1$

$n\, n^{-1} \equiv 1 \pmod{m}$, $m\, m^{-1} \equiv 1 \pmod{n}$

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $gcd(n,m)=1$

$gcd(n, m) = 1$

$Z_{nm}^{*} = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a \in Z_n^{*}, b \in Z_m^{*}\}$

$\phi(n)$ a

$gcd(a,n) = 1,\ gcd(b,m) = 1,\ gcd(x, n\, m) = 1$

$n\, n^{-1} \equiv 1 \pmod{m},\quad m\, m^{-1} \equiv 1 \pmod{n}$

$x_n \equiv m\, a \pmod{n}$

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $\gcd(n,m)=1$

$\gcd(n, m) = 1$

$$Z_{nm}^* = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a \in Z_n^*, b \in Z_m^*\}$$

$\phi(n)$ a

$\gcd(a,n) = 1$, $\gcd(b,m) = 1$, $\gcd(x, n\, m) = 1$

$n\, n^{-1} \equiv 1 \pmod{m}$, $m\, m^{-1} \equiv 1 \pmod{n}$

injective mappings $\Leftarrow \gcd(n,m)=1$

$x_n \equiv m\, a \pmod{n}$

$\phi(n\cdot m) = \phi(n)\cdot\phi(m)$ if $gcd(n,m)=1$

$gcd(n, m) = 1$

$Z_{nm}^{*} = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a\in Z_n^{*}, b\in Z_m^{*}\}$

$\phi(n)$ a

$gcd(a,n) = 1,\ gcd(b,m) = 1,\ gcd(x, n\, m) = 1$

$n\, n^{-1} \equiv 1 \pmod{m},\quad m\, m^{-1} \equiv 1 \pmod{n}$

injective mappings $\Leftarrow gcd(n,m)=1$

$x_n \equiv m\, a \pmod{n}$ there are $\phi(n)\ x_n$

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $gcd(n,m)=1$

$gcd(n, m) = 1$

$Z_{nm}^* = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a \in Z_n^*, b \in Z_m^*\}$

$\phi(n)$ a $\phi(m)$ b

$gcd(a,n) = 1,\ gcd(b,m) = 1,\ gcd(x, n\, m) = 1$

$n\, n^{-1} \equiv 1 \pmod{m}, \quad m\, m^{-1} \equiv 1 \pmod{n}$

injective mappings $\Leftarrow gcd(n,m)=1$

$x_n \equiv m\, a \pmod{n}$ there are $\phi(n)$ x_n

$x_m \equiv n\, b \pmod{m}$

$\phi(n\cdot m) = \phi(n)\cdot\phi(m)$ if $\gcd(n,m)=1$

$\gcd(n, m) = 1$

$Z_{nm}^* = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a \in Z_n^*, b \in Z_m^*\}$

$\phi(n)$ a

$\phi(m)$ b

$\gcd(a,n) = 1$, $\gcd(b,m) = 1$, $\gcd(x, n\, m) = 1$

$n\, n^{-1} \equiv 1 \pmod{m}$, $m\, m^{-1} \equiv 1 \pmod{n}$

injective mappings $\Leftarrow \gcd(n,m)=1$

$x_n \equiv m\, a \pmod{n}$ there are $\phi(n)$ x_n

$x_m \equiv n\, b \pmod{m}$

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $\gcd(n,m)=1$

$\gcd(n, m) = 1$

$Z_{nm}^* = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a \in Z_n^*, b \in Z_m^*\}$

$\phi(n)$ a $\phi(m)$ b

$\gcd(a,n) = 1$, $\gcd(b,m) = 1$, $\gcd(x, n\, m) = 1$

$n\, n^{-1} \equiv 1 \pmod{m}$, $m\, m^{-1} \equiv 1 \pmod{n}$

injective mappings $\Leftarrow \gcd(n,m)=1$

$x_n \equiv m\, a \pmod{n}$ there are $\phi(n)$ x_n

$x_m \equiv n\, b \pmod{m}$ there are $\phi(m)$ x_m

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $\gcd(n,m)=1$

$\gcd(n, m) = 1$

$Z_{nm}^{*} = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a \in Z_n^{*}, b \in Z_m^{*}\}$

$\phi(n)$ a $\phi(m)$ b

$\gcd(a,n) = 1$, $\gcd(b,m) = 1$, $\gcd(x, n\,m) = 1$

$n\, n^{-1} \equiv 1 \pmod{m}$, $m\, m^{-1} \equiv 1 \pmod{n}$

injective mappings $\Leftarrow \gcd(n,m)=1$

$x_n \equiv m\, a \pmod{n}$ there are $\phi(n)$ x_n

$x_m \equiv n\, b \pmod{m}$ there are $\phi(m)$ x_m

$x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \equiv n\, n^{-1}\, x_m + m\, m^{-1}\, x_n \pmod{n\, m}$

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $gcd(n,m)=1$

$gcd(n, m) = 1$

$$Z_{nm}^{*} = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a \in Z_n^{*}, b \in Z_m^{*}\}$$

$\phi(n)$ a $\phi(m)$ b

$gcd(a,n) = 1,\ gcd(b,m) = 1,\ gcd(x, n\, m) = 1$

$n\, n^{-1} \equiv 1 \pmod{m}, \quad m\, m^{-1} \equiv 1 \pmod{n}$

injective mappings $\Leftarrow gcd(n,m)=1$

$x_n \equiv m\, a \pmod{n}$ there are $\phi(n)$ x_n

$x_m \equiv n\, b \pmod{m}$ there are $\phi(m)$ x_m

$$x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \equiv n\, n^{-1}\, x_m + m\, m^{-1}\, x_n \pmod{n\, m}$$

$$x \equiv x_n \pmod{n} \equiv x_m \pmod{m}$$

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ if $\gcd(n,m)=1$

$\gcd(n, m) = 1$

$Z_{nm}^* = \{x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \pmod{nm},\ a \in Z_n^*, b \in Z_m^*\}$

$\phi(n)$ a $\phi(m)$ b

$\gcd(a,n) = 1$, $\gcd(b,m) = 1$, $\gcd(x, n\, m) = 1$

$n\, n^{-1} \equiv 1 \pmod{m}$, $m\, m^{-1} \equiv 1 \pmod{n}$

injective mappings $\Leftarrow \gcd(n,m)=1$

$x_n \equiv m\, a \pmod{n}$ there are $\phi(n)$ x_n

$x_m \equiv n\, b \pmod{m}$ there are $\phi(m)$ x_m

$x \equiv n\, n^{-1}\, m\, a + m\, m^{-1}\, n\, b \equiv n\, n^{-1}\, x_m + m\, m^{-1}\, x_n \pmod{n\, m}$

$x \equiv x_n \pmod{n} \equiv x_m \pmod{m}$

Through CRT, each one of $\phi(n)\phi(m)$ pairs, i.e. (x_n, x_m), uniquely maps to an x in Z_{nm} which is relatively prime to n m

$\phi(n) = n \prod_{\forall p|n} (1-1/p)$

from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$

$\phi(n) = n \prod_{\forall p|n} (1-1/p)$

from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$

from **Euler totion function's multiplicative property**:

$$\phi(n\,m) = \phi(n) \cdot \phi(m)$$

$\phi(n) = n \prod_{\forall p|n} (1-1/p)$

from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$

from **Euler totion function's multiplicative property**:

$$\phi(n\,m) = \phi(n) \cdot \phi(m)$$

$$\phi(n) = \phi(p_1^{c1} p_2^{c2} \cdots p_k^{ck}) = \phi(p_1^{c1}) \cdot \phi(p_2^{c2} \cdots p_k^{ck})$$

$\phi(n) = n \prod_{\forall p|n} (1-1/p)$

from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$

from **Euler totion function's multiplicative property**:

$$\phi(n\, m) = \phi(n) \cdot \phi(m)$$

$$\phi(n) = \phi(p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}) = \phi(p_1^{c_1}) \cdot \phi(p_2^{c_2} \cdots p_k^{c_k})$$

$$= (p_1^{c_1} - p_1^{c_1-1}) \cdot \phi(p_2^{c_2} \cdots p_k^{c_k})$$

$\phi(n) = n \prod_{\forall p|n} (1-1/p)$

from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$

from **Euler totion function's multiplicative property**:

$$\phi(n\, m) = \phi(n) \cdot \phi(m)$$

$$\phi(n) = \phi(p_1^{c1} p_2^{c2} \cdots p_k^{ck}) = \phi(p_1^{c1}) \cdot \phi(p_2^{c2} \cdots p_k^{ck})$$

$$= (p_1^{c1} - p_1^{c1-1}) \cdot \phi(p_2^{c2} \cdots p_k^{ck})$$

$$= p_1^{c1}(1-1/p_1) \cdot \phi(p_2^{c2} \cdots p_k^{ck})$$

$\phi(n) = n \prod_{\forall p|n} (1-1/p)$

from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$

from **Euler totion function's multiplicative property**:

$$\phi(n\,m) = \phi(n) \cdot \phi(m)$$

$$\begin{aligned}
\phi(n) = \phi(p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}) &= \phi(p_1^{c_1}) \cdot \phi(p_2^{c_2} \cdots p_k^{c_k}) \\
&= (p_1^{c_1} - p_1^{c_1-1}) \cdot \phi(p_2^{c_2} \cdots p_k^{c_k}) \\
&= p_1^{c_1}(1-1/p_1) \cdot \phi(p_2^{c_2} \cdots p_k^{c_k}) \\
&= p_1^{c_1}(1-1/p_1) \cdot p_2^{c_2}(1-1/p_2) \cdot \phi(p_3^{c_3} \cdots p_k^{c_k})
\end{aligned}$$

$\phi(n) = n \prod_{\forall p|n} (1-1/p)$

from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$

from **Euler totion function's multiplicative property**:

$$\phi(n\,m) = \phi(n) \cdot \phi(m)$$

$$\phi(n) = \phi(p_1^{c1} p_2^{c2} \cdots p_k^{ck}) = \phi(p_1^{c1}) \cdot \phi(p_2^{c2} \cdots p_k^{ck})$$

$$= (p_1^{c1} - p_1^{c1-1}) \cdot \phi(p_2^{c2} \cdots p_k^{ck})$$

$$= p_1^{c1}(1-1/p_1) \cdot \phi(p_2^{c2} \cdots p_k^{ck})$$

$$= p_1^{c1}(1-1/p_1) \cdot p_2^{c2}(1-1/p_2) \cdot \phi(p_3^{c3} \cdots p_k^{ck})$$

$$= \ldots$$

$\phi(n) = n \prod_{\forall p|n} (1-1/p)$

from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$

from **Euler totion function's multiplicative property**:

$$\phi(n\,m) = \phi(n) \cdot \phi(m)$$

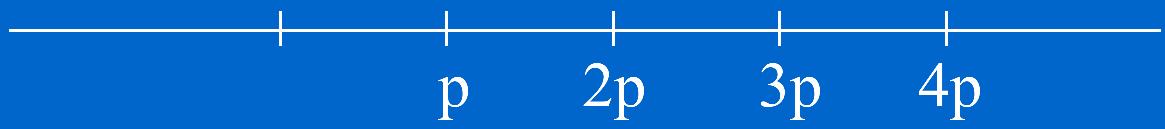
$$\begin{aligned}
\phi(n) = \phi(p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}) &= \phi(p_1^{c_1}) \cdot \phi(p_2^{c_2} \cdots p_k^{c_k}) \\
&= (p_1^{c_1} - p_1^{c_1-1}) \cdot \phi(p_2^{c_2} \cdots p_k^{c_k}) \\
&= p_1^{c_1}(1-1/p_1) \cdot \phi(p_2^{c_2} \cdots p_k^{c_k}) \\
&= p_1^{c_1}(1-1/p_1) \cdot p_2^{c_2}(1-1/p_2) \cdot \phi(p_3^{c_3} \cdots p_k^{c_k}) \\
&= \ldots \\
&= n \prod_{\forall p|n} (1-1/p)
\end{aligned}$$

How large is $\phi(n)$?

✧ $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large

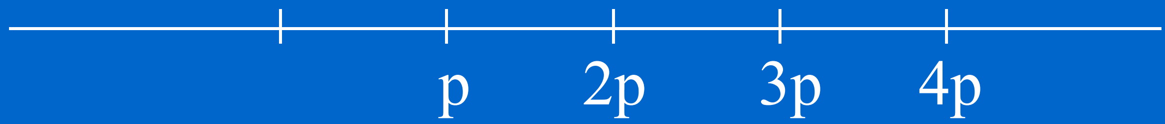
How large is $\phi(n)$?

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



How large is $\phi(n)$?

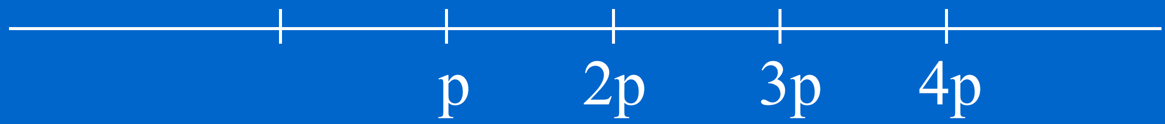
- $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large
- Probability that a prime number p is a factor of a random number r is $1/p$



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

How large is $\phi(n)$?

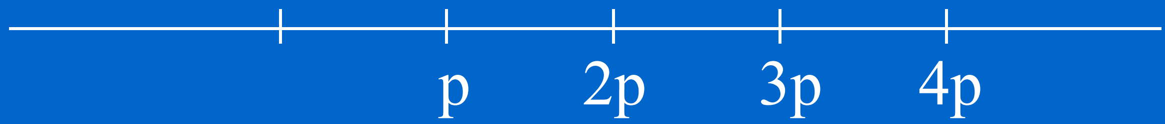
- $\phi(n) \approx n \cdot 6/\pi^2$ as n goes large
- Probability that a prime number p is a factor of a random number r is $1/p$



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



- Probability that two independent random numbers r_1 and r_2 both have a given prime number p as a factor is $1/p^2$
- 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 is $P = (1-1/2^2)(1-1/3^2)(1-1/5^2)(1-1/7^2)\ldots$

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 and r_2 relatively prime }

- Equalities:

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

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

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

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

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

$$= 6/\pi^2$$

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, $\zeta(4) = \pi^4/90 \approx 0.92$

of ord-k elements in Z_p^*

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

of ord-*k* elements in Z_p^*

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

Special case: $\phi(p-1)$ x's in Z_p^* with $\text{ord}_p(x)=p-1$,
i.e. $\phi(p-1)$ generators in Z_p^*

of ord-k elements in Z_p^*

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

pf. ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $\langle \boldsymbol{a} \rangle = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k = 1\}$ is a subgroup G, $|G| = k$ spanned by $\boldsymbol{a}$.

\# of ord-k elements in Z_p^*

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

pf. ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.

e.g. $p = 13$

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

of ord-*k* elements in Z_p^*

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

pf. ✧ If $\boldsymbol{a}$ is an ord-*k* element in Z_p^*, then <$\boldsymbol{a}$> = $\{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, |G|=*k* spanned by $\boldsymbol{a}$.

e.g. $p = 13$

{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1}

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

of ord-*k* elements in Z_p^*

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

pf. ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then <$\boldsymbol{a}$> = $\{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k{=}1\}$ is a subgroup G, |G|=k spanned by $\boldsymbol{a}$.

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}

of ord-k elements in Z_p^*

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

pf. ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.

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} ← $(2^{(p-1)/k})^j \equiv (2^2)^j$

of ord-k elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then <$\boldsymbol{a}$> = $\{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most $\boldsymbol{k/d}$

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}

of ord-*k* elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-*k* element in Z_p^*, then <$\boldsymbol{a}$> = $\{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***

$$(a^\ell)^{k/d} \equiv (a^{\ell/d})^k \equiv 1$$

e.g. $p = 13$

$\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

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

$k=12$, $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

$k=6$, $\{4, 3, 12, 9, 10, 1\}$

of ord-k elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, |G|=k spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***

$$(a^\ell)^{k/d} \equiv (a^{\ell/d})^k \equiv 1$$

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}

of ord-*k* elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, |G|=k spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***

$$(a^\ell)^{k/d} \equiv (a^{\ell/d})^k \equiv 1$$

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}

of ord-k elements in Z_p^*

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

pf.

- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k\text{-}1}, \boldsymbol{a}^k\text{=}1\}$ is a subgroup G, |G|=k spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with gcd(ℓ, k) = d > 1 have order at most ***k/d***

$$(a^\ell)^{k/d} \equiv (a^{\ell/d})^k \equiv 1$$

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}

of ord-*k* elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-*k* element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k{=}1\}$ is a subgroup G, |G|=*k* spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***

$$(a^\ell)^{k/d} \equiv (a^{\ell/d})^k \equiv 1$$

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}

of ord-k elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k*/*d***

$$(a^\ell)^{k/d} \equiv (a^{\ell/d})^k \equiv 1$$

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}

of ord-k elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then <$\boldsymbol{a}$> = $\{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, |G|=k spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***

$$(a^\ell)^{k/d} \equiv (a^{\ell/d})^k \equiv 1$$

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}

of ord-k elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $\langle \boldsymbol{a} \rangle = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k = 1\}$ is a subgroup G, $|G| = k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***

$$(a^\ell)^{k/d} \equiv (a^{\ell/d})^k \equiv 1$$

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}

of ord-k elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $\langle \boldsymbol{a} \rangle = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k{=}1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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~~}

k=6, {4, 3, 12, 9, 10, 1}

of ord-*k* elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-*k* element in Z_p^*, then <$\boldsymbol{a}$> = {$\boldsymbol{a}^1$, $\boldsymbol{a}^2$, …, $\boldsymbol{a}^{k\text{-}1}$, $\boldsymbol{a}^k$=1} is a subgroup G, |G|=*k* spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with gcd(ℓ, k) = d > 1 have order at most ***k*/*d***
- ✧ Only the order of those a^ℓ with gcd(ℓ, k) = 1 might be 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}

of ord-k elements in Z_p^*

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

pf.

- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, |G|=k spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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}

of ord-k elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k = 1\}$ is a subgroup G, $|G| = k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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}

of ord-k elements in Z_p^*

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

pf.

- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most $\boldsymbol{k/d}$
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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}

of ord-k elements in Z_p^*

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

pf.

- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, |G|=k spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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~~}, $\phi(6)$

of ord-k elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, |G|=k spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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=4, {8, 12, 5, 1}, $\phi(4)$

of ord-*k* elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k = 1\}$ is a subgroup G, |G|=k spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most $\boldsymbol{k/d}$
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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=4, {8, ~~12~~, 5, 1}, $\phi(4)$

of ord-k elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then <$\boldsymbol{a}$> = $\{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, |G|=k spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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=4, {8, ~~12~~, 5, ~~1~~}, $\phi(4)$

of ord-k elements in Z_p^*

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

pf.

- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k\text{-}1}, \boldsymbol{a}^k=1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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=4, {8, ~~12~~, 5, ~~1~~}, $\phi(4)$

k=3, {3, 9, 1}, $\phi(3)$

of ord-k elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most $\boldsymbol{k/d}$
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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=4, {8, ~~12~~, 5, ~~1~~}, $\phi(4)$

k=3, {3, 9, ~~1~~}, $\phi(3)$

of ord-k elements in Z_p^*

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

pf.

- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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=4, {8, ~~12~~, 5, ~~1~~}, $\phi(4)$

k=3, {3, 9, ~~1~~}, $\phi(3)$

k=2, {12,1}, $\phi(2)$

of ord-k elements in Z_p^*

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

pf.
- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most ***k/d***
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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=4, {8, ~~12~~, 5, ~~1~~}, $\phi(4)$

k=3, {3, 9, ~~1~~}, $\phi(3)$

k=2, {12, ~~1~~}, $\phi(2)$

of ord-k elements in Z_p^*

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

pf.

- ✧ If $\boldsymbol{a}$ is an ord-k element in Z_p^*, then $<\boldsymbol{a}> = \{\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^{k-1}, \boldsymbol{a}^k=1\}$ is a subgroup G, $|G|=k$ spanned by $\boldsymbol{a}$.
- ✧ Those a^ℓ with $\gcd(\ell, k) = d > 1$ have order at most $\boldsymbol{k/d}$
- ✧ Only the order of those a^ℓ with $\gcd(\ell, k) = 1$ might be 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=4, {8, ~~12~~, 5, ~~1~~}, $\phi(4)$

k=3, {3, 9, ~~1~~}, $\phi(3)$

k=2, {12, ~~1~~}, $\phi(2)$

k=1, {1}, $\phi(1)$

$\sum_{k|p-1} \phi(k) = p-1$

Lemma. $\sum_{k|p-1} \phi(k) = p-1$

let $\phi(1)=1$

$\Sigma_{k|p-1}\ \phi(k) = p-1$

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. $\gcd(a, p-1) = k$)

$\Sigma_{k|p-1}\, \phi(k) = p\text{-}1$

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 $p=13$, $a \in Z_p^*$

$\gcd(a, p-1)=k$, i.e. $k \mid p-1$

$\Sigma_{k|p-1}\ \phi(k) = p\text{-}1$

Lemma. $\Sigma_{\ k|p-1}\ \phi(k) = p\text{-}1$

let $\phi(1)=1$

pf. $p\text{-}1 = \Sigma_{\ k|p-1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

let p=13, $a \in Z_p^*$

gcd(a, p-1)=k, i.e. $k \mid p\text{-}1$

k=1, {1,5,7,11}, $\phi(12/1)$

$\Sigma_{k|p\text{-}1}\ \phi(k) = p\text{-}1$

Lemma. $\Sigma_{k|p\text{-}1}\ \phi(k) = p\text{-}1$ let $\phi(1)=1$

pf. $p\text{-}1 = \Sigma_{k|p\text{-}1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

let p=13, $a \in Z_p^*$

gcd(a, p-1)=k, i.e. $k \mid p$-1

k=1, {1,5,7,11}, ϕ(12/1)

k=2, {2,10}, ϕ(12/2)

$\Sigma_{k|p\text{-}1}\ \phi(k) = p\text{-}1$

Lemma. $\Sigma_{k|p\text{-}1}\ \phi(k) = p\text{-}1$

let $\phi(1)=1$

pf. $p\text{-}1 = \Sigma_{k|p\text{-}1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

let p=13, $a \in Z_p^*$

gcd(a, p-1)=k, i.e. $k \mid p\text{-}1$

k=1, {1,5,7,11}, $\phi(12/1)$

k=2, {2,10}, $\phi(12/2)$

k=3, {3,9}, $\phi(12/3)$

$\Sigma_{k|p-1}\ \phi(k) = p\text{-}1$

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, i.e. $k \mid p-1$

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)

$\Sigma_{k|p\text{-}1}\ \phi(k) = p\text{-}1$

Lemma. $\Sigma_{\,k|p\text{-}1}\ \phi(k) = p\text{-}1$ let $\phi(1)=1$

pf. $p\text{-}1 = \Sigma_{\,k|p\text{-}1}$ (# a in Z_p^* s.t. $\gcd(a, p\text{-}1) = k$)

let p=13, $a \in Z_p^*$

$\gcd(a, p\text{-}1)=k$, i.e. $k \mid p\text{-}1$

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}, $\phi(12/6)$

$\Sigma_{k|p\text{-}1}\ \phi(k) = p\text{-}1$

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 $p=13$, $a \in Z_p^*$

$\gcd(a, p-1)=k$, i.e. $k \mid p-1$

$k=1$, $\{1,5,7,11\}$, $\phi(12/1)$

$k=2$, $\{2,10\}$, $\phi(12/2)$

$k=3$, $\{3,9\}$, $\phi(12/3)$

$k=4$, $\{4,8\}$, $\phi(12/4)$

$k=6$, $\{6\}$, $\phi(12/6)$

$k=12$, $\{12\}$, $\phi(12/12)$

$\Sigma_{k|p\text{-}1}\, \phi(k) = p\text{-}1$

Lemma. $\Sigma_{k|p\text{-}1}\, \phi(k) = p\text{-}1$ let $\phi(1)=1$

pf. $p\text{-}1 = \Sigma_{k|p\text{-}1}$ (# a in Z_p^* s.t. $\gcd(a, p\text{-}1) = k$)

a/k

$= \Sigma_{k|p\text{-}1}$ (# b in $\{1,\ldots,(p\text{-}1)/k\}$ s.t. $\gcd(b, (p\text{-}1)/k) = 1$)

let $p=13$, $a \in Z_p^*$

$\gcd(a, p\text{-}1)=k$, i.e. $k \mid p\text{-}1$

$k=1$, $\{1,5,7,11\}$, $\phi(12/1)$

$k=2$, $\{2,10\}$, $\phi(12/2)$

$k=3$, $\{3,9\}$, $\phi(12/3)$

$k=4$, $\{4,8\}$, $\phi(12/4)$

$k=6$, $\{6\}$, $\phi(12/6)$

$k=12$, $\{12\}$, $\phi(12/12)$

$\Sigma_{k|p-1}\ \phi(k) = p-1$

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. $\gcd(a, p-1) = k$)

a/k

$= \Sigma_{k|p-1}$ (# b in $\{1,\ldots,(p-1)/k\}$ s.t. $\gcd(b, (p-1)/k) = 1$)

$= \Sigma_{k|p-1}\ \phi((p-1)/k)$

let $p=13$, $a \in Z_p^*$

$\gcd(a, p-1)=k$, i.e. $k \mid p-1$

$k=1$, $\{1,5,7,11\}$, $\phi(12/1)$

$k=2$, $\{2,10\}$, $\phi(12/2)$

$k=3$, $\{3,9\}$, $\phi(12/3)$

$k=4$, $\{4,8\}$, $\phi(12/4)$

$k=6$, $\{6\}$, $\phi(12/6)$

$k=12$, $\{12\}$, $\phi(12/12)$

$\Sigma_{k|p-1}\ \phi(k) = p-1$

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. $\gcd(a, p-1) = k$)

a/k

$= \Sigma_{k|p-1}$ (# b in $\{1,\ldots,(p-1)/k\}$ s.t. $\gcd(b, (p-1)/k) = 1$)

$= \Sigma_{k|p-1}\ \phi((p-1)/k)$

let $p=13$, $a \in Z_p^*$

$\gcd(a, p-1)=k$, i.e. $k \mid p-1$

$k=1$, $\{1,5,7,11\}$, $\phi(12/1)$

$k=2$, $\{2,10\}$, $\phi(12/2)$

$k=3$, $\{3,9\}$, $\phi(12/3)$

$k=4$, $\{4,8\}$, $\phi(12/4)$

$k=6$, $\{6\}$, $\phi(12/6)$

$k=12$, $\{12\}$, $\phi(12/12)$

$\phi(1\} + \phi(12) +$

$\phi(2) + \phi(6) +$

$\phi(3) + \phi(4)$

$\Sigma_{k|p-1}\ \phi(k) = p-1$

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. $\gcd(a, p-1) = k$)

a/k

$= \Sigma_{k|p-1}$ (# b in $\{1,\ldots,(p-1)/k\}$ s.t. $\gcd(b, (p-1)/k) = 1$)

$= \Sigma_{k|p-1}\ \phi((p-1)/k)$

let $p=13$, $a \in Z_p^*$

$\gcd(a, p-1)=k$, i.e. $k \mid p-1$

$k=1$, $\{1,5,7,11\}$, $\phi(12/1)$

$k=2$, $\{2,10\}$, $\phi(12/2)$

$k=3$, $\{3,9\}$, $\phi(12/3)$

$k=4$, $\{4,8\}$, $\phi(12/4)$

$k=6$, $\{6\}$, $\phi(12/6)$

$k=12$, $\{12\}$, $\phi(12/12)$

$\phi(1\} + \phi(12) +$

$\phi(2) + \phi(6) +$

$\phi(3) + \phi(4)$

$\Sigma_{k|p\text{-}1}\ \phi(k) = p\text{-}1$

<u>**Lemma**</u>. $\Sigma_{\ k|p\text{-}1}\ \phi(k) = p\text{-}1$ let $\phi(1)=1$

pf. $p\text{-}1 = \Sigma_{\ k|p\text{-}1}$ (# a in Z_p^* s.t. gcd(a, p-1) = k)

a/k

$= \Sigma_{\ k|p\text{-}1}$ (# b in $\{1,\ldots,(p\text{-}1)/k\}$ s.t. gcd(b, (p-1)/k) = 1)

$= \Sigma_{\ k|p\text{-}1}\ \phi((p\text{-}1)/k)$

let p=13, $a \in Z_p^*$

gcd(a, p-1)=k, i.e. $k \mid p$-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}, $\phi(12/12)$

$\phi(1\} + \phi(12)+$

$\phi(2) + \phi(6)+$

$\phi(3) + \phi(4)$

$\Sigma_{k|p-1} \phi(k) = p-1$

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. $\gcd(a, p-1) = k$)

a/k

$= \Sigma_{k|p-1}$ (# b in $\{1,\ldots,(p-1)/k\}$ s.t. $\gcd(b, (p-1)/k) = 1$)

$= \Sigma_{k|p-1} \phi((p-1)/k)$

let $p=13$, $a \in Z_p^*$

$\gcd(a, p-1)=k$, i.e. $k \mid p-1$

$k=1$, $\{1,5,7,11\}$, $\phi(12/1)$

$k=2$, $\{2,10\}$, $\phi(12/2)$

$k=3$, $\{3,9\}$, $\phi(12/3)$

$k=4$, $\{4,8\}$, $\phi(12/4)$

$k=6$, $\{6\}$, $\phi(12/6)$

$k=12$, $\{12\}$, $\phi(12/12)$

$\phi(1\} + \phi(12)+$

$\phi(2) + \phi(6)+$

$\phi(3) + \phi(4)$

$\Sigma_{k|p-1}\ \phi(k) = p-1$

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. $\gcd(a, p-1) = k$)

a/k

$= \Sigma_{k|p-1}$ (# b in $\{1,\ldots,(p-1)/k\}$ s.t. $\gcd(b, (p-1)/k) = 1$)

$= \Sigma_{k|p-1}\ \phi((p-1)/k)$

$= \Sigma_{k|p-1}\ \phi(k)$

$\phi(1\} + \phi(12)+$

$\phi(2) + \phi(6)+$

$\phi(3) + \phi(4)$

let $p=13$, $a \in Z_p^*$

$\gcd(a, p-1)=k$, i.e. $k \mid p-1$

$k=1$, $\{1,5,7,11\}$, $\phi(12/1)$

$k=2$, $\{2,10\}$, $\phi(12/2)$

$k=3$, $\{3,9\}$, $\phi(12/3)$

$k=4$, $\{4,8\}$, $\phi(12/4)$

$k=6$, $\{6\}$, $\phi(12/6)$

$k=12$, $\{12\}$, $\phi(12/12)$

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.

- ① # of ord-k elements in $Z_p^* \leq \phi(k)$, where $k \mid p$-1

  ② $\Sigma_{k|p\text{-}1}\ \phi(k) = p$-1

Z_p^* is a *cyclic* group

Theorem: Z_p^* is a ***cyclic*** group for a prime number p

pf.

- ① # of ord-k elements in $Z_p^* \leq \phi(k)$, where $k \mid p-1$

  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.

- ① # of ord-k elements in $Z_p^* \le \phi(k)$, where $k \mid p$-1

  ② $\Sigma_{k|p\text{-}1}\ \phi(k) = p$-1

- The order k of every element in Z_p^* divides p-1

  $\Rightarrow \Sigma_{k|p\text{-}1}$ (# of ord-k elements in Z_p^*) $= |Z_p^*| = p$-1

Z_p^* is a *cyclic* group

Theorem: Z_p^* is a ***cyclic*** group for a prime number p

pf.

- ① # of ord-k elements in $Z_p^* \le \phi(k)$, where $k \mid p$-1

  ② $\Sigma_{k|p\text{-}1}\ \phi(k) = p$-1
- The order k of every element in Z_p^* divides p-1

  $\Rightarrow \Sigma_{k|p\text{-}1}$ (# of ord-k elements in Z_p^*) $= |Z_p^*| = p$-1
- ① $\Rightarrow \Sigma_{k|p\text{-}1}$ (# of ord-k elements in Z_p^*) $\le \Sigma_{k|p\text{-}1}\ \phi(k)$,

  combined with ②, # 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.

- ① # of ord-k elements in $Z_p^* \le \phi(k)$, where $k \mid p$-1

  ② $\Sigma_{k|p\text{-}1}\ \phi(k) = p\text{-}1$
- The order k of every element in Z_p^* divides p-1

  $\Rightarrow \Sigma_{k|p\text{-}1}$ (# of ord-k elements in Z_p^*) $= |Z_p^*| = p\text{-}1$
- ① $\Rightarrow \Sigma_{k|p\text{-}1}$ (# of ord-k elements in Z_p^*) $\le \Sigma_{k|p\text{-}1}\ \phi(k)$,

  combined with ②, # of ord-k elements in $Z_p^* = \phi(k)$
- # of ord-(p-1) elements in $Z_p^* = \phi(p\text{-}1) > 1$

Z_p^* is a *cyclic* group

Theorem: Z_p^* is a ***cyclic*** group for a prime number p

pf.

- ① # of ord-k elements in $Z_p^* \le \phi(k)$, where $k \mid p$-1

  $\Sigma_{k|p\text{-}1}\ \phi(k) = p$-1

- The order k of every element in Z_p^* divides p-1

  $\Rightarrow \Sigma_{k|p\text{-}1}$ (# of ord-k elements in Z_p^*) $= |Z_p^*| = p$-1

- ① $\Rightarrow \Sigma_{k|p\text{-}1}$ (# of ord-k elements in Z_p^*) $\le \Sigma_{k|p\text{-}1}\ \phi(k)$,

  combined with ②, # of ord-k elements in $Z_p^* = \phi(k)$

- # of ord-(p-1) elements in $Z_p^* = \phi(p\text{-}1) > 1$

- 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.

- ① # of ord-k elements in $Z_p^* \leq \phi(k)$, where $k \mid p$-1

  $\Sigma_{k|p\text{-}1}\ \phi(k) = p$-1
- The order k of every element in Z_p^* divides p-1

  $\Rightarrow \Sigma_{k|p\text{-}1}$ (# of ord-k elements in Z_p^*) $= |Z_p^*| = p$-1
- ① $\Rightarrow \Sigma_{k|p\text{-}1}$ (# of ord-k elements in Z_p^*) $\leq \Sigma_{k|p\text{-}1}\ \phi(k)$, combined with ②, # of ord-k elements in $Z_p^* = \phi(k)$
- # of ord-(p-1) elements in $Z_p^* = \phi(p\text{-}1) > 1$
- 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

$Z^*_{p^s}$ is cyclic

- $Z^*_{p^s} = \{1, 2, \ldots, p-1,$
  $p+1, \ldots, 2p-1,$
  $\ldots,$
  $p^s-p+1, \ldots, p^s-1\}$

$\mathbf{Z}^*_{p^s}$ is cyclic

- $\mathbf{Z}^*_{p^s} = \{1, 2, \ldots, p-1,$
  $p+1, \ldots, 2p-1,$
  $\ldots,$
  $p^s-p+1, \ldots, p^s-1\}$

- group operator: multiplication mod p^s

$\mathbf{Z}^*_{p^s}$ is cyclic

- $\mathbf{Z}^*_{p^s} = \{1, 2, \ldots, \quad p\text{-}1,$
  $\quad p+1, \ldots, \quad 2p\text{-}1,$
  $\quad \ldots,$
  $\quad p^s\text{-}p+1, \ldots, p^s\text{-}1\}$
- group operator: multiplication mod p^s
- $|\mathbf{Z}^*_{p^s}| = \phi(p^s) = p^{s-1}(p-1)$

$\mathbf{Z}_{p^s}^*$ is cyclic

- $\mathbf{Z}_{p^s}^* = \{1, 2, \ldots, p-1,$
  $p+1, \ldots, 2p-1,$
  $\ldots,$
  $p^s-p+1, \ldots, p^s-1\}$
- group operator: multiplication mod p^s
- $|\mathbf{Z}_{p^s}^*| = \phi(p^s) = p^{s-1}(p-1)$

pf.

① $\mathbf{Z}_p^*$ is cyclic

$\mathbf{Z}^*_{p^s}$ is cyclic

✧ $\mathbf{Z}^*_{p^s} = \{1, 2, \ldots, p\text{-}1, p\text{+}1, \ldots, 2p\text{-}1, \ldots, p^s\text{-}p\text{+}1, \ldots, p^s\text{-}1\}$

✧ group operator: multiplication mod p^s

✧ $|\mathbf{Z}^*_{p^s}| = \phi(p^s) = p^{s-1}(p-1)$

pf.

① $\mathbf{Z}^*_p$ is cyclic

② assume $\mathbf{Z}^*_{p^2}, \mathbf{Z}^*_{p^3}, \ldots, \mathbf{Z}^*_{p^{s-1}}$ are cyclic

$\mathbf{Z}^*_{p^s}$ is cyclic

- $\mathbf{Z}^*_{p^s} = \{1, 2, \ldots, p\text{-}1,$
  $p+1, \ldots, 2p\text{-}1,$
  $\ldots,$
  $p^s\text{-}p+1, \ldots, p^s\text{-}1\}$
- group operator: multiplication mod p^s
- $|\mathbf{Z}^*_{p^s}| = \phi(p^s) = p^{s-1}(p\text{-}1)$

pf.

① $\mathbf{Z}^*_p$ is cyclic

② assume $\mathbf{Z}^*_{p^2}, \mathbf{Z}^*_{p^3}, \ldots, \mathbf{Z}^*_{p^{s-1}}$ are cyclic

③ $\exists\, g \in \mathbf{Z}^*_{p^{s-1}}$, $\langle g \rangle_{p^{s-1}} = \mathbf{Z}^*_{p^{s-1}}$, $\text{ord}_{p^{s-1}}(g) = p^{s-2}(p\text{-}1)$, $g^{p^{s-2}(p-1)} \equiv 1 \pmod{p^{s-1}}$

$\mathbf{Z}^*_{p^s}$ is cyclic

- $\mathbf{Z}^*_{p^s} = \{1, 2, \ldots, p\text{-}1,$
  $p+1, \ldots, 2p\text{-}1,$
  $\ldots,$
  $p^s\text{-}p+1, \ldots, p^s\text{-}1\}$
- group operator: multiplication mod p^s
- $|\mathbf{Z}^*_{p^s}| = \phi(p^s) = p^{s-1}(p-1)$

pf.

① $\mathbf{Z}^*_p$ is cyclic

② assume $\mathbf{Z}^*_{p^2}, \mathbf{Z}^*_{p^3}, \ldots, \mathbf{Z}^*_{p^{s-1}}$ are cyclic

③ $\exists\ g \in \mathbf{Z}^*_{p^{s-1}}$, $\langle g \rangle_{p^{s-1}} = \mathbf{Z}^*_{p^{s-1}}$, $\mathrm{ord}_{p^{s-1}}(g) = p^{s-2}(p-1)$, $g^{p^{s-2}(p-1)} \equiv 1 \pmod{p^{s-1}}$

④ consider the same g in ③, $\langle g \rangle_{p^i} = \mathbf{Z}^*_{p^i}$, i=1,2,…,s-2

$\mathbf{Z}_{p^s}^*$ is cyclic

- $\mathbf{Z}_{p^s}^* = \{1, 2, \ldots, p\text{-}1,$
  $p+1, \ldots, 2p\text{-}1,$
  $\ldots,$
  $p^s\text{-}p+1, \ldots, p^s\text{-}1\}$
- group operator: multiplication mod p^s
- $|\mathbf{Z}_{p^s}^*| = \phi(p^s) = p^{s-1}(p\text{-}1)$

pf.

① $\mathbf{Z}_p^*$ is cyclic

② assume $\mathbf{Z}_{p^2}^*, \mathbf{Z}_{p^3}^*, \ldots, \mathbf{Z}_{p^{s-1}}^*$ are cyclic

③ $\exists\, g \in \mathbf{Z}_{p^{s-1}}^*$, $\langle g \rangle_{p^{s-1}} = \mathbf{Z}_{p^{s-1}}^*$, $\mathrm{ord}_{p^{s-1}}(g) = p^{s-2}(p\text{-}1)$, $g^{p^{s-2}(p-1)} \equiv 1 \pmod{p^{s-1}}$

④ consider the same g in ③, $\langle g \rangle_{p^i} = \mathbf{Z}_{p^i}^*$, i=1,2,…,s-2

pf. (by contradiction, for each i=s-2, s-3, …, 1)

$\mathbf{Z}_{p^s}^*$ is cyclic

- $\mathbf{Z}_{p^s}^* = \{1, 2, \ldots, p\text{-}1,$
  $p+1, \ldots, 2p\text{-}1,$
  $\ldots,$
  $p^s\text{-}p+1, \ldots, p^s\text{-}1\}$
- group operator: multiplication mod p^s
- $|\mathbf{Z}_{p^s}^*| = \phi(p^s) = p^{s-1}(p\text{-}1)$

pf.

① $\mathbf{Z}_p^*$ is cyclic

② assume $\mathbf{Z}_{p^2}^*, \mathbf{Z}_{p^3}^*, \ldots, \mathbf{Z}_{p^{s-1}}^*$ are cyclic

③ $\exists\ g \in \mathbf{Z}_{p^{s-1}}^*$, $\langle g\rangle_{p^{s-1}} = \mathbf{Z}_{p^{s-1}}^*$, $\mathrm{ord}_{p^{s-1}}(g) = p^{s-2}(p\text{-}1)$, $g^{p^{s-2}(p-1)} \equiv 1 \pmod{p^{s-1}}$

④ consider the same g in ③, $\langle g\rangle_{p^i} = \mathbf{Z}_{p^i}^*$, i=1,2,…,s-2

pf. (by contradiction, for each i=s-2, s-3, …, 1)

if $g^k \equiv 1 \pmod{p^{s-2}}$, where $k < p^{s-3}(p\text{-}1)$ and $k \mid p^{s-3}(p\text{-}1)$, then $\exists\ \lambda$, $g^k = 1 + \lambda p^{s-2}$

$\mathbf{Z}^*_{p^s}$ is cyclic

- $\mathbf{Z}^*_{p^s} = \{1, 2, \ldots, p\text{-}1, p\text{+}1, \ldots, 2p\text{-}1, \ldots, p^s\text{-}p\text{+}1, \ldots, p^s\text{-}1\}$
- group operator: multiplication mod p^s
- $|\mathbf{Z}^*_{p^s}| = \phi(p^s) = p^{s-1}(p-1)$

pf.

① $\mathbf{Z}^*_p$ is cyclic

② assume $\mathbf{Z}^*_{p^2}, \mathbf{Z}^*_{p^3}, \ldots, \mathbf{Z}^*_{p^{s-1}}$ are cyclic

③ $\exists\, g \in \mathbf{Z}^*_{p^{s-1}}$, $\langle g \rangle_{p^{s-1}} = \mathbf{Z}^*_{p^{s-1}}$, $\text{ord}_{p^{s-1}}(g) = p^{s-2}(p-1)$, $g^{p^{s-2}(p-1)} \equiv 1 \pmod{p^{s-1}}$

④ consider the same g in ③, $\langle g \rangle_{p^i} = \mathbf{Z}^*_{p^i}$, i=1,2,…,s-2

pf. (by contradiction, for each i=s-2, s-3, …, 1)

if $g^k \equiv 1 \pmod{p^{s-2}}$, where $k < p^{s-3}(p-1)$ and $k \mid p^{s-3}(p-1)$, then $\exists\, \lambda$, $g^k = 1 + \lambda p^{s-2}$

$(g^k)^p \equiv (1+\lambda p^{s-2})^p \equiv 1 \pmod{p^{s-1}}$, where $kp < p^{s-2}(p-1)$

$\mathbf{Z}^*_{p^s}$ is cyclic

- $\mathbf{Z}^*_{p^s} = \{1, 2, \ldots, p\text{-}1,$
  $p+1, \ldots, 2p\text{-}1,$
  $\ldots,$
  $p^s\text{-}p+1, \ldots, p^s\text{-}1\}$
- group operator: multiplication mod p^s
- $|\mathbf{Z}^*_{p^s}| = \phi(p^s) = p^{s-1}(p\text{-}1)$

pf.

① $\mathbf{Z}^*_p$ is cyclic

② assume $\mathbf{Z}^*_{p^2}, \mathbf{Z}^*_{p^3}, \ldots, \mathbf{Z}^*_{p^{s-1}}$ are cyclic

③ $\exists\, g \in \mathbf{Z}^*_{p^{s-1}}$, $\langle g\rangle_{p^{s-1}} = \mathbf{Z}^*_{p^{s-1}}$, $\mathrm{ord}_{p^{s-1}}(g) = p^{s-2}(p\text{-}1)$, $g^{p^{s-2}(p-1)} \equiv 1 \pmod{p^{s-1}}$

④ consider the same g in ③, $\langle g\rangle_{p^i} = \mathbf{Z}^*_{p^i}$, i=1,2,…,s-2

pf. (by contradiction, for each i=s-2, s-3, …, 1)

if $g^k \equiv 1 \pmod{p^{s-2}}$, where $k < p^{s-3}(p\text{-}1)$ and $k \mid p^{s-3}(p\text{-}1)$, then $\exists\, \lambda$, $g^k = 1 + \lambda p^{s-2}$

$(g^k)^p \equiv (1+\lambda p^{s-2})^p \equiv 1 \pmod{p^{s-1}}$, where $kp < p^{s-2}(p\text{-}1)$

i.e. g is not a generator in $Z^*_{p^{s-1}}$, contradiction with ③

$Z^*_{p^s}$ is cyclic (cont'd)

⑤ let $n=\text{ord}_{p^s}(g)$, Euler's Thm $g^{p^{s-1}(p-1)} \equiv 1 \pmod{p^s} \Rightarrow n \mid p^{s-1}(p-1)$

$Z^*_{p^s}$ is cyclic (cont'd)

⑤ let n=ord$_{p^s}(g)$, Euler's Thm $g^{p^{s-1}(p-1)} \equiv 1 \pmod{p^s} \Rightarrow n \mid p^{s-1}(p-1)$

⑥ $g^n \equiv 1 \pmod{p^s} \Rightarrow g^n \equiv 1 \pmod{p^{s-1}} \Rightarrow$ ord$_{p^{s-1}}(g) = p^{s-2}(p-1) \mid n$

$Z_{p^s}^*$ is cyclic (cont'd)

⑤ let $n=\mathrm{ord}_{p^s}(g)$, Euler's Thm $g^{p^{s-1}(p-1)} \equiv 1 \pmod{p^s} \Rightarrow n \mid p^{s-1}(p-1)$

⑥ $g^n \equiv 1 \pmod{p^s} \Rightarrow g^n \equiv 1 \pmod{p^{s-1}} \Rightarrow \mathrm{ord}_{p^{s-1}}(g)=p^{s-2}(p-1) \mid n$

⑤,⑥ $\Rightarrow n = p^{s-2}(p-1)$ or $n = p^{s-1}(p-1)$

$Z^*_{p^s}$ is cyclic (cont'd)

⑤ let $n=\text{ord}_{p^s}(g)$, Euler's Thm $g^{p^{s-1}(p-1)} \equiv 1 \pmod{p^s} \Rightarrow n \mid p^{s-1}(p-1)$

⑥ $g^n \equiv 1 \pmod{p^s} \Rightarrow g^n \equiv 1 \pmod{p^{s-1}} \Rightarrow \text{ord}_{p^{s-1}}(g)=p^{s-2}(p-1) \mid n$

⑤,⑥ $\Rightarrow n = p^{s-2}(p-1)$ or $n = p^{s-1}(p-1)$

⑦ $\text{ord}_{p^{s-2}}(g) \overset{④}{=} p^{s-3}(p-1) \Rightarrow \exists\, \lambda,\ g^{p^{s-3}(p-1)} = 1+\lambda p^{s-2}$

$Z_{p^s}^*$ is cyclic (cont'd)

⑤ let $n=\mathrm{ord}_{p^s}(g)$, Euler's Thm $g^{p^{s-1}(p-1)} \equiv 1 \pmod{p^s} \Rightarrow n \mid p^{s-1}(p-1)$

⑥ $g^n \equiv 1 \pmod{p^s} \Rightarrow g^n \equiv 1 \pmod{p^{s-1}} \Rightarrow \mathrm{ord}_{p^{s-1}}(g)=p^{s-2}(p-1) \mid n$

⑤,⑥ $\Rightarrow n = p^{s-2}(p-1)$ or $n = p^{s-1}(p-1)$

④

⑦ $\mathrm{ord}_{p^{s-2}}(g) = p^{s-3}(p-1) \Rightarrow \exists\, \lambda,\ g^{p^{s-3}(p-1)} = 1+\lambda p^{s-2}$

$\mathrm{ord}_{p^{s-1}}(g) = p^{s-2}(p-1) \Rightarrow g^{p^{s-3}(p-1)} \neq 1 \pmod{p^{s-1}}$

$Z^*_{p^s}$ is cyclic (cont'd)

⑤ let $n=\mathrm{ord}_{p^s}(g)$, Euler's Thm $g^{p^{s-1}(p-1)} \equiv 1 \pmod{p^s} \Rightarrow n \mid p^{s-1}(p-1)$

⑥ $g^n \equiv 1 \pmod{p^s} \Rightarrow g^n \equiv 1 \pmod{p^{s-1}} \Rightarrow \mathrm{ord}_{p^{s-1}}(g)=p^{s-2}(p-1) \mid n$

⑤,⑥ $\Rightarrow$ $n = p^{s-2}(p-1)$ or $n = p^{s-1}(p-1)$

④

⑦ $\mathrm{ord}_{p^{s-2}}(g) = p^{s-3}(p-1) \Rightarrow \exists\ \lambda,\ g^{p^{s-3}(p-1)} = 1+\lambda p^{s-2}$

$\mathrm{ord}_{p^{s-1}}(g) = p^{s-2}(p-1) \Rightarrow g^{p^{s-3}(p-1)} \neq 1 \pmod{p^{s-1}}$

$\Rightarrow p \nmid \lambda$

$Z^*_{p^s}$ is cyclic (cont'd)

⑤ let $n = ord_{p^s}(g)$, Euler's Thm $g^{p^{s-1}(p-1)} \equiv 1 \pmod{p^s} \Rightarrow n \mid p^{s-1}(p-1)$

⑥ $g^n \equiv 1 \pmod{p^s} \Rightarrow g^n \equiv 1 \pmod{p^{s-1}} \Rightarrow ord_{p^{s-1}}(g) = p^{s-2}(p-1) \mid n$

⑤,⑥ $\Rightarrow n = p^{s-2}(p-1)$ or $n = p^{s-1}(p-1)$

④

⑦ $ord_{p^{s-2}}(g) = p^{s-3}(p-1) \Rightarrow \exists\, \lambda,\ g^{p^{s-3}(p-1)} = 1+\lambda p^{s-2}$

$ord_{p^{s-1}}(g) = p^{s-2}(p-1) \Rightarrow g^{p^{s-3}(p-1)} \neq 1 \pmod{p^{s-1}}$

$\Rightarrow p \nmid \lambda$

$$(g^{p^{s-3}(p-1)})^p \equiv (1+\lambda p^{s-2})^p \equiv 1 + p\lambda p^{s-2} + C_2^p \lambda^2 (p^{s-2})^2 + \ldots$$

$$\equiv 1+\lambda p^{s-1} \pmod{p^s}$$

$Z_{p^s}^*$ is cyclic (cont'd)

⑤ let $n=\mathrm{ord}_{p^s}(g)$, Euler's Thm $g^{p^{s-1}(p-1)} \equiv 1 \pmod{p^s} \Rightarrow n \mid p^{s-1}(p-1)$

⑥ $g^n \equiv 1 \pmod{p^s} \Rightarrow g^n \equiv 1 \pmod{p^{s-1}} \Rightarrow \mathrm{ord}_{p^{s-1}}(g) = p^{s-2}(p-1) \mid n$

⑤,⑥ $\Rightarrow n = p^{s-2}(p-1)$ or $n = p^{s-1}(p-1)$

④

⑦ $\mathrm{ord}_{p^{s-2}}(g) = p^{s-3}(p-1) \Rightarrow \exists\, \lambda,\ g^{p^{s-3}(p-1)} = 1+\lambda p^{s-2}$

$\mathrm{ord}_{p^{s-1}}(g) = p^{s-2}(p-1) \Rightarrow g^{p^{s-3}(p-1)} \neq 1 \pmod{p^{s-1}}$

$\Rightarrow p \nmid \lambda$

$$(g^{p^{s-3}(p-1)})^p \equiv (1+\lambda p^{s-2})^p \equiv 1 + p\lambda p^{s-2} + C_2^p \lambda^2 (p^{s-2})^2 + \ldots$$

$$\equiv 1+\lambda p^{s-1} \pmod{p^s}$$

$$p \nmid \lambda \Rightarrow g^{p^{s-2}(p-1)} \neq 1 \pmod{p^s} \quad \text{i.e. } n \neq p^{s-2}(p-1)$$

$Z^*_{p^s}$ is cyclic (cont'd)

⑤ let $n = \mathrm{ord}_{p^s}(g)$, Euler's Thm $g^{p^{s-1}(p-1)} \equiv 1 \pmod{p^s} \Rightarrow n \mid p^{s-1}(p-1)$

⑥ $g^n \equiv 1 \pmod{p^s} \Rightarrow g^n \equiv 1 \pmod{p^{s-1}} \Rightarrow \mathrm{ord}_{p^{s-1}}(g) = p^{s-2}(p-1) \mid n$

⑤,⑥ $\Rightarrow$ ~~$n = p^{s-2}(p-1)$~~ or $n = p^{s-1}(p-1)$

④

⑦ $\mathrm{ord}_{p^{s-2}}(g) = p^{s-3}(p-1) \Rightarrow \exists\, \lambda,\ g^{p^{s-3}(p-1)} = 1 + \lambda p^{s-2}$

$\mathrm{ord}_{p^{s-1}}(g) = p^{s-2}(p-1) \Rightarrow g^{p^{s-3}(p-1)} \neq 1 \pmod{p^{s-1}}$

$\Rightarrow p \nmid \lambda$

$$(g^{p^{s-3}(p-1)})^p \equiv (1+\lambda p^{s-2})^p \equiv 1 + p\lambda p^{s-2} + C_2^p \lambda^2 (p^{s-2})^2 + \ldots$$

$$\equiv 1 + \lambda p^{s-1} \pmod{p^s}$$

$p \nmid \lambda \Rightarrow g^{p^{s-2}(p-1)} \neq 1 \pmod{p^s}$ i.e. $n \neq p^{s-2}(p-1)$

$\mathbf{Z}^*_{p^s}$ is cyclic (cont'd)

⑤ let $n=\text{ord}_{p^s}(g)$, Euler's Thm $g^{p^{s-1}(p-1)} \equiv 1 \pmod{p^s} \Rightarrow n \mid p^{s-1}(p-1)$

⑥ $g^n \equiv 1 \pmod{p^s} \Rightarrow g^n \equiv 1 \pmod{p^{s-1}} \Rightarrow \text{ord}_{p^{s-1}}(g) = p^{s-2}(p-1) \mid n$

⑤,⑥ $\Rightarrow$ ~~$n = p^{s-2}(p-1)$~~ or $n = p^{s-1}(p-1)$

④

⑦ $\text{ord}_{p^{s-2}}(g) = p^{s-3}(p-1) \Rightarrow \exists\, \lambda,\ g^{p^{s-3}(p-1)} = 1+\lambda p^{s-2}$

$\text{ord}_{p^{s-1}}(g) = p^{s-2}(p-1) \Rightarrow g^{p^{s-3}(p-1)} \neq 1 \pmod{p^{s-1}}$

$\Rightarrow p \nmid \lambda$

$$(g^{p^{s-3}(p-1)})^p \equiv (1+\lambda p^{s-2})^p \equiv 1 + p\lambda p^{s-2} + C_2^p \lambda^2 (p^{s-2})^2 + \ldots$$

$$\equiv 1+\lambda p^{s-1} \pmod{p^s}$$

$p \nmid \lambda \Rightarrow g^{p^{s-2}(p-1)} \neq 1 \pmod{p^s}$ i.e. $n \neq p^{s-2}(p-1)$

⑧ $n=\text{ord}_{p^s}(g)=p^{s-1}(p-1)=|\mathbf{Z}^*_{p^s}|$

$\mathbf{Z}^*_{p^s}$ is cyclic (cont'd)

⑤ let $n=\text{ord}_{p^s}(g)$, Euler's Thm $g^{p^{s-1}(p-1)} \equiv 1 \pmod{p^s} \Rightarrow n \mid p^{s-1}(p-1)$

⑥ $g^n \equiv 1 \pmod{p^s} \Rightarrow g^n \equiv 1 \pmod{p^{s-1}} \Rightarrow \text{ord}_{p^{s-1}}(g)=p^{s-2}(p-1) \mid n$

⑤,⑥ $\Rightarrow$ ~~$n = p^{s-2}(p-1)$~~ or $n = p^{s-1}(p-1)$

④

⑦ $\text{ord}_{p^{s-2}}(g) = p^{s-3}(p-1) \Rightarrow \exists\, \lambda,\ g^{p^{s-3}(p-1)} = 1+\lambda p^{s-2}$

$\text{ord}_{p^{s-1}}(g) = p^{s-2}(p-1) \Rightarrow g^{p^{s-3}(p-1)} \neq 1 \pmod{p^{s-1}}$

$\Rightarrow p \nmid \lambda$

$$(g^{p^{s-3}(p-1)})^p \equiv (1+\lambda p^{s-2})^p \equiv 1 + p\lambda p^{s-2} + C^p_2\, \lambda^2 (p^{s-2})^2 + \ldots$$

$$\equiv 1+\lambda p^{s-1} \pmod{p^s}$$

$p \nmid \lambda \Rightarrow g^{p^{s-2}(p-1)} \neq 1 \pmod{p^s}$ i.e. $n \neq p^{s-2}(p-1)$

⑧ $n=\text{ord}_{p^s}(g)=p^{s-1}(p-1)=|\mathbf{Z}^*_{p^s}|$, hence $\langle g \rangle_{p^s}=\mathbf{Z}^*_{p^s}$ is cyclic □

Quadratic Residue modulo p^s

- For each $x \in \mathbf{Z}^*_{p^s}$, p^s-$x \neq x \pmod{p^s}$ (since if x is odd, p^s-x is even), it's clear that x and p^s-x are both square roots of a certain $y \in \mathbf{Z}^*_{p^s}$

Quadratic Residue modulo p^s

- For each $x \in \mathbf{Z}^*_{p^s}$, $p^s - x \neq x \pmod{p^s}$ (since if x is odd, $p^s - x$ is even), it's clear that x and $p^s - x$ are both square roots of a certain $y \in \mathbf{Z}^*_{p^s}$

- Because there are only $p^{s-1}(p-1)$ elements in $\mathbf{Z}^*_{p^s}$, we know that number of quadratic residues $|QR_{p^s}| \leq p^{s-1}(p-1)/2$

Quadratic Residue modulo p^s

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

Quadratic Residue modulo p^s

- For each $x \in \mathbf{Z}^*_{p^s}$, $p^s - x \neq x \pmod{p^s}$ (since if x is odd, $p^s - x$ is even), it's clear that x and $p^s - x$ are both square roots of a certain $y \in \mathbf{Z}^*_{p^s}$

- Because there are only $p^{s-1}(p-1)$ elements in $\mathbf{Z}^*_{p^s}$, we know that number of quadratic residues $|QR_{p^s}| \le p^{s-1}(p-1)/2$

- Because $\mathbf{Z}^*_{p^s}$ is cyclic, $| \{g^2, g^4, \ldots, g^{p^{s-1}(p-1)}\} | = p^{s-1}(p-1)/2$, there can be no more quadratic residues outside this set. Therefore, the set $\{g, g^3, \ldots, g^{p^{s-1}(p-1)-1}\}$ contains only quadratic non-residues

$$|\mathbf{QR}_{p^s}| = p^{s-1}(p-1)/2$$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z + \lambda_1 p$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \;\Rightarrow\; y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z+\lambda_1 p$

  $\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z + \lambda_1 p$

  $$\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$$

  $$\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s} \quad \square$$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z+\lambda_1 p$

  $$\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$$

  $$\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s} \quad \square$$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z+\lambda_1 p$

  $\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$

  $\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s}$ ▯

- Solve $z^2 \equiv b \pmod{p^s}$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z + \lambda_1 p$

  $\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$

  $\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s}$ ▯

- let b be a quadratic residue mod p and mod p^s

- Solve $z^2 \equiv b \pmod{p^s}$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z + \lambda_1 p$

  $\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$

  $\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s}$ ∎

- let b be a quadratic residue mod p and mod p^s

  i.e. $b^{(p-1)/2} \equiv 1 \pmod{p}$ and $b^{p^{s-1}(p-1)/2} \equiv 1 \pmod{p^s}$

- Solve $z^2 \equiv b \pmod{p^s}$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z+\lambda_1 p$

  $$\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$$

  $$\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s} \quad \square$$

- let b be a quadratic residue mod p and mod p^s

  i.e. $b^{(p-1)/2} \equiv 1 \pmod{p}$ and $b^{p^{s-1}(p-1)/2} \equiv 1 \pmod{p^s}$ ← not necessary

- Solve $z^2 \equiv b \pmod{p^s}$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z+\lambda_1 p$

  $\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$

  $\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s}$ □

- let b be a quadratic residue mod p and mod p^s

  i.e. $b^{(p-1)/2} \equiv 1 \pmod{p}$ and $b^{p^{s-1}(p-1)/2} \equiv 1 \pmod{p^s}$

- Solve **$z^2 \equiv b \pmod{p^s}$**

  let $q = p^s$, $r = p^{s-1}$, $e = (q-2r+1) / 2 = (p^s-2p^{s-1}+1)/2$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z+\lambda_1 p$

  $\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$

  $\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s}$ ▯

- let b be a quadratic residue mod p and mod p^s

  i.e. $b^{(p-1)/2} \equiv 1 \pmod{p}$ and $b^{p^{s-1}(p-1)/2} \equiv 1 \pmod{p^s}$

- Solve $z^2 \equiv b \pmod{p^s}$ $\phi(q) = \phi(p^s) = p^{s-1}(p-1)$

  let $q = p^s$, $r = p^{s-1}$, $e = (q-2r+1) / 2 = (p^s-2p^{s-1}+1)/2$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z+\lambda_1 p$

  $\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$

  $\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s}$ ▯

- let b be a quadratic residue mod p and mod p^s

  i.e. $b^{(p-1)/2} \equiv 1 \pmod{p}$ and $b^{p^{s-1}(p-1)/2} \equiv 1 \pmod{p^s}$

- Solve $z^2 \equiv b \pmod{p^s}$ $\phi(q) = \phi(p^s) = p^{s-1}(p-1)$

  let $q = p^s$, $r = p^{s-1}$, $e = (q-2r+1) / 2 = (p^s-2p^{s-1}+1)/2$

- If x satisfies $x^2 \equiv b \pmod{p}$, then $z \equiv \pm x^r b^e \pmod{p^s}$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod p \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod p \Rightarrow y = z+\lambda_1 p$

  $$\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$$

  $$\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s} \quad \square$$

- let b be a quadratic residue mod p and mod p^s

  i.e. $b^{(p-1)/2} \equiv 1 \pmod p$ and $b^{p^{s-1}(p-1)/2} \equiv 1 \pmod{p^s}$

- Solve $z^2 \equiv b \pmod{p^s}$ $\qquad \phi(q) = \phi(p^s) = p^{s-1}(p-1)$

  let $q = p^s$, $r = p^{s-1}$, $e = (q-2r+1) / 2 = (p^s-2p^{s-1}+1)/2$

- If x satisfies $x^2 \equiv b \pmod p$, then $z \equiv \pm x^r b^e \pmod{p^s}$

Tonelli's 1891 note

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z + \lambda_1 p$

  $\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$

  $\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s}$ ▯

- let b be a quadratic residue mod p and mod p^s

  i.e. $b^{(p-1)/2} \equiv 1 \pmod{p}$ and $b^{p^{s-1}(p-1)/2} \equiv 1 \pmod{p^s}$

- Solve $z^2 \equiv b \pmod{p^s}$ $\qquad \phi(q) = \phi(p^s) = p^{s-1}(p-1)$

  let $q = p^s$, $r = p^{s-1}$, $e = (q-2r+1)/2 = (p^s-2p^{s-1}+1)/2$

- If x satisfies $x^2 \equiv b \pmod{p}$, then $z \equiv \pm x^r b^e \pmod{p^s}$

  Tonelli's 1891 note

pf. $z^2 \equiv (x^r b^e)^2$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod{p} \Rightarrow y = z+\lambda_1 p$

  $\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$

  $\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s}$ ▯

- let b be a quadratic residue mod p and mod p^s

  i.e. $b^{(p-1)/2} \equiv 1 \pmod{p}$ and $b^{p^{s-1}(p-1)/2} \equiv 1 \pmod{p^s}$

- Solve $z^2 \equiv b \pmod{p^s}$ $\phi(q) = \phi(p^s) = p^{s-1}(p-1)$

  let $q = p^s$, $r = p^{s-1}$, $e = (q-2r+1) / 2 = (p^s-2p^{s-1}+1)/2$

- If x satisfies $x^2 \equiv b \pmod{p}$, then $z \equiv \pm x^r b^e \pmod{p^s}$

  Tonelli's 1891 note

pf. $z^2 \equiv (x^r b^e)^2 \equiv b^{p^{s-1}} \cdot b^{p^s-2p^{s-1}+1}$

Square root mod prime power p^s

- Lemma: $y \equiv z \pmod p \;\Rightarrow\; y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

  pf. $y \equiv z \pmod p \Rightarrow y = z + \lambda_1 p$

  $$\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$$

  $$\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s} \qquad \square$$

- let b be a quadratic residue mod p and mod p^s

  i.e. $b^{(p-1)/2} \equiv 1 \pmod p$ and $b^{p^{s-1}(p-1)/2} \equiv 1 \pmod{p^s}$

- Solve $z^2 \equiv b \pmod{p^s}$ $\qquad \phi(q) = \phi(p^s) = p^{s-1}(p-1)$

  let $q = p^s$, $r = p^{s-1}$, $e = (q-2r+1)/2 = (p^s-2p^{s-1}+1)/2$

- If x satisfies $x^2 \equiv b \pmod p$, then $z \equiv \pm x^r b^e \pmod{p^s}$

Tonelli's 1891 note

pf. $z^2 \equiv (x^r b^e)^2 \equiv b^{p^{s-1}} \cdot b^{p^s-2p^{s-1}+1}$

$x^2 \equiv b \pmod p \;\Rightarrow\; (x^2)^r \equiv b^r \pmod{p^s}$

Square root mod prime power p^s

➢ Lemma: $y \equiv z \pmod{p} \Rightarrow y^{p^{s-1}} \equiv z^{p^{s-1}} \pmod{p^s}$

pf. $y \equiv z \pmod{p} \Rightarrow y = z + \lambda_1 p$

$$\Rightarrow y^{p^{s-1}} \equiv (z+\lambda_1 p)^{p^{s-1}} \equiv z^{p^{s-1}} + p^{s-1}\lambda_1 p + \ldots \pmod{p^s}$$

$$\Rightarrow y^{p^{s-1}} = z^{p^{s-1}} \pmod{p^s} \quad \square$$

➢ let b be a quadratic residue mod p and mod p^s

i.e. $b^{(p-1)/2} \equiv 1 \pmod{p}$ and $b^{p^{s-1}(p-1)/2} \equiv 1 \pmod{p^s}$

➢ Solve $z^2 \equiv b \pmod{p^s}$ $\quad \phi(q) = \phi(p^s) = p^{s-1}(p-1)$

let $q = p^s$, $r = p^{s-1}$, $e = (q-2r+1)/2 = (p^s-2p^{s-1}+1)/2$

➢ If x satisfies $x^2 \equiv b \pmod{p}$, then $z \equiv \pm x^r b^e \pmod{p^s}$

Tonelli's 1891 note

pf. $z^2 \equiv (x^r b^e)^2 \equiv b^{p^{s-1}} \cdot b^{p^s-2p^{s-1}+1} \equiv b^{p^{s-1}(p-1)} \cdot b \equiv b \pmod{p^s} \quad \square$

$x^2 \equiv b \pmod{p} \Rightarrow (x^2)^r \equiv b^r \pmod{p^s}$

Square root mod n

- Solve $z^2 \equiv b \pmod{n}$

Square root mod n

- Solve $z^2 \equiv b \pmod{n}$

- from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$

Square root mod *n*

- Solve $z^2 \equiv b \pmod{n}$

- from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$
  - check if b is a quadratic residue modulo $p_i^{c_i}$

Square root mod *n*

- Solve $z^2 \equiv b \pmod{n}$

- from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$
  - check if b is a quadratic residue modulo $p_i^{c_i}$
  - find square roots modulo each prime power $p_i^{c_i}$

Square root mod n

- Solve $z^2 \equiv b \pmod{n}$
- from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$
  - check if b is a quadratic residue modulo $p_i^{c_i}$
  - find square roots modulo each prime power $p_i^{c_i}$
- combine the results using Chinese Remainer Theorem

Square root mod *n*

- Solve $z^2 \equiv b \pmod{n}$

- from **Unique Prime Factorization Theorem**: $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$
  - check if b is a quadratic residue modulo $p_i^{c_i}$
  - find square roots modulo each prime power $p_i^{c_i}$

- combine the results using Chinese Remainer Theorem
  - there are 2^k square roots