Two Divisors, CRT, Basic Combinatorics

Lecture 6 : Summer of Competitive Programming

Soumil Aggarwal

Algorithms and Coding Club
Indian Institute of Technology Delhi

18 July 2021

Resources

Some of the content in these slides was inspired from cp-algorithms.com.
The images were taken from geeksforgeeks and Wikimedia Commons.

Two Divisors
Some observations

- If $\gcd(d_1, d_2) = g$, then $g|(d_1 + d_2)$ and $g|d_1|a$, so g has to be 1.
- Not possible for prime powers
- If $p_1^{k_1} p_2^{k_2} \dots p_i^{k_i}$ is the prime factorisation of a, then $\gcd(d_1 + d_2, a) = 1$ is equivalent to:
  $\gcd(d_1 + d_2, p_j) = 1$ for all $j = 1$ to i
- One way to do so is to choose d_1, d_2 so that each prime p_j divides exactly one of d_1, d_2.

Two Divisors

How to actually do it

- We can calculate the smallest prime divisor p_1 using a sieve, then calculate the largest power of p_1 dividing a.
- Choosing $d_1 = p_1^{k_1}$ and $d_2 = p_2^{k_2} \dots p_i^{k_i} = \frac{n}{d_1}$ would work.

Chinese Remainder Theorem

If $a_1, a_2, \ldots, a_n$ are pairwise relatively prime integers, then the set of congruences:

$$x \equiv b_1 \mod a_1$$
$$x \equiv b_2 \mod a_2$$
$$\vdots$$
$$x \equiv b_n \mod a_n$$

has a unique solution modulo $A = a_1 a_2 \ldots a_n$.

Chinese Remainder Theorem

Example

Suppose $a_1 = 2, a_2 = 3, a_3 = 25$, (so $A = 150$) and $b_1 = 0, b_2 = 2, b_3 = 1$, then all the valid values of x are given by $26 + 150m$, where m can be any integer.

Chinese Remainder Theorem

Proof

Suppose $0 \leq x_1 < x_2 < A$, then there exists a_i such that $a_i \not| (x_2 - x_1)$. So $x_1 \not\equiv x_2 \mod a_i$. So the value of x has to be unique modulo A (if it exists).

The sequence $(x_1 \mod a_1), (x_1 \mod a_2), \ldots, (x_1 \mod a_n)$ is different from the sequence $(x_2 \mod a_1), (x_2 \mod a_2), \ldots, (x_n \mod a_n)$. Since there are A numbers between 0 and $A - 1$, and A possible choices for $(b_1, b_2, \ldots b_n)$, each $(b_1, b_2, \ldots b_n)$ must have a corresponding valid choice of x.

$\phi(a_1 a_2) = \phi(a_1)\phi(a_2)$ if $\gcd(a_1, a_2) = 1$.
Proof: x is relatively prime to $a_1 a_2$ if and only if it is relatively prime to a_1, a_2 separately. Let $x \equiv b_1 \mod a_1$, $x \equiv b_2 \mod a_2$.
We just need $\gcd(b_1, a_1) = \gcd(b_2, a_2) = 1$.
There are $\phi(a_1)$ choices for b_1, $\phi(a_2)$ choices for b_2, and each choice of (b_1, b_2) produces a unique corresponding x (using CRT).
So $\phi(a_1 a_2) = \phi(a_1)\phi(a_2)$.

Calculating Binomial Coefficients

- Usually computed modulo a large prime, say p.
- Using Pascal's Identity :

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

$O(n^2)$ to calculate all values from $\binom{0}{0}$ to $\binom{n}{n}$. Can use a dp with $\text{dp}[i][0] = dp[i][i] = 1$, and $\text{dp}[n][k] = (\text{dp}[n-1][k-1] + \text{dp}[n-1][k]) \% p$

Calculating Binomial Coefficients

- Can precompute the values of factorials and their inverses modulo p upto $n!$ in $O(n)$ time. After that, fetching a single binomial coefficient takes $O(1)$ time.
- $\text{fact}[0] = 1$, $\text{fact}[i] = (\text{fact }[i-1] \times i)\%p$
- $\text{invfact[i]} = (\text{invfact}[i+1] \times (i+1))\%p$

Inclusion-Exclusion

To compute the size of a union of multiple sets, it is necessary to sum the sizes of these sets separately, and then subtract the sizes of all pairwise intersections of the sets, then add back the size of the intersections of triples of the sets, subtract the size of quadruples of the sets, and so on, up to the intersection of all sets.

Inclusion-Exclusion

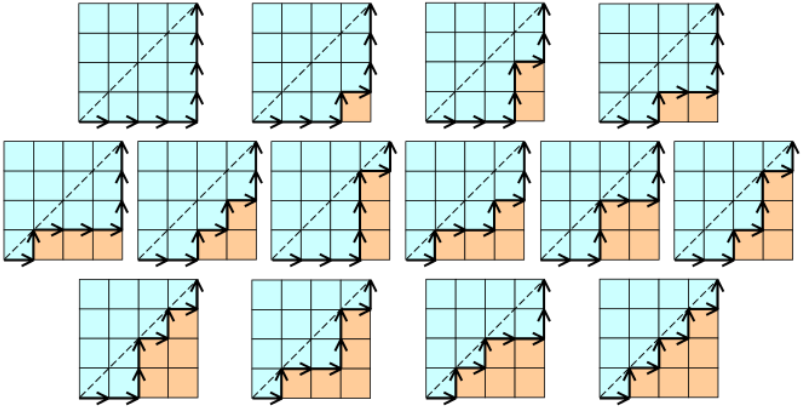
Example : Calculate the number of integers between 1 and 100 which are divisible by atleast one of $2, 3, 5$.

$$(100/2 + 100/3 + 100/5) - (100/6 + 100/10 + 100/15) + 100/30$$

where division is integer division.
Inclusion-exclusion is a humble tool that can be helpful in solving various kinds of problems. Example - Calculating the number of coprime integer pairs in a range, number of integers in a range divisible by at least one of a given set of integers, number of derangements, and various combinatorial problems

Catalan Numbers - The Reflection Trick

Count the number of paths C_n from $(0, 0)$ to (n, n) such that in each step, you either move right, or up, by 1 unit, and the x-coordinate is always $\geq$ the y-coordinate. For example, $C_4 = 14$.



Catalan Numbers - The Reflection Trick

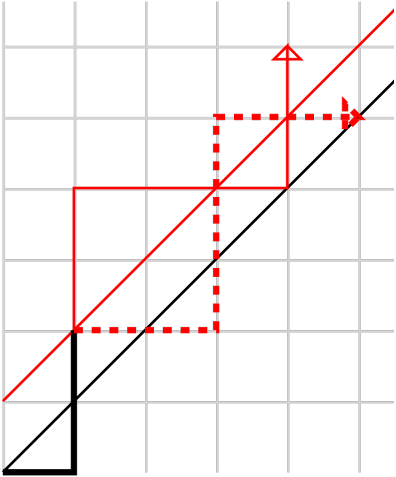
We will count the number of *bad* paths instead, i.e., the number of paths that do cross the line $y = x$.

To do that, we construct a bijection. For any bad path, consider the first instant when we have $y = x + 1$, and reflect the path after that point about the line $y = x + 1$. This will give a path from $(0, 0)$ to $(n - 1, n + 1)$, and one can check that this is process is reversible, so it is a bijection.

So, the number of bad paths is $\binom{2n}{n+1}$, and

$$C_n = \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n}$$

Catalan Numbers - The Reflection Trick



Catalan Numbers - The Reflection Trick

Catalan numbers solve various counting problems. A select few examples are -

- Number of correct bracket sequences consisting of n opening and n closing brackets
- Number of triangulations of a convex polygon with $(n+2)$ sides
- Number of ways to connect $2n$ points on a circle to form n disjoint chords