Number Theory.

* $n = p_1^{\alpha_1} \, p_2^{\alpha_2} \cdots p_k^{\alpha_k}$
* number of factors $= \prod_{i=1}^{k} (\alpha_i + 1)$
* Perfect number is something when the factor sum up to the numbers.
* Sum of factors $= \prod_{i=1}^{k} \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right)$
* There are infinite numbers of prime.
* Density of primes - $\pi(n) \approx \frac{n}{\ln n}$
* Goldbach's Conjecture - Each even integers $n > 2$ can be represented as a sum $n = a + b$ where a & b are primes.
* Twin prime Conjecture - There are infinite number of pair $(p, p+2)$ where both p and $p+2$ are prime.
* Legendre's Conjecture - There is always a prime number between n^2 & $(n+1)^2$ where $n > 0 \in I$.
* Algorithms - If a number is not prime then it has a factor between 2 to $\sqrt{n}$ using this we can find whether number is prime and prime factor ization in $O(\sqrt{n})$ time.
* Sieve of Eratosthenes :- Initially we would mark Every number as zero then we will check whether the number is prime or not

0	0	1		2		1	1	1		2		1		1	
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

$$\sum_{x=2}^{n} n/x = n/2 + n/3 + n/4 + \cdots\cdots n/n = O(n \log n)$$

* Euclid's Algorithm - $\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$. $\gcd(\text{int } a, \text{int } b) = \gcd(a, a\%b)$
* Euler's totient function - Comprime? $f(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$
* Modular Exponentiation -

$$x^n = \begin{cases} 1 & n = 0 \\ x^{n/2} \cdot x^{n/2} & n \text{ is even} \\ x^{n-1} \cdot x & n \text{ is odd} \end{cases}$$

```
int modpow(int x, int n, int m) {
    if (n == 0) return 1%m;
    long long u = modpow(x,n/2,m);
    u = (u*u)%m;
    if (n%2 == 1) u = (u*x)%m;
    return u;
}
```

* Diophantine equation - $ax + by = c$ * It can only be solved when $c = \gcd(a,b)$
* Chinese remainder theorem -