CIS 3362 10/17/22

---

eventually Public Key Cryptography

Background: Num Theory

Prime Numbers - Fundamental Thm Algebra
Fermat's Theorem

Prime: Int 2 or greater divisible by only 1 and itself.

every int has a unique prime factorization

$75 = 3^1 \times 5^2$

I want you to be able to prime factorize a number by hand and/or comp prog.

$$225{,}000{,}000 = 225 \times 10^6$$
$$= 15^2 \times 2^6 \times 5^6$$
$$= 3^2 \times 5^2 \times 2^6 \times 5^6$$
$$= \boxed{2^6 \times 3^2 \times 5^8}$$

by calc: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29

(a) Primality Test
(b) "Code" prime factorization
(c) Prime Sieve

```
boolean isPrime(int n) {
    int i = 2;
    while (i*i <= n) {
        if (n%i == 0)
            return false;
        i++;
    }
    return true;
}
```

Run-time
$O(\sqrt{n})$

---

Get prime fact do same prime test when you get a divisor, divide it out

```
i = 2;
while (i*i <= n) {
    while (n%i == 0) {
        print(i);
        n /= i;
    }
    i++;
}
if (n > 1) print(n);
```

Run-time
Same as prime test

---

```
boolean isPrime[n+1];
//fill array true from index 2 on
for (i = 2; i*i <= n; i++)
    for (j = 2*i; j <= n; j += i)
        isPrime[j] = false;
```

For very large integers, our basic prime test is too slow. We would like a faster one!

Goal: to determine if a # is prime or not faster.

Observation #1: too many trial divisions! We have to avoid trying all of them.

Observation #2: We seek to find some "property" that is true of primes, but false for composites.

Let's consider the set of remainders when dividing by a prime $p$, except 0:

$S = \{1, 2, 3, 4, 5, \ldots, p-1\}$

What happens if we multiply each item in $S$ by $a$, $\gcd(a,p) = 1$ and reduce the values mod $p$?

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

$p = 7, a = 4$

$S = \{1, 2, 3, 4, 5, 6\}$

$T = \{4, 8, 12, 16, 20, 24\}$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

$1 \quad 5 \quad 2 \quad 6 \quad 3$

Sets $S$ and $T$ are the same when reduced mod $p$ to range $\{0, 1, 2, \ldots p-1\}$

Goal: Prove each item in $T$ is unique mod $p$, and that no item in $T$ is divisible by $p$.

$\{a\cdot 1, a\cdot 2, a\cdot 3, \ldots a\cdot(p-1)\}$, $\gcd(a,p)=1$.

Only way to be divisible by a prime is to have it as a divisor, but $a$ isn't divisible $p$ and none of $1, 2, 3, \ldots p-1$ are either.

To prove the first item, we'll use proof by contradiction. Assume the opposite that 2 values in the set $T$ are equivalent mod $p$:

$$a_i \equiv a_j \pmod p \qquad i \neq j$$
$$1 \leq i, j \leq p-1.$$
$$a_i - a_j \equiv 0 \pmod p$$
$$a(i-j) \equiv 0 \pmod p$$
$$\Rightarrow p \mid [a(i-j)]$$
$$\Rightarrow \cancel{p \mid a} \quad \vee \quad p \mid (i-j)$$

not possible

$$1 \leq |i-j| \leq p-2$$

Contradicts given info about $i$ and $j$.

Thus our initial assumption was incorrect. It follows that each element in $T$ is unique mod $p$.

$\Rightarrow$ Conclude $S$ and $T$ are equivalent sets mod $p$

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

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

Gauss!

$$\underbrace{\prod_{i=1}^{p-1} a \cdot i}_{\text{product of items in } T} \equiv \underbrace{\prod_{i=1}^{p-1} i}_{\text{product of items in } S} \pmod{p}$$

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

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

$$(p-1)!\,(a^{p-1} - 1) \equiv 0 \pmod{p}$$

$$\Rightarrow p \mid [(p-1)!\,(a^{p-1}-1)]$$

Since $p$ is prime $\Rightarrow p \mid (p-1)! \vee \underbrace{p \mid (a^{p-1}-1)}_{\text{TRUE}}$

$p \mid (p-1)!$ is false since $p$ isn't a divisor of $(p-1)!$.

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

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

Fermat's thm: Given a prime $p$, and int $a$, $\gcd(a,p) = 1$,

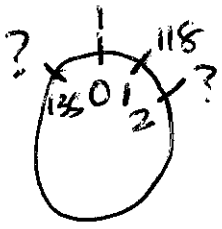
$p = 101, a = 45 \quad 45^{100} \equiv 1 \pmod{101}$

$p = 137, a = 118 \quad 118^{136} \equiv 1 \pmod{137}$

How I test

Use fermat's thm to find the remainder when $118^{409}$ is divided by 137

By fermat's thm since 137 is prime $118^{136} \equiv 1 \bmod 137$




$$118^{409} = 118^{3(136)+1}$$

$$= (118^{136})^3 \times 118^1$$

$$\equiv 1^3 \times 118 \pmod{137}$$

$$\equiv \boxed{118 \pmod{137}}$$