CIS 3362 - 10/11/2023

Number Theory Intro

Fund Theorem Arith

every pos int can be uniquely prime factorized

Prime: int divisible by only 1 and itself

$$36 = 4 \times 9$$
$$= 2 \times 2 \times 3 \times 3 = 2^2 \times 3^2$$

$$n = \prod_{p_i \in Prime} p_i^{a_i} = 2^2 \times 3^2 \times 5^0 \times 7^0 \times \ldots$$

How to prime factorize: trial division

If a #, "n", is composite, then it has at least 1 divisor $\leq \sqrt{n}$

assume opposite $a \times b = n$ and $a > \sqrt{n}$ and $b > \sqrt{n}$

$$a \times b > \sqrt{n} \times \sqrt{n}$$
$$= n$$

Write a function to prime factorize a number upto 10^{12}.

Fermat's Thm

If $\gcd(a,p)=1$ and $p \in \text{Prime}$, then

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

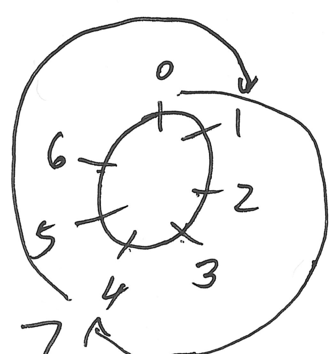
$p=101 \quad a=68 \quad 68^{100} \equiv 1 \pmod{101}$

$S = \{1, 2, 3, \ldots, p-1\}$ all non-zero remainder when divide by p
$\gcd(i,p)=1$
for all $1 \le i \le p-1$.

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

Prove that the elements of T taken mod p are the same set as S.

$p=7, \ a=4$



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

$T \ \{4, 8, 12, 16, 20, 24\} \bmod 7$

$\quad 4 \ \ 1 \ \ 5 \ \ 2 \ \ 6 \ \ 3$

$\gcd(4,7)=1$

Assume the opposite $S \neq T$ (elements mod p)

None of the elements of $T \equiv 0 \pmod{p}$

all must be $\equiv x \bmod p$ $x > 0$.

If all elements unique the $S = T$.

T has a repeat element.

$$ai \equiv aj \pmod{p} \quad 1 \leq i < j \leq n-1$$

~~$a(i-$~~

$$ai - aj \equiv 0 \pmod{p}$$

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

$$\Rightarrow p \mid a(i-j)$$

$$\Rightarrow p \mid a \quad \vee \quad p \mid (i-j)$$

$\times$ wrong

$0 < |i-j| < p-1$

$\times$ wrong

$a \mid b$ - "b is divisible by a"

$\exists c \in \mathbb{Z} \mid b = ac$.

"there exists an integer c such that $b = ac$.

CONTRADICTION!

Conclude that our initial assumption was wrong! It follows that $S = T$ as desired.

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

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

$$\prod_{x \in T} x \equiv \prod_{y \in S} y \pmod{p}$$

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

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

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

$$\Rightarrow p \,\Big|\, \prod_{i=1}^{p-1} i \quad \vee \quad p \,\big|\, (a^{p-1} - 1)$$

$\times$ not true

This $\underline{\underline{\text{IS}}}$ true!

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

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

If you ~~taken~~ any base any exponentiate it, mod p, you'll a looping/cyclic pattern of size k where $k \mid (p-1)$.

base \ exp	0	1	2	3	4	5	6	
1	1	1	1	1	1	1	1	cycle size 1
2	1	2	4	1	2	4	1	cycle size 3
3	1	3	2	6	4	5	1	$\boxed{\text{cycle size } 6}$
4	1	4	2	1	4	2	1	cycle size 3
5	1	5	4	6	2	3	1	$\boxed{\text{cycle size } 6}$
6	1	6	1	6	1	6	1	cycle size 2

generators or primitive roots

Euler Phi Function

$\phi(n)$ = the number of ints from 1 to n that are relatively prime with n.

$\phi(6) = 2$ 1 ~~2~~ ~~3~~ ~~4~~ 5 ~~6~~

$\phi(15) = 8$ 1 2 ~~3~~ 4 ~~5~~ ~~6~~ 7 8 ~~9~~ ~~10~~ 11 ~~12~~ 13 14 ~~15~~

possible keys affine w/ alphabet size n

$= n\,\phi(n)$

n: # choices b

$\phi(n)$: # choices a

Euler's Thm

If $\gcd(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$

$$|S| = \phi(n) \quad S = \{\overset{a_1}{1}, \overset{a_2}{2}, \overset{a_3}{4}, \overset{\cdots}{7}, 8, 11, 13, \overset{a_{\phi(n)}}{14}\}$$

S = all values from 1 to n rel prime to n

reduced residue system mod 15

$a=4$

$$T = \{\overset{aa_1,}{4}, \overset{aa_2,}{8}, \overset{\cdots}{16}, 28, 32, 44, 52, \overset{a \cdot a_{\phi(n)}}{56}\}$$

$$4 \quad 8 \quad 1 \quad 13 \quad 2 \quad 14 \quad 7 \quad 11$$

Prove $S = T$.

either $S = T$ or T has a repeat!

$$aa_i \equiv aa_j \pmod{n} \qquad a_i \neq a_j$$

$$aa_i - aa_j \equiv 0 \pmod{n}$$

$$a(a_i - a_j) \equiv 0 \pmod{n}$$

$$\Longrightarrow n \mid (a \cdot (a_i - a_j))$$

Adjusted Rule
if $\gcd(n,a) = 1$ and $n \mid ab$, then $n \mid b$.

we know ~~nt~~ $\gcd(n,a) = 1$ so

$$\Longrightarrow n \mid (a_i - a_j)$$

$$0 < |a_i - a_j| < n-1 \quad \text{Contradiction}$$

$$\prod_{i=1}^{\phi(n)} aa_i \equiv \prod_{i=1}^{\phi(n)} a_i \pmod{n}$$

$$\prod_{i=1}^{\phi(n)} aa_i - \prod_{i=1}^{\phi(n)} a_i \equiv 0 \pmod{n}$$

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

$\longrightarrow \; n \mid \left(\prod_{i=1}^{\phi(n)} a_i\right)\left(a^{\phi(n)} - 1\right)$, but

$\gcd(n, \underbrace{\prod_{i=1}^{\phi(n)} a_i}_{\text{all rel prime to } n}) = 1$, so it follows that

$$n \mid \left(a^{\phi(n)} - 1\right)$$

$$\longrightarrow \; a^{\phi(n)} - 1 \equiv 0 \pmod{n}$$

$$a^{\phi(n)} \equiv 1 \pmod{n}$$