Part 1: Prime numbers

Definition: A Prime Number is divisible only by itself and 1.

Notation of divide: $d \mid n$

Mersenne Prime: $2^n - 1$ (Not all primes Mersenne) ie: 15

Fermat numbers: $2^{2^n} - 1$ (Not all Fermat numbers are prime)

Proof: There are infinitely many primes.

For any finite set $\{p_1 \cdots p_r\} \subset P$, consider the number $n = p_1 \cdots p_r + 1$

Note that $p_i \nmid n$ for all $i = 1 \cdots r$ then

either n is a prime
or n has a divisor $p \notin \{p_1 \cdots p_r\}$, then either way a new prime is being generated.

Practice $p \in \mathbb{P}$, if $p \mid n^2+2$, then $p=2$ or $p \equiv 1$ or $3 \pmod 8$

Prove: infinitely many primes of the form $8m+3$ $m \in \mathbb{N}$

(Hint if $a \equiv a' \pmod n$ $b \equiv b' \pmod n$, $a+b \equiv a'+b' \pmod n$, $ab \equiv a'b' \pmod n$.)

Assume $\{p_1 \cdots p_k\}$ be finite set that contains all the primes in the form of $8m+3$, $m \in \mathbb{N}$

$N = n^2+2$ $n = p_1 \cdots p_k$ if p doesn't exit, N is a new prime.

By given theorem $p=2$ or $p \equiv 1$ or $3 \pmod 8$

Since $p_1 \cdots p_k$ is in form $8m+3$ So n^2+2 is odd, so $p \neq 2$.

① Assume $p' \equiv 1 \pmod 8$ for all $p \mid N$, $N = p_1' \cdots p_r'$

$N \equiv 1 \pmod 8$

Since $N = p_1^2 p_2^2 \cdots p_{k+2}^2$, $p_1 \cdots p_k \equiv 3 \pmod 8$

$p_1^2 \cdots p_k^2 \equiv 1 \pmod 8$

$N \equiv 1 + 2 \equiv 3 \pmod 8$ Contradicts!

Not all $p|N$ are in the form $8m+1$.

② There exists one $p = 8m+3$. $p_1 \cdots p_k \nmid N$

generate

Part 2: Greatest Common Divisor.

Important Fact:

① if $m|n$ then $\gcd(n, m) = m$

② if $n = qm + r$ $(q \geq 0, 0 \leq r < m)$, then $\gcd(n, m) = \gcd(m, r)$

③ There exists unique q and r $(q \geq 0, 0 \leq r < m)$ so that $n = qm + r$

* ④ $\gcd\left(\frac{d}{\gcd(k,d)}, \frac{k}{\gcd(k,d)}\right) = 1$ $m = \gcd(k, d)$, $n_1 = \frac{d}{m}$, $n_2 = \frac{k}{m}$, $\gcd(n_1, n_2) = 1$

⑤ p be prime. if $p|ab$, then $p|a$ or $p|b$

* ⑥ If $c|ab$, $\gcd(b, c) = 1$, then $c|a$

Hint: To prove two numbers are equal: $a|b$ and $b|a \Leftrightarrow a = b$

To prove $d|k$ ① consider $k = qd + r$ and prove $r = 0$ ② Consider Lagrange Theorem

. :

Practice: prove if $a \in G$, $|a| = d$. If $\exists k$, such that $a^k = e$ then $d | k$ (By using ①)

$k = qd + r \quad (0 \le r < d)$

Then $a^k = e = a^{qd+r} \quad a^{qd} \cdot a^r = e$

Given that $|a| = d$, d is the smallest positive integer s.t.

$a^d = e \Rightarrow (a^d)^q = e$, $a^r = e$, $r > 0$ or $r = 0$

$\Rightarrow r = 0$

$k = qd \quad d | k$.

✡ Euclidean Algorith & Diophantine Equation

Euclidean Algorithm: used to find $\gcd(n, m)$

Diophantine Equation: $mx + ny = \gcd(m, n)$, find x, y satisfy the equation.

Practice: find x, y s.t. $42823x + 6409y = 17 = \gcd(42823, 6409)$

Solution: $42823 = 6409 \times 6 + 4369$

$6409 = 4369 \times 1 + 2040$

$4369 = 2040 \times 2 + 289$

$2040 = 289 \times 7 + 17$

$289 = 17 \times 17 + 0$

Back tracking: $17 = 2080 - 289 \times 7$

$=$ ⋮

$= 6409 \times 147 - 42823 \times 22$.

$x = -22$, $y = 147$

Part 3: Group Theorem

To prove G is a group:

① Closure: if $a \in G$, $b \in G$, $a \circ b \in G$

② Associative composition $(a \circ b) \circ c = a \circ (b \circ c)$

③ Identity Element 1 exisits s.t. $1 \cdot a = a \cdot 1 = a$ for $\forall a \in G$

④ For $\forall a \in G$, $\exists a'$ s.t. $a \cdot a' = 1$

Practice: Given $a, b \in R$, define $T_{a,b}: R \to R$ $x \mapsto ax+b$

① Closure

$T_{c,d}$, $T_{a,b} \in G$, then $T_{cd} \circ T_{ab} \in G$.

$T_{cd} \circ T_{ab} = c(ax+b) + d = cax+cb+d = T_{ca,\, cb+d}(x) \in G$

where $ca \in R$ $(cd \neq 0)$

$cb+d \in R$

② Associative: $ax+b$ is associative $\Rightarrow$ $\circ$ composition associative.

③ Identity element $T_{cd} \circ T_{ab} = cax + cb + d = cx + d$.

$$\begin{cases} c = ca \\ cb = 0 \end{cases} \Rightarrow \begin{cases} a = 1 \\ c = 0 \end{cases}$$

$T_{1,0}(x)$, identity element for G. $T_{1,0}(x) = e$.

④ Inverse $T_{c,d} \circ T_{a,b}(x) = T_{1,0}(x) = x = cax + cb + d$.

$$\begin{cases} ac = 1 \\ cb + 1 = 0 \end{cases}$$

$c = \frac{1}{a}$, $d = -\frac{b}{a}$

$T_{a,b}(x)^{-1} = T_{\frac{1}{a}, -\frac{b}{a}}(x)$

Theorem if $S = a\mathbb{Z} + b\mathbb{Z}$, $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, $d = ra + sb$

1. $d|a$, $d|b$ 2. If $e|a$, $e|b$ then $e|d$ 3. $d = \gcd(a,b)$

Least common multiple $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, $m = \mathrm{lcm}(a,b)$

Fact: $d = \gcd(a,b)$, $m = \mathrm{lcm}(a,b)$ $ab = dm$

Part 4: Cyclic Group

Definition: A group is cyclic if it can be generated by single element.

① order: Smallest integer $x^d = e$ $|x| = d$

② order of generator = order of cyclic group $|x| = |\langle x \rangle|$

③ $|x| = n$, $x^k = 1$, then $n|k$, useful to prove $n|k$!

Important Theorems

① $|x| = n \in \mathbb{N} \setminus \{0\}$, $\langle x^k \rangle = \langle x^{\gcd(n,k)} \rangle$ $|x^k| = \frac{n}{\gcd(n,k)}$

② $\langle x^i \rangle = \langle x^j \rangle \Leftrightarrow |x^i| = |x^j| \Leftrightarrow \gcd(n,i) = \gcd(n,j)$

③ $\langle x \rangle = \langle x^j \rangle \Leftrightarrow \gcd(n,j) = 1 = \gcd(n,1)$

④ For each $k|n$, $\langle x \rangle$ has exactly one subgroup of order k

Euler Torient Function

$\varphi(n) = |\{k \in \mathbb{N} \mid \gcd(k,n)=1,\ 1 \le k \le n\}|$

for $p \in \mathbb{P}$, $\varphi(p) = p-1$, $\varphi(p^k) = p^k - p^{k-1}$

Property $\varphi(n)$ is multiplicative:

$\varphi(m_1, m_2) = \varphi(m_1)\varphi(m_2)$ if $\gcd(m_1, m_2) = 1$

☆ For cyclic group: The number of element of order d is given by $\varphi(d)$.

Part 5: Homomorphism

Definition: Given groups G, G' $f: G \to G'$ s.t for all $x, y \in G$.

$f(x \circ_G y) = f(x) \circ_{G'} f(y)$

① Take care: operation of $G(\circ_G)$ and $G'(\circ_{G'})$ may be different.

Property of homomorphism

1. for $a_1 \cdots a_k \in G$, $f(a_1 \cdots a_k) = f(a_1) \cdots f(a_k)$

2. $f(1_G) = 1_{G'}$

3. $f(a^{-1}) = f(a)^{-1}$

② Image of f: $\mathrm{Im} f = \{x \in G' \mid x = f(a),\ a \in G\}$

kernal of f: $\ker f = \{a \in G \mid f(a) = 1_{G'}\}$

③ Prove injective of homomorphism: iff $\ker f = \{1_G\}$

Isomorphism: f is bijective. Prove ① $\ker f = \{1_G\}$

② $\mathrm{Im} f = G'$

④ if f is Isomorphism then f' is also isomorphism.

Cosets

① Left Coset: $aH = \{g \in G \mid g = ah$ for some $h \in H\}$. $H \leq G$

* for coset aH a is a fixed element from G.

② cosets are equivalence classes

③ Index: $[G:H]$ is number of left coset of H in G.

* ④ Counting Formula: $|G| = |H| \cdot [G:H]$

⑤ Lagrange Theorem: $|H| \mid |G|$ The order of H divides order of G.

Practice: Give $a, n \in \mathbb{N}$ and $a, n > 1$ Show that $n \mid \varphi(a^n - 1)$

(Hint: order of $(\mathbb{Z}/m\mathbb{Z})^\times$ is $\varphi(m)$ $(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$)

$\varphi(m)$ $m = a^n - 1$ $\varphi(a^n - 1) = |\mathbb{Z}/(a^n - 1)\mathbb{Z}|$ for $\forall a^n - 1$

$\gcd(a, a^n - 1) = 1 \Rightarrow a \in \mathbb{Z}/(a^n - 1)\mathbb{Z}$

Then prove order of a, $|a| = n$, Since $a^n - 1 \mid a^n - 1$ So $a^n \equiv 1 \pmod{a^n - 1}$

Also for $0 < x < n$ $a^x \not\equiv 1 \pmod{a^n - 1}$ $a^x < a^n - 1$.

$|H| \mid |G|$, so ... $n \mid \varphi(a^n - 1)$

Normal Subgroup

Definition: if for all $a \in N$ and $g \in G$, $gag^{-1} \in N$

① if f is homomorphism, then $\ker f \trianglelefteq G$

② Center: $Z := \{z \in G \mid zx = xz \text{ for all } x \in G\}$ center is normal subgroup

③ To prove normal subgroup: 1° prove subgroup (closure)

2° prove the following

$$\begin{cases} 1.\ gHg^{-1} = H \text{ for all } g \in G \\ 2.\ gH = Hg \text{ for all } g \in G \end{cases}$$

Part 6: Modular Arithmetic

① mod operation property

$a \equiv b \pmod{c}$ & $d \equiv e \pmod{c}$ Then $a+d \equiv b+e \pmod{c}$, $ad \equiv be \pmod{c}$

② Fermat's Little Theorem:

1° $a^{p-1} \equiv 1 \pmod{p}$ if $\gcd(a,p)=1$ $p \in$ Prime, $a \in Z$.

2° $a^p \equiv a \pmod{p}$ if $a \in Z$, $p \in$ Prime

③ Multiplicative Group

$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n)=1\}$

✡: $|(\mathbb{Z}/n\mathbb{Z})^{\times}| = \varphi(n)$ by definition of Euler Totient Function

④ Euler Theorem:

if $\gcd(a,m)=1$, $a^{\varphi(m)} \equiv 1 \pmod{m}$

(✡ For Fermat Theorem, m is required to be prime, in Euler, it's arbitrary).

Part 7: Chinese Remainder Theorem.

① Let $m,n \in \mathbb{N}\setminus\{0\}$ and $\gcd(m,n)=1$, then $C_{mn} \cong C_m \times C_n$

(C_n means cyclic group of order n)

② $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if $\gcd(m,n)=1$

③ Solve equation: Find x s.t. $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$, $\gcd(m,n)=1$

1° Find u, v, s.t. $mu+nv=1$

2° $t = bmu + anv$ is the solution.

$x \equiv 3 \pmod 8$

$x \equiv 1 \pmod{15}$

$x \equiv 11 \pmod{20}$

$1 \quad x \quad x^2 \quad x^3$

$$x \equiv 11 \pmod{20} \Rightarrow \begin{cases} x \equiv 11 \pmod 4 \\ x \equiv 11 \pmod 5 \end{cases} \Rightarrow \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 5 \end{cases}$$

$$x \equiv 1 \pmod{15} \Rightarrow \begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \end{cases}$$

$$\begin{cases} x \equiv 3 \pmod 8 \\ x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \end{cases} \qquad \begin{cases} x \equiv 3 \pmod 8 \\ x = 1 \pmod{15} \end{cases}$$

$$\begin{cases} x = 8z + 3 \\ x = 15y + 1 \end{cases} \qquad \underline{8z + 3 = 15y + 1}$$

$15y - 8z = 2 \quad \gcd(8, 15) = 1 \quad 15y' - 8z' = 1 \quad y = 2y', z = 2z'$

$y' = -1 \quad z' = -2 \quad$ So $\begin{cases} y = -2 \\ z = -4 \end{cases}$

$x = 15y + 1 = -29$

$x \equiv -29 \pmod{15 \times 8} = -29 \pmod{120}$

Part 8: RSA

Condition

① $n = p_1 \cdot p_2$ (p_1, p_2 are different primes)

② select arbitrary E st $\gcd(E, \varphi(n)) = 1$

③ Publish key (n, E)

Compute ① Private key D st $D = E^{-1} (\mod \varphi(n))$ or $D\underline{E} = 1 (\mod \varphi(n))$

③ Decrypt message $x = d(y) = y^D (\mod n)$

② Encrypt message x: $y = x^E (\mod n)$

Condition $n = 2077$, $E = 97$ $2077 = 31 \times 67$ $p_1 = 31$, $p_2 = 67$

(i) $D\underline{E} = 1 (\mod \varphi(n))$ $\varphi(n) = \varphi(p_1) \cdot \varphi(p_2) = (31-1) \times (67-1)$

$= 1980$

$D \cdot 97 \equiv 1 (\mod 1980)$ $D \cdot 97 - 1980 \cdot k = 1$

$D \cdot 97 - 1980 k = 1$

$1980 = 97 \times 20 + 40$

$97 = 40 \times 2 + 17$

$40 = 17 \times 2 + 6$

$17 = 6 \times 2 + 5$

$6 = 5 \times 1 + 1$

$1 = 6 - 5 \times 1$

$= 6 - (17 - 6 \times 2) \times 1$

$\vdots$

$1 = 1980 \times 17 - 97 \times 347$

$k = -17$ $D = -347$

$D \equiv 1633 (\mod 1980)$

(ii) $x = d(y) = y^D \pmod n$

$D = 1633$, $y = 279$, $x = 279^{1633} \pmod{2077}$

$1633 = 2^{10} + 2^9 + 2^6 + 2^5 + 2^0$

$x = 279^{2^{10}+2^9+2^6+\cdots 2^0} \pmod{2077}$

$= 279^{2^{10}} \cdot 279^{2^9} \cdots 279^{2^0}$

$x = k_1 \cdots k_5 \pmod n$

$279^{2^{10}} \equiv k_1 \pmod n$

$6x =$

3 mod.

$35x + 3 = 12y + 4$

$35x - 12y = 1$

FTTFTFTFFFFFTFFTT