Lecture 1,2,3 - Introduction, Diophantine Equations, Divisibility, GCD

- Finding all integer solutions x , y such that for integers a, b, c, we have $ax + by = c$

1. Definitions

- **Divisibility**: a, b are integers. We say "a divides b" or "b is a multiple of a" if $b = ka$ for an integer k. We write $a|b$ in that case and $a \nmid b$ otherwise.
  - Let a be any natural number. Then, we have
    - $a \mid 0$
    - $a \mid a$
    - $a \mid -a$
    - $1 \mid a$
  - Similarly, we have
    - $a \mid b \wedge b \mid c \rightarrow a \mid c$
    - $a \mid b \wedge c \mid d \Leftrightarrow ac \mid bd$
    - Let $m \neq 0$. $a \mid b \Leftrightarrow ma \mid mb$
    - $x \mid a \wedge x \mid b \rightarrow x \mid ma + nb$
    - $a \mid b \wedge b \mid a \rightarrow a = \pm b$
    - $a \mid b \rightarrow |a| <= |b|$ unless $b = 0$
- **Division Algorithm**: Given $a, b \in Z$ with $a > 0$, $\exists q, r \in Z$ such that $b = aq + r$, $0 <= r < a$
  - We can partition the integers into several classes using Division Algorithms
    - even: $2k$, odd:$2k + 1$
    - $3k$, $3k + 1$, $3k + 2$
    - $4k$, $4k + 1$, $4k + 2$, $4k + 3$
    - $2k$, $4k + 1$, $4k + 3$
- **GCD and LCM**
  - c is a common divisor of a and b if $c \mid a$ and $c \mid b$.
  - d is a common multiple of a and b if $a \mid d$ and $b \mid d$.
  - $gcd(a, b) = (a, b)$
    - eg. $(10, 12) = 2$
  - $lcm(a, b) = [a, b]$
    - eg. $[10, 12] = 60$
    - $[a, b] = \frac{ab}{(a,b)}$
  - $(a, b, c) = ((a, b), c)$

- $(ma, mb) = m(a, b)$
- $(a, b) = 1 \to [a, b] = |a, b|$ if $a, b \neq 0$

2. Theorems on GCD

- There are integers x, y such that $ax + by = (a, b)$
- $a = kb + r$ then $(a, b) = (b, r)$
- $ax + by = c$ has solution if and only if $(a, b) \mid c$
- GCD is the smallest positive integer that can be written as ax+by.
- $c \mid a$ and $c \mid b \Leftrightarrow c \mid (a, b)$
- Common divisors are divisors of greatest common divisor
- We say a and b are relatiely prime if $(a, b) = 1$

Lecture 3,4,5,6 - Euclidean Algorithm, Primes

1. Step by Step - Solve Diophantine Equations

Back to the equation $ax + by = c$.

Step 1 - Find gcd(a,b)

- Use Euclid's algorithm, find x_0 and y_0 such that $ax_0 + by_0 = (a, b)$.

Step 2 - If divisible, then

- Check whether $gcd(a, b) \mid c$.
- If not divisible, then there is no solution to the dioiphantine equation. If divisible, proceed to step3.

Step 3 - Find general solution

- From step 1, we have $ax_0 + by_0 = (a, b)$.
- if $k(a, b) = c$, thus we have $k(ax_0 + by_0) = k(a, b) = c$
- Thus, one solution is $x = kx_0, y = ky_0$
- General solutions:
  - $x = x_0 + m \cdot \frac{b}{(a,b)}$
  - $y = y_0 - m \cdot \frac{a}{(a,b)}$

😃 Diophantine Equations Examples

Find all integers (x, y) such that

- $66x + 121y = 100$

- Sol: $(66,121) = 11 \nmid 100 \rightarrow$ no solution
- $14x + 8y = 6$
  - Use Euclidean algorithm to find GCD
    - $14 = 1 * 8 + 6$
    - $8 = 1 * 6 + 2$
    - $6 = 3 * 2 + 0$
    - Thus, gcd(14,8)=2
  - Thus, exist x and y such that 14x+8y=2
    - $2 = 8 - 1 \times 6 = 8 - 6 = 8 - (14 - 8) = 2 \times 8 - 14$
    - Thus, $14 * -1 + 8 * 2 = 2$
    - Thus, $3 * (14 * -1 + 8 * 2) = 6$
    - Thus, $(-3 * 14 + 6 * 8) = 6$
    - Thus, one solution is $x_0 = -3$, $y_0 = 6$
  - Thus, $x = -3 + m\frac{8}{2} = 4m - 3, y = 6 - m\frac{14}{2} = 6 - 7m$

2. Prime and Divisibility

- $p >= 2$ is called prime if 1 and p are its only positive divisors
- $n >= 2$ is called composite if it is not prime.
  - it has a divisor $a \mid n$ such that $1 < a < n$
  - $n = ab$ with $1 < a, b < n$
- p prime. n integer. Then, $(n, p) = 1$ or p.
- $p \mid ab \rightarrow p \mid a \vee p \mid b$

3. Fundamental Theorem of Arithmetic

- Every $n >= 2$ has a prime factorization $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ where p_i are distinct primes and a_i are positive integers. This factoriztion is unique up to re-ordering.
- Similarly, we have
  - $ab = p_1^{a_1+b_1} p_2^{a_2+b_2} ... p_k^{a_k+b_k}$
  - $\frac{a}{b} = p_1^{a_1-b_1} p_2^{a_2-b_2} ... p_k^{a_k-b_k}$
  - $a^m = p_1^{ma_1} p_2^{ma_2} ... p_k^{ma_k}$
  - $gcd(a,b) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} ... p_k^{min(a_k,b_k)}$
  - $lcm(a,b) = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} ... p_k^{max(a_k,b_k)}$
- if $a_1 <= b_1, a_2 <= b_2, ..., a_k <= b_k$, then a divide b.
- $gcd(a,b) * lcm(a,b)$
  $= p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} ... p_k^{min(a_k,b_k)} * p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} ... p_k^{max(a_k,b_k)}$
  $= p_1^{min(a_1,b_1)+max(a_1,b_1)} p_2^{min(a_2,b_2)+max(a_2,b_2)} ... p_k^{min(a_k,b_k)+max(a_k,b_k)}$
  $= p_1^{a_1+b_1} p_2^{a_2+b_2} ... p_k^{a_k+b_k}$

$= ab$

4. Rational Number

- **Definition**: If n is a rational number, then it can be written in the form of $\frac{a}{b}$ where a and b are integers.
- $\sqrt{2}$ is not a rational number
  - Proof:
    Assume $\sqrt{2}$ is a rational number.
    Then, $\sqrt{2} = \frac{a}{b}$.
    Thus, $a = \sqrt{2} \cdot b$.
    Thus, $a^2 = 2b^2$
    As per Fundamental Theorem of Arithmetic $a = 2^{a_1}...$ and $b = 2^{b_1}...$
    Then, we have $2^{2a_1} = 2^{2b_1+1}$
    Thus, $2a_1 = 2b_1 + 1$.
    Reach contradiction.
- Fully Divisibility
  - We say that p^e fully divides a (i.e. $p^e||a$) if $p^e|a$ and $p^{e+1} \nmid a$. That is, p^e is the highest power of p contained in a.
  - $(p^x||a) \wedge (p^y||b) \rightarrow (p^{x+y}||ab) \wedge (p^{x-y}||\frac{a}{b})$
  - $(p^x||a) \wedge (p^y||b) \wedge (x < y) \rightarrow p^x||a + b$

5. Square

- $(a, b) = 1$ and ab is a square $\rightarrow$ a and b are both square
- $n(n + 1)$ is never a square

6. Dirchlet's Theorem

There are infinitely many primes of the form $ak + b$ if and only if $(a, b) = 1$.

- Infinitely many primes ($4k + 3$)
  - Suppose $p_1 = 3, p_2 = 7, p_3, ...p_n$ are all the primes of the form 4k+3.
  - $m = 4p_1p_2p_3...p_n - 1$, which is of the form 4k+3
  - m has a prime divisor of the form 4k+3
  - Let $p_i \mid m$
  - Then, $p_i \mid 4p_1p_2..p_n \rightarrow p_i \mid 1$
  - Thus, reach contradiction.

7. Check Primeness

- If n is composite, then it must have a prime divisor $p <= \sqrt{n}$.
- **Divisibility by 2**
  $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_k \cdot 10^k$
  Thus, $2|n \leftrightarrow 2|a_0$
- **Divisibility by 4**
  Notice that $4/100{,}1000$,...
  Thus, $4|n \leftrightarrow 4|a_0 + 10a_1$
- **Divisibility by 5** : $5|a_0$
- **Divisibility by 3**
  $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_k \cdot 10^k = a_0 + a_1 + ... + a_k + 9a_1 + 99a_2 + ... + (10^k - 1)a_k$
  Thus, $3|n \leftrightarrow 2|a_0 + a_1 + a_2 + ... + a_k$
- **Divisibility by 11**
  $n = a_0 - a_1 + a_2 - ... + (-1)^k a_k + (11a_1) + (10^2 - 1)a_2 + ... + (10^k - (-1)^k)a_k$
  Thus, $11|n \leftrightarrow 11|a_0 - a_1 + a_2 - ... + (-1)^k a_k$

8. Factoring

- $x^a - 1 = (x-1)(x^{a-1} + x^{a-2} + x^{a-3} + ... + x + 1)$
- $x^{2a+1} + 1 = (x+1)(x^{2a} - x^{2a-1} + x^{2a-2} - ... - x + 1)$

9. Consider $p = 2^m + 1$

- m **is not odd**
  $p = 2^m + 1 = (2+1)(x^{m-1} - x^{m-2} + ... - x + 1) \rightarrow$ p is divisible by 3 $\rightarrow$ p is not prime.
- m **is not divisible by any odd number except 1**
  - Assume m can be divided by a odd number $2a+1$.
  - Then, we have $m = (2a+1)k$
  - This means that $2^m + 1 = 2^{(2a+1)k} + 1 = 2^{k(2a+1)} = (2^k + 1)(2^{2ak}...)$
- if $2^m + 1$ is prime, then $m = 2^n$ for some n.

9. Consider $p = 2^m - 1$

- m must be a prime, otherwise $m = ab$ with $1 < a, b < m$ and $2^m - 1 = 2^{ab} - 1$ is divisible by $2^b - 1$, cannot be prime.

Lecture 6,7 - Modular Arithmetic

Definitions

- Fermat Numbers: $F_n = 2^{2^n} + 1$
- Mersenne Numbers: $M_p = 2^p - 1$

Congruence Class

Integers are partitioned into n sets (congruence classes)

- $\mathbf{Z_n} = \{[0]_n, [1]_n, ..., [n-1]_n\}$
- $[a]_n = [b]_n \leftrightarrow n \mid a - b$. (i.e. $a \equiv b \pmod{n}$)
- $[a]_n + [b]_n = [a+b]_n$
- $[a]_n \cdot [b]_n = [ab]_n$

Theorems

- If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then
  - $a + b \equiv c + d \pmod{n}$
  - $ab \equiv cd \pmod{n}$
  - $a^k \equiv c^k \pmod{n}$ where $k \in N$
- Also, we have
  - $x \equiv x \pmod{n}$
  - $x \equiv y \pmod{n} \to y \equiv x \pmod{n}$
  - $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n} \to x \equiv z \pmod{n}$
  - $a \equiv 0 \pmod{n}$ means a is divisible by n
- Let $p(x)$ be a polynomial with integer coefficients, then $a \equiv b \pmod{n} \to p(a) \equiv p(b) \pmod{n}$
- Suppose $d \geqslant 1$ and $d \mid m$, then $a \equiv b \pmod{m} \to a \equiv b \pmod{d}$
- Suppose $c > 0$, then $a \equiv b \pmod{m} \to ac \equiv bc \pmod{mc}$
- $ax \equiv ay \pmod{m} \to x \equiv y \pmod{\frac{m}{(m,a)}}$

Step by Step - Solve $ax \equiv b \pmod{m}$

- Step 1
  Check whether $gcd(a, m)$ divides b. If not, then there is no solution. Elsewise, proceed to step 2.
- Step 2
- Find x_0 and then $x = x_0 + t\frac{m}{(a,m)}$.
- We can find x_0 using Euclid's algorithm
  - $ax \equiv b \ (\text{mod m}) \to ax \equiv mk + b \ (\text{mod m}) \to ax - mk = b$
- That is, the set of all solutions : $\{x \in Z : x \equiv x_0(\text{mod}\frac{m}{(a,m)})\}$

Examples

- **Find remainder of $113 \cdot 114$ after dividing by 120**

$113 \equiv 7 \pmod{120}$
$114 \equiv 6 \pmod{120}$
$\rightarrow 113 \cdot 114 \equiv 7 \cdot 6 \equiv 42 \pmod{120}$

- **Find remainder of 5^{16} after dividing by 17**

  $5^2 = 25 \equiv 8 \pmod{17}$
  $5^4 \equiv 8^2 \equiv 64 \equiv -4 \pmod{17}$
  $5^8 \equiv (-4)^2 \equiv 16 \equiv -1 (\bmod 17)$
  $5^{16} \equiv (-1)^2 \equiv 1 \pmod{17}$

- **Prove that n^3 is of the form $7k$ or $7k+1$ or $7k+6$**
  - That is, we want to show that $n^3 \equiv 0, 1, 6 \pmod{7}$
  - n can be either of form $7a, 7a+1, 7a+2, 7a+3, 7a+4, 7a+5, 7a+6$
    - $(7a)^3 \equiv 0^3 \equiv 0 \pmod{7}$
    - $(7a+1)^3 \equiv 1^3 \equiv 1 \pmod{7}$
    - $(7a+2)^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod{7}$
    - $(7a+3)^3 \equiv 3^3 \equiv 27 \equiv 6 \pmod{7}$
    - $(7a+4)^3 \equiv 4^3 \equiv (2^3)^2 \equiv 1 \pmod{7}$
    - $(7a+5)^3 \equiv 5^3 \equiv (-2)^3 \equiv -8 \equiv 6 \pmod{7}$
    - $(7a+6)^3 \equiv 6^3 \equiv (-1)^3 \equiv 6 \pmod{7}$
- **Prove that $n \cdot (n+1) \cdot (n+2)$ is divisible by 6**
  - n can be either of form $6a, 6a+1, 6a+2, 6a+3, 6a+4, 6a+5$
  - Let $N = n \cdot (n+1) \cdot (n+2)$
  - Then, consider the six cases
    - $N \equiv_6 0 * 1 * 2 \equiv_6 0$
    - $N \equiv_6 1 * 2 * 3 \equiv_6 6 \equiv_6 0$
    - $N \equiv_6 2 * 3 * 4 \equiv_6 0$
    - $N \equiv_6 3 * 4 * 5 \equiv_6 0$
    - $N \equiv_6 4 * 5 * 6 \equiv_6 0$
    - $N \equiv_6 5 * 6 * 7 \equiv_6 0$
  - Thus N is divisible by 6 is proved
- **Prove that $x^3 - x + 1 = 42$ has no integer solution**
  - $p(x) = x^3 - x + 1$ and $p(x) \equiv 42 \equiv 0 \pmod{3}$
  - $x \equiv 0, 1, 2 \pmod{3}$
  - Thus, $p(x) \equiv p(0) \vee p(1) \vee p(2)$
    - $p(1) = 1^3 - 1 + 1 = 1 \equiv 1 \pmod{3}$

- $p(2) = 2^3 - 2 + 1 = 7 \equiv 1$ (mod 3)
- $p(3) = 3^3 - 3 + 1 = 25 \equiv 1$ (mod 3)
- Thus, no such integer solution.

- **Which integers x satisfy $15x \equiv 30$ (mod 40)?**
  - $gcd(15, 40) = 5$
  - Thus, $x \equiv 2 (\text{mod } \frac{40}{5})$ i.e. $x \equiv 2 (\text{mod } 8)$
  - Thus, we have $x - 2 = 8t$
  - That is, $x = 8t + 2$ where $t \in Z$
- **Solve $3x \equiv 7$ (mod 11)**
  - $gcd(11, 3) = 1 \rightarrow$ there exists solution
  - $11 = 3 * 3 + 2$, $3 = 2 * 1 + 1$, $2 = 1 * 2 + 0$
  - $1 = 3 - 2 = 3 - 11 + 3 * 3 = 3 * 4 + 11 * 1$
  - Thus, solve the original linear congruence by multiplying 4. That is, we need to solve $12x \equiv 28 \equiv 6$ (mod 11)
  - $2x \equiv 1$ (mod 11) as $gcd(2, 11) = 1$
    - Notice that $1 = 2 * 6 - 1$
    - Thus, $2 * 6 \equiv 1$ (mod 11)
  - Thus, $x_0 = 6$ is one of the solutions. As a result, we have the general solution : $x \equiv 6$ (mod 11) as $gcd = 1$
- **Solve $9x \equiv 6$ (mod 12)**
  - gcd(9,12)=3 which divides 6.
  - Thus, we have $3x \equiv 2$ (mod 4)
  - thus $x_0 = 2$ and $x = 2 + 4t$
  - i.e. $x \equiv_4 2$
- **Solve $66x \equiv 100$ (mod 121)**
  - $gcd(121, 66) = 11$ which does not divide 100
  - Thus, no solution
- **Solve $14x \equiv 1$ (mod 45)**
  - gcd(14,45)=1
  - Euclidean algorithm
    - 45 = 3*14 + 3
    - 14 = 4*3 + 2
    - 3 = 1*2+1
  - $1 = 3 - 2 = 45 - 4 * 14 + 4 * (45 - 3 * 14) = 5 * 45 - 16 * 14$
  - $x \equiv_{45} -16$
- **Solve $30x \equiv 56$ (mod 71)**
  - Eucledian algo
    - gcd(30,71)=1

- $71 = 2 \cdot 30 + 11$
- $30 = 2 \cdot 11 + 8$
- $11 = 1 \cdot 8 + 3$
- $8 = 2 \cdot 3 + 2$
- $3 = 1 \cdot 2 + 1$
- $2 = 2 \cdot 1 + 0$

- Thus,
  - $1 = 3 - 1 \cdot 2$
    $= 3 - 8 + 2 \cdot 3$
    $= 3 \cdot 3 - 8$
    $= 3 \cdot (11 - 8) - (30 - 2 \cdot 11)$
    $= 5 \cdot 11 - 3 \cdot 8 - 30$
    $= 5 \cdot 11 - 3 \cdot 8 - (2 \cdot 11 + 8)$
    $= 3 \cdot 11 - 4 \cdot 8$
    $= 3 \cdot (71 - 2 \cdot 30) - 4 \cdot (30 - 2 \cdot 11)$
    $= 3 \cdot 71 - 10 \cdot 30 + 8 \cdot 11$
    $= 3 \cdot 71 - 10 \cdot 30 + 8 \cdot (71 - 2 \cdot 30)$
    $= 11 \cdot 71 - 26 \cdot 30$
- Thus, we have $-26 \cdot 30x \equiv_{71} 56 \cdot -26$
- That is, $x \equiv_{71} 56 \cdot -26 \equiv_{71} 35$

Lecture 8,9 - Chinese Remainder Theorem

1.Theorem

$x \equiv_{m_1} a, x \equiv_{m_2} a, ..., x \equiv_{m_k} a$ is equivalent to $x \equiv_m a$ where $m = lcm[m_1, m_2, ..., m_k]$

- for example, to prove that x is divisible by 120, we can show that x is divisible by all of $8, 3$ and 5

2.Chinese Remainder Theorem (pairwise coprime moduli)

$x \equiv a_1$ (mod m_1), $x \equiv a_2$ (mod m_2),...,$x \equiv a_k$ (mod m_k) with $(m_i, m_j) = 1$ for all $i \neq j$ has a unique solution $x \equiv a$ (mod $m_1 m_2 .. m_k$) in $Z_{m_1 m_2 .. m_k}$ for some a.

3.Simultaneous non-linear congruences

- Example: Consider the simultaneous congruences $x^2 \equiv 1$ (mod 3) and $x \equiv 2$ (mod 4).
  - $x^2 \equiv 1$ (mod 3) is equivalent to $x \equiv 1$ (mod 3) AND $x \equiv 2$ (mod 3)
  - Then, we need to consider the following two cases:
    - $x \equiv 2$ (mod 4) AND $x \equiv 1$ (mod 3)

        - Then, solve this by CRT.
        - $x = 4k + 2 \equiv 1$ (mod 3) $\rightarrow 4k \equiv 2$ (mod 3)
        - Then, we have $2k \equiv 1$ (mod3)
        - Then, $k = 2 + 3t \rightarrow x = 10 + 12t$
        - Thus, $x \equiv_{12} 10 \equiv_{12} -2$
      - $x \equiv 2$ (mod 4) AND $x \equiv 2$ (mod 3)
        - Then, solve this by CRT.
        - Similarly, $x = 4k + 2 \equiv 2$ (mod 3) $\rightarrow 4k \equiv 0$ (mod 3)
        - Then, we have $k \equiv 0$ (mod3)
        - Then, $k = 3t \rightarrow x = 12t + 2$
        - Thus, $x \equiv_{12} 2$
    - Thus, the general solution should be $x \equiv \pm 2$ (mod 12)
- **Number of solutions to $x^2 \equiv 1$ (mod n) in Z_n**
    - if $n \equiv 0$ (mod 8), then $N = 2^{k+1}$ where k is the number of primes in prime factorization of n.
    - if $n \equiv 2$ (mod 4), then $N = 2^{k-1}$ where k is the number of primes in prime factorization of n.
    - elsewise, $N = 2^k$

Examples

- **Which integers x satisfy both $x \equiv 1 \pmod 5$ and $x \equiv 5 \pmod 7$**
    - $x \equiv 1 \pmod 5 \rightarrow x \equiv_{35} 1, 6, 11, 16, 21, 26$,...
    - $x \equiv 5 \pmod 7 \rightarrow x \equiv_{35} 5, 12, 19, 26...$
- **Solve $x \equiv_{15} 2$ and $x \equiv_7 3$**
    - $x = 7k + 3 \equiv_{15} 2$
    - $7k \equiv_{15} -1 \equiv_{15} 14$
    - Thus, $k \equiv_{15} 2$ as $gcd(7, 15) = 1$
    - Thus, $k = 15l + 2$
    - Thus, $x \equiv_{15} 7k + 3 \equiv_{15} 7(15l + 2) + 3 \equiv_{15} 105l + 17$
    - Thus, we get $x \equiv_{105} 17$
- Check the isolated pdf on exercises on Chinese Remainder Theorem

Lecture 10 - Congruence Class, lagrange, Fermat Theorem

1. Linear Congruences : $ax \equiv b$ (mod p)

- If $(p, a) = p$ i.e $p \mid a$, then we have -- solution x exists $\leftrightarrow b \equiv 0$ (mod p)

- If $(p,a)=1$, then there exist a unique solution x in $Z_{\frac{p}{(p,a)}}$=Z_p
  - In particular, a^{-1} always exist (mod p) unless $a \equiv 0$ (mod p)

2. Lagrange Theorem

$f(x) = a_d x^d + a_{d-1}x^{d-1} + ... + a_1 x + a_0$ is a polynomial with integer coefficients such that $a_i \neq 0$ for at least one i. Then, $f(x) \equiv 0$ (mod p) has at most d solutions in Z_p

3. Lemma based on Lagrange

- If $f(x) = a_d x^d + a_{d-1}x^{d-1} + ... + a_1 x + a_0 \equiv_p 0$ has more than d roots, then $a_i \equiv 0$ (mod p) for all i.

4. Fermat Theorem

For $a \not\equiv 0$ (mod p), then $a^{p-1} \equiv 1$ (mod p)

Examples

- **Compute 2^{1003} (mod 11)**
  - By Fermat's Theorem, since 11 is prime, thus, $2^{10} \equiv 1$. Thus, $2^{1000} \cdot 8 \equiv 1 \cdot 8 \equiv 8$ (mod 11)
- **Prove that $n^{25} - n$ is divisible by 30 for all n**
  - show $n^{25} - n$ is divisible by 2
    - By Fermat's theorem, $n \equiv 1$ (mod 2)
    - Thus, $n^{25} - n \equiv 1 - 1 \equiv 0$ (mod 2)
  - show $n^{25} - n$ is divisible by 3
    - By Fermat's theorem, $n \equiv 2$ (mod 3)
    - Thus, $n^5 \equiv 2^5 \equiv 2$ (mod 3)
    - Thus, $n^{25} \equiv 2^5 \equiv 2$ (mod 3)
    - Thus, $n^{25} - n \equiv 2 - 2 \equiv 0$ (mod 3)
  - show $n^{25} - n$ is divisible by 5
    - By Fermat's theorem, $n \equiv 2^4 \equiv 1$ (mod 5)
    - Thus, $n^{25} - n \equiv 1 - 1 \equiv 0$ (mod 5)
- **Solve $x^{17} + 6x^{14} + 2x^5 + 1 \equiv_5 0$**
  - By Fermat's Theorem, $x^4 \equiv_5 1$
  - Thus, equivalent to $x + 6x^2 + 2x + 1 \equiv_5 0$
  - That is, $6x^2 + 3x + 1 \equiv_5 0$
  - Thus, $x^2 - 2x + 1 \equiv_5 0$
  - Thus, $(x-1)^2 \equiv_5 0$
  - Thus, $x \equiv 1$ (mod 5)

Lecture 11,12,13,14 - Wilson Theorem, Base a Test

1. Wilson Theorem

- $n \geq 2$ is a prime if and only if $(n-1)! \equiv -1$ (mod n)
- p odd prime. $x^2 + 1 \equiv 0$ (mod p) has a solution if and only if $p \equiv 1$ (mod 4)

2. Check Prime or Not

- Use Wilson Theorem (hard to compute)
  - $(n-1)! \not\equiv 1$ (mod n) $\rightarrow$ ¬prime(n)]
- Use Fermat's theorem
  - if not $a^p \equiv a$ (mod p), then p is not prime
  - We call this the "base a test"
  - Composite numbers that can pass the "base 2 test" are all pseudoprimes
    - 341=11*31 is a pseudoprime
      - Notice that $2^{10} \equiv 1$ (mod 11) and $2^{30} \equiv 1$ (mod 31)
      - Thus, $2^{341} \equiv 2^{11 \cdot 31} \equiv 2^{31} \equiv 2$ (mod 31)
    - There are infinitely many pseudoprimes as for any pseudoprime n, $2^n - 1$ is also a pseudoprime. (Textbook Theorem 4.7)

3. Carmichael Numbers

- Numbers that pass base a test for all a are called Carmichael numbers.
  - Example: 561 is a Carmichael number
    - WTS: $a^{561} \equiv a$ (mod 561)
    - $561 = 3 \cdot 11 \cdot 17$
    - By Fermat's Theorem, $a^2 \equiv 1$ (mod 3), $a^{10} \equiv 1$ (mod 11), $a^{16} \equiv 1$ (mod 17)
    - Thus,
      - $a^{561} \equiv (a^2)^{280} \cdot a \equiv a$ (mod 3)
      - $a^{561} \equiv (a^{10})^{51} + a \equiv a$ (mod 11)
      - $a^{561} \equiv (a^{16})^{35} + a \equiv a$ (mod 17)
    - Thus, by CRT, $a^{561} \equiv a$ (mod $3 * 11 * 17 = 561$)
- Suppose $n = p_1 p_2 ... p_k$ is a product of distinct primes such that $p_i - 1 \mid n - 1$ for $i = 1, 2, ..., k$, then n is a Carmichael number

4. Congruences modulo p^k

We now focus on $f(x) \equiv 0$ (mod p^k).
We can solve $f(x) \equiv 0$ (mod p), using the solution we will find we can next solve $f(x) \equiv 0$ (mod p^2) and then $f(x) \equiv 0$ (mod p^3), ..., until mod p^k

- **Example :** $x^3 - x^2 - x + 4 \equiv 0$ **(mod** 27**)**
  $27 = 3^3$
  - *STEP 1: Solve* $x^3 - x^2 - x + 4 \equiv 0$ *(mod* 3*)*
    - $x \equiv 1, 2$ (mod 3)
    - Thus, x = 3k+1 or x=3k+2
  - *STEP 2: Plug in x raise to second power*
    - Case #1: x = 3k+1
      - $(3k+1)^3 - (3k+1)^2 - (3k+1) + 4 \equiv 0$ (mod 9)
      - 3 \equiv 0 (mod 9)
      - Thus, no solution
    - Case #2: x = 3k+2
      - $(3k+2)^3 - (3k+2)^2 - (3k+2) + 4 \equiv 0$ (mod 9)
      - $-15k + 6 \equiv 0$ (mod 9)
      - $-5k + 2 \equiv 0$ (mod 3)
      - $k + 2 \equiv 0$ (mod 3)
      - $k \equiv -2$ (mod 3)
      - $k \equiv 1$ (mod 3)
      - Thus, $k = 3l + 1$
      - Thus, $x = 3(3l+1) + 2 = 9l + 5$
  - *STEP 3: Plug in x raise to third power*
    - $(9l+5)^3 - (9l+5)^2 - (9l+5) + 4 \equiv 0$ (mod 27)
    - $-99l + 99 \equiv 0$ (mod 27)
    - $-11l + 11 \equiv 0$ (mod 3)
    - $l + 2 \equiv 0$ (mod 3)
    - $l \equiv -2 \equiv 1$ (mod 3)
    - $x = 9l + 5 = 9(3m+1) + 5 = 27m + 14$
    - Thus, $x \equiv 14$ (mod 27)

5. Hensel's Lemma

If $f(a) \equiv 0$ (mod p^j) and $f'(a) \equiv 0$ (mod p).

- Case 1: $\frac{f(a)}{p^j} \not\equiv 0$ (mod p) $\rightarrow a$ cannot be lifted to mod p^{j+1}
- Case 2: $\frac{f(a)}{p^j} \equiv 0$ (mod p) $\rightarrow f(a + tp^j) \equiv 0$ (mod p) for all $t = 0, 1, ..., p-1$, i.e. a can be lifted to p solutions in mod p^{j+1}.
- When $f'(a) \equiv 0$ (mod p), either every lift is a solution or none of them is a solution.

If $f(a) \equiv 0$ (mod p^j) and $f'(a) \not\equiv 0$ (mod p), then there is a unique $0 \leq t \leq p-1$ such that $f(a + tp^j) \equiv 0$ (mod p^{j+1})

Examples

- $x^3 - x^2 + 4x + 1 \equiv 0$ **(mod 125)**
  - 125 = 5^3
  - Thus, lets try to solve $x^3 - x^2 + 4x + 1 \equiv 0$ (mod 5).
  - Plug in 1 to 5, we get that x=1 or 4.
  - Case 1: x=1
    - $f'(x) = 3x^2 - 2x + 4$
    - $f'(1) = 3 - 2 + 4 = 5 \equiv 0$ (mod 5)
    - $\frac{f(1)}{5} = 1 \not\equiv 0$ (mod 5)
    - Thus, no solution
  - Case 2: x=4
    - $f'(4) = 44 \equiv 4 \not\equiv 0$ (mod 5).
    - Thus, unique solution.
- $f(x) = x^2 + x + 7$ **;** $f(x) \equiv 0$ **(mod 27)**
  - $27 = 3 * 3 * 3$. Thus, try to solve $f(x) \equiv 0$ (mod 3)
    - $f(0) = 7 \equiv 1$ (mod 3)
    - $f(1) = 2 + 7 = 9 \equiv 0$ (mod 3)
    - $f(2) = 4 + 2 + 7 = 13 \equiv 1$ (mod 3)
  - $f'(x) = 2x + 1$ and $f'(1) = 2 + 1 = 3 \equiv 0$ (mod 3)
  - Thus, in this case, $a = 1, p = 3$ and $f(a) \equiv 0$ (mod p^1) and $f'(a) \equiv 0$ (mod p). Thus, by Hensel's Lemma, it can be lifted to mod p^2, i.e. $3^2 = 9$. Either every lift is a solution or none of them is a solution.
  - Since $f(1) \equiv 9 \equiv 0$ (mod 9), we know that 1 is a solution. Thus, 1,4,7 are all solutions mod 9.
    - $f(1) = 9 \not\equiv 0$ (mod 27) $\rightarrow 1, 10, 19$ are not solutions in mod 27
    - $f(4) = 27 \equiv 0$ (mod 27) $\rightarrow 4, 4 + 9 = 13, 4 + 2 * 9 = 22$ are solutions in mod 27
    - $f(7) = 63 \not\equiv 0$ (mod 27) $\rightarrow 7, 16, 25$ are not solutions in mod 27
  - Thus, $x \equiv 4, 13, 22$ (mod 27)
- $f(x) = x^3 + 4x^2 + 19x + 1$; $f(x) \equiv 0$ (mod 25)
  - $25 = 5^2$
  - Try to solve $f(x) \equiv 0$ (mod 5)
    - $f(0) = 1 \not\equiv_5 0$
    - $f(1) = 25 \equiv_5 0$
    - $f(2) = 63 \equiv_5 3 \not\equiv_5 0$
    - $f(3) = 121 \equiv_5 1 \not\equiv_5 0$
    - $f(4) = 205 \equiv_5 0$
    - Thus, $x \equiv 1, 4$ (mod 5)

- $f'(x) = 3x^2 + 8x + 19$
  - $f'(1) = 30 \equiv 0$ (mod 5)
  - $f'(4) = 99 \equiv 4$ (mod 5)
- Thus, when x=4, there is a unique solution.
- Otherwise, when x=1, $\frac{f(1)}{5} = 5$. This means that it can be lifted to mod 25. Either every lift is a solution or none of them is a solution.
- $f(1) = 25 \equiv 0$ (mod 25) $\rightarrow 1, 6, 11, 16, 21$ are solutions in mod 25
- Thus, there are a total of 6 solutions in mod 25.

6. Unit Modulo n

We will say u is a unit modulo n if it has an inverse (or equivalently $(u, n) = 1$).

- Units of Z_8: $1, 3, 5, 7$
- Units of Z_9: $1, 2, 4, 5, 6, 7, 8$
- Units of Z_{10}: $1, 3, 7, 9$
- Units of Z_p: $1, 2, ..., p-1$

Let u and v be units in Z_n. Then u^{-1}, v^{-1}, $-u$, $-v$, uv are also units in Z_n.

Lecture 15,16,17,18,19 - Euler's Function

$$\phi(n) = \text{number of units in } Z_n = |\{u : 1 \leq u \leq n-1 \wedge (u, n) = 1\}|$$

- $\phi(8) = |\{1, 3, 5, 7\}| = 4$
- $\phi(9) = |\{1, 2, 4, 5, 7, 8\}| = 6$
- $\phi(10) = |\{1, 3, 7, 9\}| = 4$
- $\phi(p) = p - 1$

1. Euler's Theorem

Suppose (a,n)=1, then we have $a^{\phi(n)} \equiv 1$ (mod n)

- Example: $n = 12$
  - $(a, 12) = 1 \rightarrow (a, 3) = 1$ and $(a, 4) = 1$
  - $(a, 3) = 1$ means that a mod 3 can be either 1 or 2
    - thus, a mod 3 = 1 or 2
    - That is,
      - $a \equiv 1$ (mod 3)
      - $a \equiv 2$ (mod 3)
  - $(a, 4) = 1$ means that a mod 4 can be either 1 or 3

- thus, a mod 4 = 1 or 3
- That is,
  - $a \equiv 1$ (mod 4)
  - $a \equiv 3$ (mod 4)

- Thus, by CRT, we know there are four possibility of solutions
  - $a \equiv 1$ (mod 12)
  - $a \equiv 5$ (mod 12)
  - $a \equiv 7$ (mod 12)
  - $a \equiv 11$ (mod 12)
- Thus, $\phi(12) = \phi(4)\phi(3) = 4$

2. Theorems

Let p be a prime number. Let $k \geq 1$.

- For $(m, n) = 1$, we have $\phi(mn) = \phi(m) \cdot \phi(n)$
- $\phi(1) = 1$
- $\phi(p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})...\phi(p_k^{\alpha_k})$
- $\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$
- $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} \rightarrow \phi(n) = n \cdot \prod_{i=1}^{k}(1 - \frac{1}{p_i})$
- $\phi(p^2) = p(p-1)$

Examples

- $\phi(42) = \phi(2 \cdot 3 \cdot 7) = \phi(2)\phi(3)\phi(7) = 1 \cdot 2 \cdot 6 = 12$
- $\phi(48) = \phi(2^4 \cdot 3) = 48 \cdot \frac{1}{2} \cdot \frac{2}{3} = 16$
- $\phi(60) = \phi(2^2 \cdot 3 \cdot 5) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$
- Lst two digits of 3^{2001}
  - That is, we want to find 3^{2001} mod 100
  - $\phi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$
  - By Euler's Theorem, we have $a^{40} \equiv 1$ (mod 100) as long as (a,100)=1 for any a.
  - Since (3,40)=1, we have $(3^{40})^{50} \cdot 3 \equiv 3$ (mod 100)
  - Thus, the last two digits are 03
- Show that $a^{12} \equiv 1$ (mod 42) for (a,42)=1
  - $\phi(42) = 42 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 12$
  - Thus, by Euler's Theorem, we have shown the asked relation.

3. Structure of the units of Z_n

- units of Z_3: $\{1, 2\} \equiv \{2, 2^2\}$ (mod 3)
- units of Z_5: $\{1, 2, 3, 4\} \equiv \{2, 2^2, 2^3, 2^4\}$ (mod 5)

Let p be any prime. There exists an integer such that $\{1, 2, ..., p-1\} \equiv \{g, g^2, g^3, ..., g^{p-1}\}$ in Z_p . g satisfying this condition will be called a primitive root.

Theorem

A unit u is a primitive root mod p if and only if the smallest positive integer k satisfying $u^k \equiv 1$ (mod p) is $k = p-1$

Definition

Let u be a unit in Z_n. We call the smallest positive integer k satisfying $u^k \equiv 1$(mod n) the order of u modulo n, denoted by $ord_n(u)$

- A primitive root modulo p is a unit of order p-1

Theorem

- g is a primitive root modulo p and $k \geq 0$ is an integer. Then, $g^k \equiv 1$ (mod p) $\leftrightarrow p-1 \mid k$
- Take a unit modulo p, it can be written g^a in Z_p for some $1 \leq a \leq p-1$. Then, $ord_p(g^a) = \frac{p-1}{gcd(p-1,a)}$
- Order of a unit modulo p always divides p-1
- Let d be a positive divisor of p-1 then there are exactly $\phi(d)$ units modulo p of order d
- There are $\phi(p-1)$ primitive roots modulo p
- $\sum_{d|p-1} \phi(d) = p-1$
- $k \geq 0$ and $u^k \equiv 1$ (mod n) $\leftrightarrow ord_n(u) \mid k$. In particular, $ord_n(u) \mid \phi(n)$
- $ord_n(u^a) = \frac{ord_n(u)}{(ord_n(u),a)}$
- $\sum_{m|n} \phi(m) = n$

4. Primitive Roots Modulo n

WE say g is a primitive root modulo n if it generates all units of Z_n, i.e. $\{1 \leq u \leq n : (u,n) = 1\} = \{g, g^2, g^3, ..., g^{\phi(n)}\}$ (mod n)

- g is a primitive root modulo n if and only if $ord_n(g) = \phi(n)$
- If g is a primitive root modulo n, then $g^k \equiv 1$ (mod n) $\leftrightarrow \phi(n) \mid k$
- $ord_n(g^a) = \frac{\phi(n)}{gcd(\phi(n),a)}$
- Suppose Z_n has a primitive root and d is a positive divisor of $\phi(n)$. Then, there are exactly $\phi(d)$ units of order d. In particular, there will be $\phi(\phi(n))$ primitive roots in Z_n
- Which Z_n has primitive roots?
    - exactly when $n = 1, 2, 4$ or $n = p^m$where p is a odd prime, or $n = 2 \cdot p^m$
    - Otherwise, no primitive roots

- Let n be odd. If g is a primitive root modulo n and g is odd, then g is also a primitive root modulo 2n.
- If $n = ab$ with $(a, b) = 1$, and $a, b > 2$, then Z_n has no primitive root.
- Let u be an odd integer and $e \geq 3$, then $u^{2^{e-2}} \equiv 1$ (mod 2^e)
    - Hence, $ord_{2^e} \leq 2^{3-2} \leq 2^{e-1} \leq \phi(2^e)$
- $ord_{2^n}(5) \equiv 2^{n-2}$
- Units of Z_{2^n} can be generated by two units: 5 and -1.
    - In other words, units of Z_{2^n} = $\{\pm 5^k : 1 \leq k \leq 2^{n-2}\}$

Lecture 20 - Cryptography

1. Caesar's Cipher

$A \rightarrow B, B \rightarrow C, C \rightarrow D$, ..., $Y \rightarrow Z, Z \rightarrow A$

2. Modular Exponentian Ciper

Two parties A and B want to exchange messages. Say x is the message that A wants to send B.

1. Choose prime number p, which is a public information that everyone knows.
2. They agree on a secret key e such that $(e, p-1) = 1$ before starting to exchange messages. e is known by A and B only
3. A will compute $m \equiv x^e$ (mod p) and send the encoded message m to B
4. To decode the received message, B first finds the inverse of e modulo $p-1$, which is equivalent to x (mod p) by Fermat's Theorem.
    - $m^f \equiv (x^e)^f \equiv x^{ef} \equiv x^{k \cdot (p-1)+1} \equiv x^{k(p-1)} \cdot x \equiv x$ (mod p)

3. Diffie-Hellman Key Exchange

A and B want to agree on a key securely to use later.

1. They pick a large prime p and an integer $1 \leq g \leq p$. p and g are public information, everyone knows.
2. A chooses a secret integer a and B chooses a secret integer b.
    - a is only known by A
    - b is only known by B
3. A computers $a' \equiv g^a$ (mod p) and sends it to B. B computes $b' \equiv g^b$ (mod p) and sends it to A.
    - a' and b' are public information, everyone knows.
4. A and B compute $(a')^b \equiv (b')^a$ (mod p) using their secret integers, this will be their key

4. RSA Public Key

1. Pick two very large distinct primes p and q and an encryption key e such that (e, (p-1)(q-1))=1.
   - pq and e are public information
   - The pair (pq,e) is called the public key.
2. Say someone wants to send us the message x securely. They will compute $m \equiv x^e$ (mod pq) and send the encoded message m to us.
3. To decode the received message, we first find the inverse of e modulo $(p-1)(q-1)$, which is equivalent to x (mod pq) by Euler's theorem.
   - f is the private key, where $fe \equiv 1$ (mod $(p+1)(p-1)$)
   - Thus, $ef = k(p+1)(p-1)+1$
   - $m^f \equiv x^{ef} \equiv x^{k(p+1)(p-1)+1} \equiv x^{\phi(pq)} \cdot x \equiv x$ (mod pq)

Examples

- Modular Exponentian Ciper
  - Encode $x = 7$ using $e = 26$ and $p = 101$
    $x^e \equiv m$ (mod p) $\rightarrow 7^{26} \equiv (7^4)^6 \cdot 7^2$
    $7^4 \equiv 78$ (mod 101)
    $7^8 \equiv 78^2 \equiv 24$ (mod 101)
    $7^{16} \equiv 24^2 \equiv 71$ (mod 101)
    $7^{20} \equiv 71 \cdot 78 \equiv 84$ (mod 101)
    $7^{24} \equiv 84 \cdot 78 \equiv 88$ (mod 101)
    $7^{26} \equiv 88 \cdot 49 \equiv 70$ (mod 101)
    Thus, $m = 70$
  - Decode m=13, with e=7 and p=101
    - Find f such that $ef \equiv 1$ (mod p-1)
    - That is, find f such that $7f \equiv 1$ (mod 100)
    - Now, use Euclidean Algorithm, to find f.
    - We have,
      - $100 = 14 \cdot 7 + 2$
      - $7 = 3 \cdot 2 + 1$
      - $2 = 2 \cdot 1 + 0$
    - Thus, $1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (100 - 14 \cdot 7) = 43 \cdot 7 - 3 \cdot 100$
    - Thus, f= 43
    - Then, $x^{ef} \equiv x \equiv m^f \equiv 13^{43} \equiv 9 \pmod{101}$
- Diffie-Hellman Key Exchange
  - $g = 2, p = 101, a = 23, b = 73$
    - $g^{ab} = g^{ba} \equiv 2^{23 \cdot 73} \equiv (2^{100})^{16} \cdot 2^{79} \equiv 2^{79} \equiv 42$ (mod 101)

- RSA Public Key
  - $p = 73, q = 139, e = 119, m = 9247$
    - $m = x^e$ (mod (pq))
    - We want to find f such that $fe \equiv 1$ (mod $(p-1)(q-1)$)
      - $119f \equiv 1$ (mod $72 \cdot 138$)
      - Thus, $f = 167$ by Euclidena algorithm
    - Then, $m^f = x^{ef} \equiv x \equiv 9247^{167} \equiv 3$ (mod $pq = 10147$)

Lecture 21,22,23 - Quadratic Residues

n is a positive integer and a is a unit in Z_n. Consider the congruence $x^2 \equiv a$ (mod n). If there is a solution, then a is called a quadratic residue (QR). Otherwise, it will be called a quadratic non-residue (QNR) modulo n.

- $n = 4$. units = 1 (QR),3 (QNR).
- $n = 7$. units = 1 (QR),2 (QR),3 (QNR),4 (QR),5 (QNR),6 (QNR).

Quadratic Residues modulo odd prime p

Legendre Symbol

$$(\frac{a}{p}) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if a is a QR} \\ -1 & \text{if a is a QNR} \end{cases}$$

Let g be a primitive root of Z_p, then we have

$$(\frac{g^k}{p}) = \begin{cases} 1 & \text{if k is a even} \\ -1 & \text{if k is a odd} \end{cases}$$

$$(\frac{2}{p}) = \begin{cases} 1 & p \equiv 1,7 \pmod 8 \\ -1 & p \equiv 3,5 \pmod 8 \end{cases}$$

$$(\frac{3}{p}) = \begin{cases} 1 & p \equiv 1,11 \pmod{12} \\ -1 & p \equiv 5,7 \pmod{12} \\ 0 & p \equiv 3 \pmod{12} \end{cases}$$

Number of Quadratic Residues

There are $\frac{p-1}{2}$ QR and $\frac{p-1}{2}$ QNR
$p^{k-1} \cdot \frac{p-1}{2}$ QR and $p^{k-1} \cdot \frac{p-1}{2}$ QNR

Properties of Legendre Symbol

1. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
2. $\left(\frac{1}{p}\right) = 1$, i.e. 1 is a QR
3. a is a unit. $\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)$
4. If a is a unit, then $\left(\frac{a^2}{p}\right) = 1$
5. If a is a unit, then $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$
6. Euler's Criterion: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ (mod p)
    - $x^2 \equiv a^{p-1} \equiv 1$ (mod p)
    - Thus, $x \equiv \pm 1$ (mod p)
7. $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$ (mod p)
8. −1 is a quadratic residue modulo p if and only if $p \equiv 1$ (mod4)

QNR and primitive root

Every primitive root has to be a quadratic nonresidue.

Gauss' Lemma

Suppose a is a unit modulo p. Write each of $a, 2a, ..., \frac{p-1}{2}a$ between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$ modulo p, and say there are n negative signs. Then, $\left(\frac{a}{p}\right) = (-1)^n$. The product of the elements will be $\left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)!(-1)^n$ (mod p)

Related Theorems & Lemma

Consider $S = \{a, 2a, 3a, ..., \frac{p-1}{2}a\}$

- $p = 7, a = 3$
  $S = \{3, 6, 9\} \equiv \{2, 3, 6\} \equiv \{-1, 2, 3\}$
- $p = 12, a = 2$
  $S = \{2, 4, 6, 8, 10, 12\} \equiv \{-1, 2, -3, 4, -5, 6\}$

Law of Quadratic Reciprocity

- Suppose $p \neq q$ are odd primes, then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$
- Suppose $p \neq q$ are odd primes. if p or q or both $\equiv 1$ (mod 4), then we have $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Else if $p \equiv q \equiv 3$ (mod 4), then $\left(\frac{q}{p}\right) = \left(-\frac{p}{q}\right)$

The case of 2^k

Let $k \geq 3$, then a is a QR modulo 2^k if and only $a \equiv 1$ (mod 8). Therefore, there are 2^{k-3} QR modulo 2^k and $3 \cdot 2^{k-3}$ QNR modulo 2^k

The general case $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$

Suppose (a,n)=1
a is a QR modulo n if and only if a is a QR modulo each $p_i^{\alpha_i}$

Exercises

- **What are the quadratic residues modulo 17?**
  - No need to check above $\frac{p-1}{2} = 8$ as $9 \equiv -8$ (mod 17)
  - $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 16, 5^2 \equiv 8, 6^2 \equiv 2, 7^2 \equiv 15, 8^2 \equiv 13$
- **Is 7 a quadratic residue modulo 23?**
  - In number theory, Euler's criterion is a formula for determining whether an integer is a quadratic residue modulo a prime.
  - Euler's criterion can be concisely reformulated using the Legendre symbol $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}$ (mod p)
  - $7^{11} \equiv 13 \cdot 7 \equiv -1$ (mod 17)
  - So, $(\frac{7}{23}) \equiv 7^{\frac{23-1}{2}} \equiv -1$
  - Thus, not a QR.
- **Show : There are infinitely many primes of the form 4k+1**
  - Suppose there are finitely many primes $p_1, p_2, ..., p_k$ of the form 4k+1.
  - Let $m = (2p_1p_2...p_k)^2 + 1$
  - Clearly, m is of the form $4k+1$
  - Since m is not one of $p_1, p_2, ..., p_k$, it must be a composite number. That is, there must be a prime number p such that $p \mid m$. That is, $(2p_1p_2...p_k)^2 + 1 \equiv 0$ (mod p)
  - Then, we have $(2p_1p_2...p_k)^2 \equiv -1$ (mod p)
  - Thus, -1 is a quadratic residue (QR)
  - That is, $(\frac{-1}{p}) = 1$
  - Thus, $p \equiv 1$ (mod 4)
  - Thus, $p_1, p_2, ..., p_k \nmid m$, contradiction.
- Consider $(\frac{2^3 \cdot 17^2 \cdot 19 \cdot 23^3}{71})$
  - = $(\frac{2^2 \cdot 17^2 \cdot 23^3}{71})(\frac{19}{71})(\frac{2}{71})$
    = $(\frac{19}{71})(\frac{23}{71})$ as $71 \bmod 8 = 7$