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: $(66, 121) = 11 \nmid 100 \to$ 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.
- $p \mid ab \to p \mid a \vee p \mid b$

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**
  $p = 2^m + 1 = (2+1)(x^{m-1} - x^{m-2} + ... - x + 1) \to$ p is divisible by 3 $\to$ 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. $a \equiv b$ (mod n))
- $[a]_n + [b]_n = [a+b]_n$
- $[a]_n \cdot [b]_n = [ab]_n$

Theorems

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

Step by Step - Solve $ax \equiv b$ (mod 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
  - $ax \equiv b \text{ (mod m)} \rightarrow ax \equiv mk + b \text{ (mod m)} \rightarrow ax - mk = b$
- 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**

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

- **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)**
    - Eucledieans 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

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

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.

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)