Modular Arithmetic

For CP

Contents

The Modulo Operator

- For an integer a, and modulo (integer) m
- b = a % m, b is the remainder a when divided by m
- i.e repeatedly subtracting m from a until a < m

Modular Addition

- Int a, int b, int mod
- Find (a+b) % mod
- What if (a+b) overflows?
- (a+b) % mod = ((a%mod) + (b%mod)) % mod

Modular Multiplication

- Int a, int b, int mod

- Find (a * b) % mod
- But a * b may overflow

- (a * b) % mod = ((a % mod) * (b % mod)) % mod

Problem #1

- https://leetcode.com/problems/maximum-subarray-min-product/
- https://leetcode.com/problems/sum-of-floored-pairs/
- https://leetcode.com/problems/largest-palindrome-product/

Binary Exponentiation

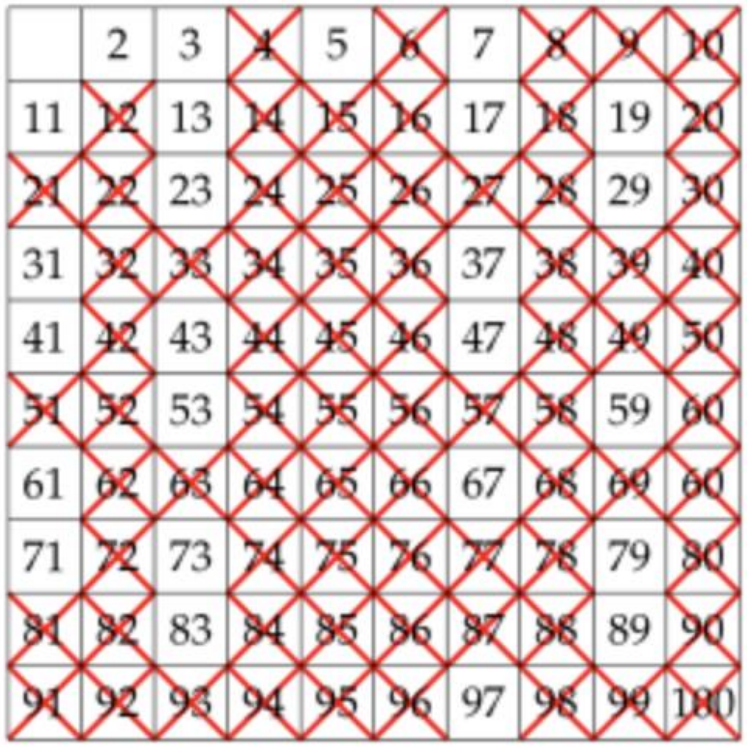
```
public static long binpow(long a, long b, long m) {
a %= m;
long res = 1;
while (b > 0) {
if (b%2==1) {
res = res * a % m;
}
a = a * a % m;
b >>= 1;
}
return res;
}
```

Modular Division

```
public static long moddiv(long a, long b, long m) {
return (a%m * binpow(b,m-2,m)%m)%m;
}
```

- https://pi.math.cornell.edu/~morris/135/mod.pdf
- https://en.wikipedia.org/wiki/Modular_multiplicative_inverse

Sieve of Eratosthenes



Problem Set

- https://codeforces.com/contest/1881/problem/D

- (difficult) https://codeforces.com/contest/1886/problem/D