Basic Number theory

Prof. Ashok K Bhateja, IIT Delhi

Algorithms Complexity

- **Polynomial-time algorithm** is an algorithm whose worst-case running time function is of the form $O(n^k)$, where n is the input size and k is a constant.
- **Subexponential-time algorithm** is an algorithm whose worst-case running time function is of the form $e^{O(n)}$, where n is the input size.

  A subexponential-time algorithm is asymptotically faster than an algorithm whose running time is fully exponential in the input size, while it is asymptotically slower than a polynomial-time algorithm.
- Definition: **Decision problems**, i.e., problems which have either YES or NO as an answer.

Algorithms Complexity

- The **complexity class NP** is the class of problems that can be verified by a polynomial-time algorithm.
- Definition The **complexity class NP** is the set of all decision problems for which a YES answer can be verified in polynomial time using some extra information, called a certificate.
- Example: COMPOSITES belongs to NP because if an integer n is composite, then this fact can be verified in polynomial time if one is given a divisor a of n, where $1 < a < n$ (the certificate in this case consists of the divisor a).

NP Complete

- Definition Let L_1 and L_2 be two decision problems. **L_1 is said to polytime reduce to L_2**, written $L_1 \leq_p L_2$, if there exists a polynomial-time computable function f such that $f(L_1) = L_2$.

  This function f is called the **reduction function**, and a polynomial-time algorithm that computes f is a **reduction algorithm**.

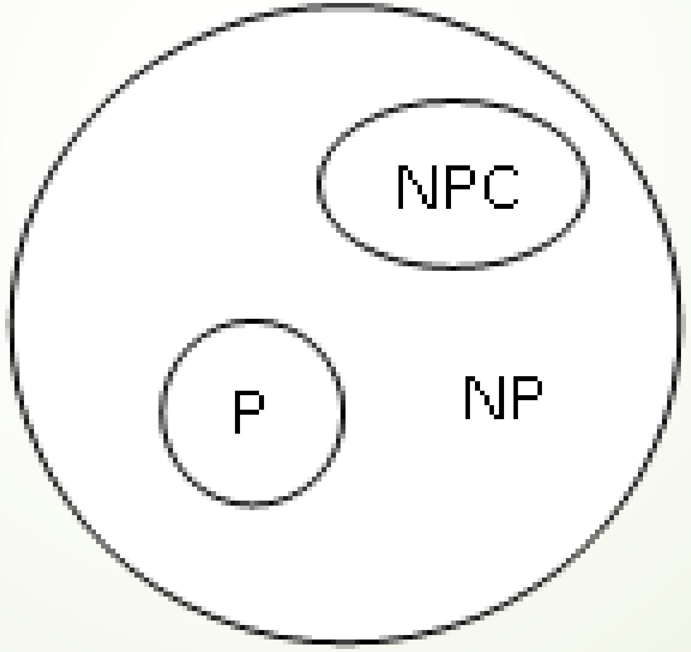
- Definition A decision problem L is said to be **NP-complete** if

  1. $L \in NP$ and
  2. $L_1 \leq_p L$ for every $L_1 \in NP$.

  Example: Subset sum problem, clique problem, vertex cover problem

- If a problem L satisfies property 2, but not necessarily property 1, we say that L is ***NP-hard***.

- Example (NP-hard problem): Given positive integers $a_1, a_2, ..., a_n$ and a positive integer s, finding a subset of the a_i which sums to s, provided that such a subset exists. This problem is NP-hard.



Greatest Common Divisor

- Definition: An integer c is a **common divisor** of a and b if c/a and c/b.
- Definition A non-negative integer d is the greatest common divisor of integers a and b, denoted $d = \gcd(a, b)$, if
  1. d is a common divisor of a and b; and
  2. whenever c/a and c/b, then c/d.
- Example: The common divisors of 12 and 18 are $\{\pm 1, \pm 2, \pm 3, \pm 6\}$, and gcd (l2, 18) = 6.
- Fact: For any integer $k \neq 0$, $\gcd(ka, kb) = |k| \gcd(a, b)$.

Euclidean algorithm or Euclid's algorithm

- It is an efficient method for computing GCD of two numbers, the largest number that divides both without leaving a remainder.
- It is named after the ancient Greek mathematician Euclid.

For two given numbers a and b, such that $a \geq b$

if b / a, then gcd (a, b) = b,

otherwise gcd (a, b) = gcd (b, a mod b).

Euclidean algorithm (Example)

gcd (138, 105)

$138 = 1 \times 105 + 33$

$105 = 3 \times 33 + 6$

$33 = 5 \times 6 + 3$

$6 = 2 \times 3 + 0$

Therefore gcd (138, 105) = 3

- If gcd $(a, b) = 1$, then a and b are said to be coprime (or relatively prime) e.g., 6 and 35

Fact: If a and b are not both zero, then for any integers x and y

$$\gcd(a, b) \mid (ax + by).$$

(Bezout's Theorem): If a and b are integers, not both zero, then there are integers x and y such that $ax + by = \gcd(a, b)$.

Use the Euclidean Algorithm to determine the GCD, then work backwards using substitution.

gcd (138, 105) $138 = 1 \times 105 + 33$ $105 = 3 \times 33 + 6$ $33 = 5 \times 6 + 3$ $6 = 2 \times 3 + 0$	$3 = 33 - 5\times6$ $3 = 33 - 5 \times (105 - 3\times33)$ $3 = 16 \times 33 - 5 \times 105$ $3 = 16 \times (138 - 1\times105) - 5 \times 105$ $3 = 16 \times 138 - 21\times105$

Lemma: If a and b are integers such that there are integers x and y with $ax + by = 1$, then $\gcd(a, b) = 1$.

Congruences

- Given three integers a, b and n; a is congruent to b modulo n i.e., write $a \equiv b \bmod n$, if the difference $a - b$ is divisible by n.
- n is called the modulus of the congruence.
- Theorem: Let $a, a', b, b', n \in Z$ with $n > 0$. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

  $a + b \equiv a' + b' \pmod{n}$ and $a \cdot b \equiv a' \cdot b' \pmod{n}$.

Theorem: Let $a, x, y \in Z$ and $n \in N$. Then

$$a\,x \equiv a\,y \pmod{n} \Leftrightarrow x \equiv y \pmod{n/\gcd(a, n)}.$$

If $a\,x \equiv a\,y \pmod{n}$ and $\gcd(a, n) = 1$, then $x \equiv y \pmod{n}$

Proof. Observe first that when $\gcd(a, n) = 1$, then

$$n \mid a\,(x - y) \Leftrightarrow n \mid (x - y).$$

i.e. whenever $(a, n) = 1$,

$a\,x \equiv a\,y \pmod{n}$ implies $x \equiv y \pmod{n}$

When $\gcd(a, n) > 1$, on the other hand, one does at least have

$$\left(\frac{a}{\gcd(a,n)}, \frac{n}{\gcd(a,n)}\right) = 1, \text{ so that}$$

$$n \mid a(x-y) \;\Leftrightarrow \frac{n}{\gcd(a,n)} \,\Big|\, \frac{a}{\gcd(a,n)}(x-y) \Leftrightarrow \frac{n}{\gcd(a,n)} \,\Big|\, (x-y)$$

Multiplicative Inverse of *a* modulo *n*

Let $a \in Z_n$. The **multiplicative inverse of *a* modulo *n*** is an integer $x \in Z_n$, s.t., $ax \equiv 1 \pmod{n}$. If such an x exists, then it is unique, and a is said to be invertible, or a unit.

Theorem: If $ax + by = 1$ then $x^{-1} \bmod y \equiv a$

Proof: $ax + by = 1$

Taking mod y both sides

$ax \bmod y + by \bmod y \equiv 1 \bmod y$

$\Rightarrow ax \bmod y \equiv 1 \Rightarrow x^{-1} \bmod y \equiv a$

Multiplicative Inverse : Example

Find $35^{-1} \bmod 51$

$51 = 1 \times 35 + 16$

$35 = 2 \times 16 + 3$

$16 = 5 \times 3 + 1$

$16 = 5 \times 3 + 1 \Rightarrow 1 = 16 - 5 \times 3$

$\Rightarrow 1 = 16 - 5 \times (35 - 2 \times 16)$ because $3 = 35 - 2 \times 16$

$\Rightarrow 1 = 11 \times 16 + (-5) \times 35$

$\Rightarrow 1 = 11 \times (51 - 1 \times 35) + (-5) \times 35$

$\Rightarrow 1 = 11 \times 51 + (-16) \times 35$

Taking mod 51 both side $(-16) \times 35 \equiv 1 \bmod 51 \Rightarrow 35^{-1} \bmod 51 \equiv -16$

or $35^{-1} \bmod 51 \equiv 35$

Theorem: If a and b are integers, m is a positive integer. Given the congruence $ax \equiv b \pmod{m}$.

1. If gcd $(a, m) = 1$, then the congruence has a unique solution.
2. If gcd $(a, m) = d$ and $d \mid b$, then the congruence has d solutions.
3. If gcd $(a, m) = d$ and $d \nmid b$, then the congruence has no solution.

Proof : Case 1: Let y be another solution to $ax \equiv b \pmod{m}$

$ax \equiv ay \equiv b \pmod{m} \Rightarrow a\,(x - y) \equiv 0 \pmod{m}$

then m divides $a\,(x - y)$ and as m and a are relatively prime and have no factors in common, m divides $x - y$.

Hence $x \equiv y \pmod{m}$.

As gcd $(a, m) = 1$, $\exists$ integers x and y s.t. $ax + my \equiv 1 \pmod{m}$

i.e., $ax \equiv 1 \pmod{m}$. Hence x is a unique solution to $ax \equiv b \pmod{m}$.

Theorem: If a and b are integers, m is a positive integer. Given the congruence $ax \equiv b \pmod{m}$.

1. If gcd $(a, m) = 1$, then the congruence has a unique solution.
2. If gcd $(a, m) = d$ and $d \mid b$, then the congruence has d solutions.
3. If gcd $(a, m) = d$ and $d \nmid b$, then the congruence has no solution.

Case 2: gcd $(a, m) = d$ and $d \mid b$.

Let $m' = m/d$ and $a' = a/d$; gcd $(a', m') = 1$

Then $ax \equiv b \pmod{m} \Longrightarrow ax - b$ is divisible by m

$\Longrightarrow a'd\,x - dk$ is divisible by $m'd$. So, $a'x - k$ is divisible by m'

or $a'x \equiv k \pmod{m'}$ which has exactly one solution.

Let that solution be g. Any solution x must be so that $x \equiv g \pmod{m'}$

$\Longrightarrow$ there are d such x, where $x = g + jm'$; $0 \le j < d$

Theorem: If a and b are integers, m is a positive integer. Given the congruence $ax \equiv b \pmod{m}$.

1. If gcd $(a, m) = 1$, then the congruence has a unique solution.
2. If gcd $(a, m) = d$ and $d \mid b$, then the congruence has d solutions.
3. If gcd $(a, m) = d$ and $d \nmid b$, then the congruence has no solution.

Proof : Case 3: Suppose that x_0 is a solution of $ax \equiv b \pmod{m}$.

$\therefore\ ax_0 \equiv b \pmod{m}$, hence, $ax_0 - b = km$ for some integer k.

Since $d \mid a$ and $d \mid m$ it follows that $d \mid b$.

By contraposition, if $d \nmid b$, then no solution exists to $ax \equiv b \pmod{m}$.

Prime Number

An integer $p \geq 2$ is said to be **prime** if its only positive divisors are 1 and p. Otherwise, p is called composite.

Prime Number Theorem: Let $\pi(x)$ denotes the number of prime numbers $\leq x$. Then

$$\lim_{x\to\infty} \frac{\pi(x)}{x/ln(x)} = 1$$

i.e., for large values of x, $\pi(x)$ is closely approximated by the expression $x/\ln(x)$. e.g. for $x = 10^{10}$, $\pi(x) = 455{,}052{,}511$.

Euler phi-function

Let n be a positive integer. The Euler phi-function $\varphi(n)$ is defined as $\varphi(n)$ = number of nonnegative integers less than n which are co-prime to n.

Properties of Euler phi-function:

1. $\varphi(1) = 1$
2. If p is a prime, then $\varphi(p) = p - 1$
3. If gcd $(m, n) = 1$, then $\varphi(mn) = \varphi(m) \cdot \varphi(n)$
   i.e., Euler phi function is multiplicative.
4. If $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is the prime factorization of n, then

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right)$$

$$= n\,(1 - 1/p_1).\,(1 - 1/p_2) \ldots (1 - 1/p_k).$$

Chinese Remainder Theorem (CRT)

Let $m_1, m_2 \ldots m_r$ be relatively coprime. Then the system of equations

$$x \equiv a_1 \bmod m_1,$$
$$x \equiv a_2 \bmod m_2,$$
$$\ldots \quad \ldots$$
$$x \equiv a_r \bmod m_r$$

has a unique solution $x \equiv \sum_{i=1}^{r} a_i N_i z_i \bmod N$

where $N = m_1 . m_2 \ldots m_r$, $N_i = \frac{N}{m_i}$ and $z_i = N_i^{-1} \bmod m_i$

CRT: Example

Example: Solve the system of congruences

$x \equiv 1 \bmod 3$

$x \equiv 4 \bmod 5$

$x \equiv 6 \bmod 7$

Solution: Here $N = 105$, $N_1 = 35$, $N_2 = 21$, $N_3 = 15$

$$x \equiv \{(1 \cdot 35 \cdot 35^{-1} mod\ 3) + (4 \cdot 21 \cdot 21^{-1} mod\ 5) + (6 \cdot 15 \cdot 15^{-1} mod\ 7)\}\ mod\ 105$$

$$x \equiv \{(1 \cdot 35 \cdot 2) + (4 \cdot 21 \cdot 1) + (6 \cdot 15 \cdot 1)\}\ mod\ 105$$

$$\equiv 244\ mod\ 105 \equiv 34\ mod\ 105$$

Fact: If $\gcd(n_1, n_2) = 1$, then the pair of congruences $x \equiv a \pmod{n_1}$, $x \equiv a \pmod{n_2}$, has a unique solution $x \equiv a \pmod{n_1 n_2}$.

Solution of linear congruences when moduli are not relatively prime

- CRT works only if pair of moduli are coprime.
- If a pair of congruences are not coprime, then we can split each of the congruences into two congruences so that the new moduli are relatively prime.
- If both m_1 and m_2 are divisible by prime p, then split each of the congruences into two congruences where one of the new moduli is the factor having highest power of p.

Splitting a single congruence

- A single congruence

  $x \equiv a \bmod (m_1 m_2)$ can be written as

  $x \equiv a \bmod m_1$ and $x \equiv a \bmod m_2$

  Example: $x \equiv 3 \bmod 63$ is equivalent to

  $x \equiv 3 \bmod 7$ and $x \equiv 3 \bmod 9$

Splitting of two congruences both divisible by a prime

Example: $x \equiv 3 \bmod 63$ and $x \equiv 5 \bmod 108$

Here 3 is a prime, both 63 (= $3^2 \times 7$) and 108 (= $3^3 \times 4$) are divisible by 3.

Split into four congruences:

$x \equiv 3 \pmod 9$

$x \equiv 5 \pmod{27}$

$x \equiv 3 \pmod 7$

$x \equiv 5 \pmod 4$

- If both the congruences involve powers of a same prime p, then one of following will be true
  - The congruences are contradictory and so there are no solutions.

  Example: $x \equiv 3 \pmod 9$

  $x \equiv 5 \pmod{27}$; $x = 5, 32, 59, \ldots \not\equiv 3 \pmod 9$

  - Both congruences for powers of p are implied by the congruence with the higher power. So, the other congruence (with lower power of p) may be ignored.

  Example: $x \equiv 5 \pmod 9$

  $x \equiv 23 \pmod{27}$; $x = 23, 50, \ldots \equiv 5 \pmod 9$

- Example: Solve the system of congruences

$$x \equiv 7 \pmod{200}$$
$$x \equiv 82 \pmod{375}$$

- Split each into two congruences

$$x \equiv 7 \pmod{25}$$
$$x \equiv 82 \pmod{125}$$
$$x \equiv 7 \pmod{8}$$
$$x \equiv 82 \pmod{3}$$

Here 1^{st} congruence is a special case of 2^{nd} congruence.

Therefore 1^{st} congruence can be ignored.

- The congruence equations with relatively prime moduli are

$$x \equiv 82 \pmod{125}$$
$$x \equiv 7 \pmod{8}$$
$$x \equiv 82 \pmod{3}$$

These can be solved by CRT. Solution: $x = 1207 \pmod{3000}$

Equivalence Relation

Theorem: Let n be a positive integer. For all a, b, $c \in$ Z

1. $a \equiv a \pmod{n}$;
2. $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$;
3. $a \equiv b \pmod{n}$ & $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

This means for any fixed +ve integer n, the binary relation "$\cdot \equiv \cdot \pmod{n}$" is an equivalence relation on the set Z.

This relation partitions the set Z into equivalence classes.

We denote the equivalence class containing the integer a by $[a]$.

i.e., $z \in [a] \Leftrightarrow z \equiv a \pmod{n} \Leftrightarrow z = a + ny$ for some $y \in$ Z.

These equivalence classes are called residue classes modulo n

Z_n to be the set of residue classes modulo n.

Z_n consists of the n distinct residue classes $[0], [1], \ldots, [n - 1]$.

Example: The residue classes modulo 6 :

$[0] = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$; $[1] = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$

$[2] = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$; $[3] = \{\ldots, -9, -3, 3, 9, 15, \ldots\}$

$[4] = \{\ldots, -8, -2, 4, 10, 16, \ldots\}$; $[5] = \{\ldots, -7, -1, 5, 11, 17, \ldots\}$

Facts:

- The residue class [0] acts as an additive identity
- The residue class [1] acts as a multiplicative identity
- Every $\alpha \in Z_n$ has a unique additive inverse
- Not all $\alpha \in Z_n$ have multiplicative inverse. If $\alpha = [a]$ and $\beta = [b]$, then β is a multiplicative inverse of α if and only if $ab \equiv 1 \pmod{n}$.

We define Z_n^* to be the set of elements of Z_n that have a multiplicative inverse.

$$Z_n^* = \{[a] : a = 0, \ldots, n - 1, \gcd(a, n) = 1\}.$$

If n is prime, then gcd $(a, n) = 1$ for $a = 1, \ldots, n - 1$, and $Z^*_n = Z_n \backslash \{[0]\}$.

Order of Z_n^* i.e., $|Z_n^*| = \varphi(n)$

Example: List the elements of Z_{15}^*

α	[1]	[2]	[4]	[7]	[8]	[11]	[13]	[14]
α^{-1}	[1]	[8]	[4]	[13]	[2]	[11]	[7]	[14]

Example: $Z_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$, $|Z_{26}^*| = 12$.

Order of an Element

Multiplicative order of an element: Let $a \in Z_n^*$ and gcd $(a, n) = 1$

(a is representative of residue class $\alpha = [a]$ with $a \in$ Z).

The order of a, denoted $\mathrm{ord}_n(a)$, is the least positive integer k such that

$a^k \equiv 1 \pmod{n}$.

Example: Let $n = 21$.

$Z_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

$\varphi(21) = \varphi(7)\varphi(3) = 12 = |Z_{21}^*|$.

The orders of elements in Z_{21}^* are

$a \in Z_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20
order of a	1	6	3	6	2	6	6	2	3	6	6	2

Finding multiplicative order

Theorem: Suppose $\alpha \in Z_n^*$ has multiplicative order k. Then for every $m \in \mathrm{Z}$, the multiplicative order of α^m is $k/\gcd(m, k)$.

Example: $Z_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

$\varphi(21) = \varphi(7)\,\varphi(3) = 12 = |\, Z_{21}^* \,|$.

The orders of elements in Z_{21}^* are

$a \in \mathrm{Z}_{21}{}^*$	1	2	4	5	8	10	11	13	16	17	19	20
order of a	1	6	3	6	2	6	6	2	3	6	6	2

order of 2 is 6, order of 8 = 2^3 will be 6/gcd(3, 6) = 6/3 = 2 which is true.

Primitive root modulo *n*

- Primitive root modulo n: Let n be a positive integer. $a \in Z$ with gcd $(a, n) = 1$ is a primitive root modulo n if the multiplicative order of a modulo n is equal to $\varphi(n)$.
- Example: Let $n = 7$; Primitive root modulo 7 are 3, 5

$k \rightarrow$	1	2	3	4	5	6
1^k mod 7	1	1	1	1	1	1
2^k mod 7	2	4	1	2	4	1
3^k mod 7	3	2	6	4	5	1
4^k mod 7	4	2	1	4	2	1
5^k mod 7	5	4	6	2	3	1
6^k mod 7	6	1	6	1	6	1

Primitive roots for the first few numbers

n	**Primitive roots modulo *n***
2	1
3	2
4	3
5	2, 3
6	5
7	3, 5
9	2, 5
10	3, 7
11	2, 6, 7, 8
12	2, 6, 7, 11

Fermat's little theorem: For any prime p, and any integer $a \neq 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Moreover, {or any integer a, $a^{p} \equiv a \pmod{p}$.

Euler's Theorem: For any positive integer n, and any integer a relatively prime to n,

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

In particular, the multiplicative order of a modulo n divides $\varphi(n)$.

Example: Find the remainder 29^{196} when divided by 13.

Sol: gcd (29, 13) = 1.

$196 = 12(16) + 4$

Hence $29^{196} \bmod 13 \equiv (29^{12})^{16} \cdot 29^{4} \bmod 13 \equiv (1)^{16} \cdot 29^{4} \bmod 13$

Using Euler's theorem $(29^{12}) \equiv 1 \bmod 13$

$\therefore 29^{196} \bmod 13 \equiv 29^{4} \pmod{13}$.

$\equiv (29 \bmod 13)^{4} \pmod{13}$

$\equiv (3)^{4} \pmod{13} \equiv 81 \pmod{13} \equiv 3 \pmod{13}$

Hence when 29^{196} is divided by 13, the remainder is 3.

Quadratic Residues

- Quadratic residues: An integer a is called a quadratic residue modulo n, or a square modulo n, if there exists an $x \in Z_n^*$ such that $x^2 \equiv a \bmod n$. If no such x exists, then a is called a quadratic nonresidue modulo n.

Example: Let $n = 21$, $Z_{21} = \{0, 1, 2, \ldots, 20\}$,

$Z_n^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

x	1	2	4	5	8	10	11	13	16	17	19	20
$x^2 \bmod 21$	1	4	16	4	1	16	16	1	4	16	4	1

Then $Q_{21} = \{1, 4, 16\}$ and $\bar{Q}_{21} = \{2, 5, 8, 10, 11, 13, 17, 19, 20\}$.

- Fact: Let p be an odd prime and let α be a primitive root (generator) of Z_p^*. Then $a \in Z_p^*$ is a quadratic residue modulo p iff $a = \alpha^i \bmod p$, where i is an even integer.

Therefore, $|Q_p| = (p-1)/2$ and $|\bar{Q}_p| = (p-1)/2$;

Example: $\alpha = 6$ is a generator of Z_{13}^*. The powers of α are:

i	1	2	3	4	5	6	7	8	9	10	11	12
$\alpha^i \bmod 13$	6	10	8	9	2	12	7	3	5	4	11	1

Hence $Q_{13} = \{1, 3, 4, 9, 10, 12\}$ and $\bar{Q}_{13} = \{2, 5, 6, 7, 8, 11\}$.

Theorem: Let p be a prime $a \in Z_p^*$ and gcd $(a, p) = 1$, then a is quadratic residue modulo p, iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Proof: Suppose a is quadratic residue modulo p i.e., $\exists\, x$ s.t. $x^2 \equiv a \bmod p$ & gcd $(a, p) = 1$.

$\Rightarrow p \nmid a$

$\therefore p \nmid x^2$ because $x^2 \equiv a \bmod p$

$\Rightarrow p \nmid x \Rightarrow \gcd(p, x) = 1$

Therefore, by Fermat's theorem

$$x^{p-1} \equiv 1 \pmod{p} \Rightarrow (x^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

or $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

Conversely: Suppose $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

Let g be a primitive root mod p, then $g^{\varphi(p)} \equiv 1 \bmod p$.

and $g^{k} \neq 1 \bmod p \;\; \forall\; 0 < k < \varphi(p)$

Also let $a = g^{r} \bmod p$, because g is primitive root modulo p

$$g^{r\cdot\left(\frac{p-1}{2}\right)} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

i.e., $g^{r\cdot\left(\frac{p-1}{2}\right)} \equiv 1 \pmod{p} \Rightarrow (p - 1) \mid r \cdot \left(\frac{p-1}{2}\right)$

because g is a primitive root mod p

$\Rightarrow \frac{r}{2}$ is an integer i.e. $r = 2s$

Let $x = g^{s}$, then $x^{2} = g^{2s} = g^{r} = a \pmod{p}$,

i.e. $x^{2} \equiv a \pmod{p}$. Hence a is quadratic modulo p.

Square root of a modulo n

- Definition: Let $a \in Q_n$. If $x \in Z_n^*$ satisfies $x^2 \equiv a \bmod n$, then x is called a square root of a modulo n.
- Fact: (number of square roots): If p is an odd prime and $a \in Q_p$, then a has exactly two square roots modulo p.
- More generally, let $n = {p_1}^{e_1} \cdot {p_2}^{e_2} \dots {p_k}^{e_k}$ where the p_i are distinct odd primes and $e_i \geq 1$. If $a \in Q_n$, then a has precisely 2^k distinct square roots modulo n.

Square root of *a* modulo *n*

Example 1: The square roots of 12 modulo 37 are 7 and 30.

Example 2: The square roots of 121 modulo 315 are 11, 74, 101, 151, 164, 214, 241, and 304.

$315 = 3^2 \times 5 \times 7$; there are 3 prime factors, therefore number of square roots modulo 315 are $2^3 = 8$

Finding Modular Square Roots

To find Square root of a modulo p

Case 1: when $p \equiv 3 \bmod 4$, p be an odd prime

$\therefore\ p = 4k + 3$ for some integer k.

For $a \in Z_p^*$, $a^{(p-1)/2} \equiv 1 \bmod p$

$\therefore\ a^{(p-1)/2+1} \equiv a \bmod p$

$\therefore\ a^{2k+2} \equiv a \bmod p$ or $(a^{k+1})^2 \equiv a \bmod p$

$\therefore\ a^{k+1}$ i.e. $a^{(p+1)/4}$ is square root of a

$\therefore$ Square root of a modulo p is $x = a^{(p+1)/4}$

Finding Modular Square Roots

Case 2: When $p \equiv 1 \bmod 4$

$\therefore\ p = 4r + 1$ for some integer r

Let $\frac{p-1}{2} = 2^l \cdot m$, where l and m are integers with $l \geq 1$ and m is odd.

For $a \in Z_p^*$, $\therefore a^{(p-1)/2} \equiv 1 \bmod p$

$\therefore a^{2^l \cdot m} \equiv 1 \bmod p$ ... (1)

$\therefore a^{2^{(l-1)} \cdot m} \bmod p$ is a square root of 1.

$\therefore a^{2^{(l-1)} \cdot m} \equiv \pm 1 \bmod p$

Finding Modular Square Roots

Case 2.1: If $a^{2^{(l-1)} \cdot m} \equiv 1 \bmod p$

If $l - 1 = 0$, then $a^m \equiv 1 \bmod p$

Multiply both side by a, then $a^{m+1} \equiv a \bmod p$

Therefore $a^{(m+1)/2} \bmod p$ is a square root of a modulo p

If $l - 1 \neq 0$, then $a^{2^{(l-2)} \cdot m} \equiv \pm 1 \bmod p$ continue as done in step 2

Case 2.2: If $a^{2^{(l-1)} \cdot m} \equiv -1 \bmod p$

Select a quadratic non-residue $b \in Z_p^*$, this is easy:

Since $b^{\frac{p-1}{2}} \equiv -1 \bmod p$

$\therefore b^{2^l \cdot m} \equiv -1 \bmod p$, and $a^{2^{(l-1)} \cdot m} \cdot b^{2^l \cdot m} = (-1)(-1) \equiv 1 \bmod p$

proceed as per Case 2.1

Example: Find square root of 4 modulo 17.

Sol: Here p = 17 and a = 4 i.e. $p \equiv 1 \bmod 4$

$p = 4\cdot4 + 1$, $r = 4$

$(p - 1)/2 = 2^3$

$4^{2^3} \equiv 1 \bmod 17$

$\therefore\ 4^{2^2} \equiv \pm 1 \bmod 17$

By calculation, $4^{2^2} = 1 \bmod 17$ and so no correction term is needed

Continuing, since 4^2 is a square root of 1, so it must be equal to $\pm 1 \bmod 17$.

Therefore $4^2 \equiv -1 \bmod 17$.

Therefore, choose a quadratic non-residue $b \in Z_p^*$, let it be 3 (= b)

Multiply both sides by $b^{2^l \cdot m}$ i.e., 3^{2^3}, i.e. $4^2 \cdot 3^{2^3} \equiv 1 \bmod 17$

Example: Find square root of 4 modulo 17 (cont.)

Finally, consider $4 \cdot 3^{2^2} \equiv 1 \bmod 17$.

Multiplying, both sides by 4 gives

$$4^2 \cdot 3^{2^2} \equiv 4 \bmod 17$$

Therefore, $4 \cdot 3^2 \equiv 2 \bmod 17$ is a square root of 4.

Another square root of 4 modulo 17 is

$$-4 \text{ modulo } 17 \equiv 13 \bmod 17$$

Square roots of 4 modulo 17 are 2 and 13 Ans.

Wilson's theorem

Wilson's theorem: p is prime iff $(p - 1)! \equiv -1 \pmod{p}$.

Take $p = 11$.

$$\begin{aligned} 10! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\ &= 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \\ &= 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) \\ &= -1 \end{aligned}$$

$(p - 1)! \equiv -1 \pmod{p}$ implies that p is prime.

Strong Prime and Safe Prime

- **Strong Prime**: A prime number p is said to be a strong prime if integers r, s, and t exist such that the following three conditions are satisfied:
  - p - 1 has a large prime factor, denoted r;
  - p + 1 has a large prime factor, denoted s; and
  - r - 1 has a large prime factor, denoted t.
- A strong prime is a prime number that is greater than the arithmetic mean of nearest prime numbers i.e., next and previous prime numbers.
- The first few strong primes are

  11, 17, 29, 37, 41, 59, 67, 71, 79, 97, 101
- **Safe Prime**: A safe prime p is a prime of the form $p = 2q + 1$ where q is prime. Prime q is called Sophie Germain prime.

  Examples (Safe prime): 5, 7, 11, 23, 47, 59, 83, 107