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

Lienar 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

There are no non-negative solutions to $ax + by = ab - a - b$

For 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 $d_p = \min(a_p, b_p)$

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