Divisibility

$d \mid a$ and $d \mid b \implies d$ divides any linear combination of a, b

Euclid Theorem: there are an infinite number of primes

Ways of finding $\gcd(a, b)$

- List all prime factors and take the largest factor
- Take a linear combination of a, b to find possible factors
- Euclidean Algorithm

Any common divisor of a, b divides $\gcd(a, b)$

From Extended Euclidean Algorithm, we can write $\gcd(a, b) = ax + by$

If n is composite then $2^n - 1$ is composite

If m is NOT a power of 2, then $2^m + 1$ is composite

Linear Diophantine Equations

We want to be able to find integer solutions (x, y) to $ax + by = c$

- Solutions exist if and only if $\gcd(a, b) \mid c$

General steps for solving Linear Diophantine problems

1. Verify $\gcd(a, b) \mid c$
2. Divide the equation by $d = \gcd(a, b) \implies a'x + b'y = c'$ where $\gcd(a', b') = 1$
3. Use Extended Euclidean Algorithm to solve (x, y) for $a'x + b'y = 1$. Then multiply the solution by c
4. If a solution variable (e.g. x) is negative, perform Extended Euclidean Algorithm with positive x then flip the sign at the end
5. General solutions will be $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$

For relatively prime a, b, there are no non-negative solutions to $ax + by = ab - a - b$

For relatively prime a, b and any $n > ab - a - b$, there is a non-negative solution to $ax + by = n$

Unique Factorization

Fundamental Theorem of Arithmetic: any positive integer greater than 1 can be uniquely factored into a product of primes

$\gcd(a, b) = 2^{d_2}3^{d_3}\cdots$ where $d_p = \min(a_p, b_p)$

$\operatorname{lcm}(a, b) = 2^{e_2}3^{e_3}\cdots$ where $e_p = \max(a_p, b_p)$

Linear Congruence

$a \equiv b \pmod{m} \implies m \mid a - b$ AND $a = b + km$ AND $\gcd(a, n) = \gcd(b, n)$

- Example $\gcd(1234, 10) = \gcd(4, 10)$ since $1234 \equiv 4 \pmod{10}$

Linear Congruence problem $ax \equiv b \pmod{m}$ can be reduced to a Diophantine Problem with $(a, -m, b)$

- Let $d = \gcd(g, m)$. Then $d \mid b \implies$ the congruence problem has d distinct solutions mod m

Steps to solve $ax \equiv b \pmod{m}$ where $\gcd(a, m) = 1$

1. Convert the problem into Linear Diophantine problem $ax - my = b$
2. Use Extended Euclidean Algorithm to find x_0, y_0 such that $ax_0 - my_0 = 1$
3. Compute $x = bx_0$

Steps to find an inverse of $a \pmod{m}$ with $\gcd(a, m) = 1$

1. Convert the problem into Linear Diophantine problem $ax - my = b$
2. Use Extended Euclidean Algorithm to find x_0, y_0 such that $ax_0 - my_0 = 1$
3. $x_0 \pmod{m}$ is the inverse of $a \pmod{m}$

Chinese Remainder Theorem: Given $x \equiv a_i \pmod{m_i}$ for relatively pairwise prime m_i then

$$x \equiv \sum_{i=1}^{n} a_i n_i u_i \qquad n_i = \prod_{j \neq i} m_j \qquad u_i = n_i^{-1} \pmod{m_i}$$

- Can factor composite modulues m into distinct prime powers and solve the system of congruence