COP 4516 2/18/2025

1. Topic - Math (Mostly Number Theory)
2. Make Up Final Ind - Sky After Class (Thursday) 2/27
3. USACO Scores - After Class

gcd(a,b) - greatest common divisor

- return b == 0 ? a : gcd(b, a%b)

lcm(a,b) = a/gcd(a,b) * b

a^{-1} mod n exists iff gcd(a,n) = 1

- code in notes

If n is prime, then $a^{-1} \equiv \boxed{a^{n-2} \bmod n}$

Reason: Fermat's Thm if p prime gcd(a,p)=1 $a^{p-1} \equiv 1 \pmod p$

$a^{p-2} \times a \equiv 1 \pmod p$

inverses of each other!

When is mod inverse useful?

What is $\sum_{i=1}^{n} i \bmod 10^9+7$

n can be upto 10^9

$= \frac{n(n+1)}{2} \equiv n(n+1)2^{-1} \bmod 10^9+7$

Prime Factorization

n - runtime $O(\sqrt{n})$

$2^3 \times 3^4$

(2,3), (3,4), ...

pseudo code

```
primefact = [ ]
i = 2
while (i*i <= n) {
    exp = 0
    while (n % i == 0) {
        exp++;
        n = n / i;
    }
    if (exp > 0)
        primefact.add((i, exp))
    i++;
}
if (n > 1) primefact.add((n, 1));
```

$$\text{NUMDIVISORS} = p_1^{a_1} p_2^{a_2} \cdots = (a_1+1)(a_2+1)(a_3+1)\cdots$$

$$\text{SUMDIVISORS} = \frac{(p_1^{a_1+1}-1)}{(p_1-1)} \times \frac{(p_2^{a_2+1}-1)}{(p_2-1)} \times \cdots$$

PRIME SIEVE

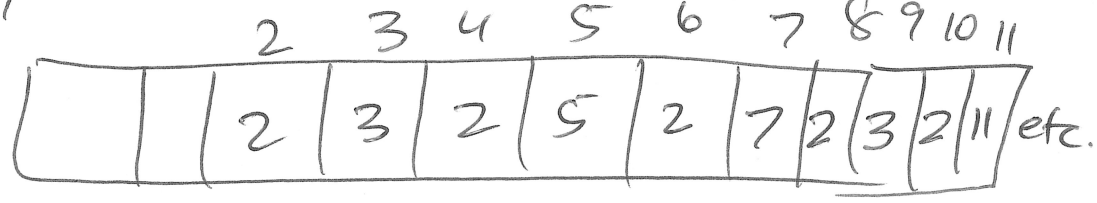
Identify all primes from 1 to n

boolean array set all indexes 2 to n to TRUE

CROSS OFF ALL MULTIPLES OF PRIMES (EXCEPT PRIME)

```
for (i=2; i*i<=n; i++)        // 2i, 3i, 4i, ...
    for (j=2*i, j<=n; j+=i)
        sieve[j] = false;
```

my modified



Problem : cses.fi

EULER PHI FUNCTION

$\phi(n)$ = # of integers, q range $1 \ldots n$, s.t.

$$gcd(a,n) = 1$$

$\phi(15) = 8$, [1, 2, 4, 7, 8, 11, 13, 14]

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

$n = 2$

p is prime $\phi(p_1^{a_1} p_2^{a_2} p_3^{a_3}) = \phi(p_1^{a_1})\,\phi(p_2^{q_2})\,\phi(p_3^{q_3}) \ldots$

$$= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) p_2^{q_2}\left(1 - \frac{1}{p_2}\right) \ldots$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots$$