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

Division Algorithm: Let $a, b \in Z$ with $b > 0$. Then there exists unique $q, r \in Z$ such that $a = bq + r$ with $0 \leq r < b$

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 $\gcd(a, b)$

Bezout Theorem: $\gcd(a, b) = ax + by$

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 and $a, b \geq 0$, there are no non-negative solutions to $ax + by = ab - a - b$

For relatively prime a, b, $a, b \geq 0$, and any $n > ab - a - b$, there is a non-negative solution to $ax + by = n$

Unique Factorization

Theorem 4.1: Let p be prime and $a, b \in Z$ such that $p \mid ab$. Then $p \mid a$ or $p \mid b$

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 $d_p = \min(a_p, b_p)$

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

Applications of Unique Prime Factorization

Proposition 5.1: n is a kth power if and only if all exponents in its prime factorization are multiples of k

Example: Find A such that $\frac{2}{3}A$ is a cube

Let $A = 2^a 3^b 5^c \cdots$ be the prime factorization of A

Then $\frac{2}{3}A^2 = 2^{2a+1}3^{2b-1}5^{2c}\cdots$ means that eaech exponent is a multiple of 3 Thus

$3 \mid 2a+1 \implies a = 1 \qquad 3 \mid 2b-1 \implies b = 2 \qquad 3 \mid 2c \implies c$ is a multiple of 3 (same for $d, e, \ldots$)

Thus $A = 18B^3$ for $B \geq 1$

Irrationality Proof

Show that $\sqrt{3}$ is irrational

BWOC suppose $\sqrt{3} = \frac{a}{b} \implies 3b^2 = a^2$

$\gcd(a,b) = 1 \implies 3 \mid a^2 \implies 3 \mid a$ by (UPF)

Thus $3b^2 = 9k^2$ for some $k \in Z \implies b^2 = 3k^2 \implies 3 \mid b$. Contradiction thus $\sqrt{3} \notin Q$

Theorem 5.3: n is not a perfect kth power $\implies \sqrt[k]{n}$ is irrational

Proof By contraposition: Suppose $\sqrt[k]{n} = \frac{a}{b} \implies nb^k = a^k$

Looking at prime factorization, $nb^k = p_1^{x_1+y_1k}\cdots = p_1^{z_1k}\cdots = a^k$

Thus $x_i + y_ik = z_ik \implies x_i = k(z_i - y_i) \implies n$ is a perfect kth power

Rational Root Theorem

Theorem 5.4: For $P(x) = a_nx^n + \cdots a_1x + a_0$ with $a_i \in Z$ and $a_n, a_0 \neq 0$, if $r = \frac{u}{v} \in Q$ and $\gcd(u,v) = 1$ and $P(u/v) = 0$, then $u \mid a_0$ and $v \mid a_n$

Proof: $a_n(\frac{u}{v})^n + \cdots + a_1(\frac{u}{v}) + a_0 = 0 \implies a_nu^n + \cdots + a_1uv^{n-1} + a_0v^n = 0$

Because $\gcd(u,v) = 1$, we have $v \mid a_n$ and $v \mid a_0$

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

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

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