CIS 3362 10/14/24

My Schedule

Leave Wed right after class (OH W 1:30 cancelled)

Fri - NOT HERE (VIDEO WILL BE RECORDED today in the afternoon)

Quiz 4 - pushed back, HS - posted, pushed back

Homework - Program (Wed sample so every follows the format I want.)

Number Theory Background

Prime Number: pos int greater than 1, whose only divisors are 1 and itself.

$N = ab$ if $a > \sqrt{N}$ and $b > \sqrt{N}$

then $ab \geq \sqrt{N}\sqrt{N} = N$ so this isn't possible

if a number, N, is NOT prime (composite) it will have at least one divisor, a, $1 < a \leq \sqrt{N}$.

```
int isprime(int n) {
    for (int i = 2; i*i <= n; i++)
        if (n % i == 0)
            return 0; // NOT PRIME
    return 1; // IS PRIME
}
```

Runtime $O(\sqrt{n})$

if $n = 10^{12}$ $\sqrt{n} = 10^6$, and this is fast. (< 1 sec)

But if you did $O(n)$ for $n = 10^{12}$ $\Rightarrow$ pretty slow (~1 hr)

Note divisors come in pairs except for the square root if it's an int

36: 1 2 3 4 6 / 36 18 12 9

24: 1 2 3 4 / 24 12 8 6

C: long long (upto ~ 10^{18})

List all prime #s upto n, prime sieve

```
boolean prime[n+1]   // Pseudocode
fill(prime, true); prime[0] = prime[1] = false;
for (int i = 2; i*i <= n; i++)
    for (int j = 2*i; j <= n; j += i)
        prime[j] = false
```

(i: 2i, 3i, 4i, 5i)

$O(\sqrt{n} \lg n)$

---

for our purposes, we'll eventually need to deal with really large integers, so we're going to try to find some properties that will help us develop a faster prime test.

Let p be a prime number and consider all of the non-zero remainders:

$$S = \{1, 2, 3, 4, \ldots, p-1\}$$

Pick a integer a with $\gcd(a,p)=1$. (Don't pick a multiple of p.

$p=7$

	1	2	3	4	5	6
$a=4$	4	8	12	16	20	24
	4	1	5	2	6	3

$$T = \{a, 2a, 3a, 4a, \ldots (p-1)a\}$$

Create set T, so each # in T is a number in S multiplied by a and taking remainders when divided by p, then T and S are the same set!!!

① no element of T is equal to 0.

all elements of T are the product of a and i, $1 \le i \le p-1$. $\gcd(i,p)=1, \gcd(a,p)=1$

$\Rightarrow \gcd(ai,p)=1 \quad ai \not\equiv 0 \pmod p$.

② no 2 elements of T are equivalent mod p.

Assume the opposite $ai \equiv aj \pmod p$

$1 \le i < j \le p-1$.

$aj - ai \equiv 0 \pmod p$

$a(j-i) \equiv 0 \pmod p$

$p \mid a$ or $p \mid (j-i)$ NOT POSSIBLE

not true $j-i > 0$, $j-i < p-1$

Thus, our assumption was wrong and all items in T are different mod p.

Fermat said, let's multiply all elements of S and take the remainder when divided p. Do the same for T. These remainders have to be the same

$$\prod_{i=1}^{p-1} ai \equiv \prod_{i=1}^{p-1} i \pmod{p}$$

$a(2a)(3a)(4a)\dots((p-1)a)$
Product of items in T

$1\times2\times3\times\dots(p-1)$
Product items in S

$$\prod_{i=1}^{p-1} ai - \prod_{i=1}^{p-1} i \equiv 0 \pmod{p}$$

$$a^{p-1}\prod_{i=1}^{p-1} i - \prod_{i=1}^{p-1} i \equiv 0 \pmod{p}$$

$$\left(\prod_{i=1}^{p-1} i\right)\left(a^{p-1}-1\right) \equiv 0 \pmod{p}$$

$$p \mid \prod_{i=1}^{p-1} i \quad \text{OR} \quad \boxed{p \mid \left(a^{p-1}-1\right)}$$

This is false all primes in product $< p$.

This MUST BE TRUE

Fermat's Theorem

$a^{p-1} - 1 \equiv 0 \pmod{p}$

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

if $\gcd(a,p)=1$ & p is prime then

$p = 101$ (prime)

$69^{100} \equiv 1 \pmod{101}$

$72^{100} \equiv 1 \pmod{101}$

What is the remainder when $14^{10,002}$ is divided by 101?

$$14^{10,002} = 14^{10000} \times 14^2$$

$$= (14^{100})^{100} \times 196$$

$$\equiv 1^{100} \times 95 \pmod{101}$$

$$\equiv \boxed{95 \pmod{101}}$$