Part 1: Prime numbers Definition: A Prime Number is divisible only by itself and 1. Notation of divide: dln Mersenne Prime: 2n-1 (Not all primes Mersenne) ie:15 Fermat numbers: 22 -1 (Not all Fermat numbers are prime) Proof There are infinitely many primes. For any finite set {p. pr}Cp, consider the number h=p. -- pr+1 Note that pith for all i=1-- r then either n is a prime or n has a divisor pa (p. pr), then either way a new prime is Practice $p \in |P|$, if $p|n^2+2$, then p=2 or p=1 or $3 \pmod{8}$ Prove: infinitely many primes of the form 8mt3 mEIN (Hint if a = a'(mod n) b=b'(mod n), atb=a'tb'(mod n), ab=a'b'(mod n)) Assume (p. - px) be finite set that contains all the primes in the form. N=n²+2 n=p...-pk if p doesn't exit, N is a new prime-By given theorem p=2 or p=1 or 3 (mod 8) of 8mt3, melly Since P.-Pr is in form 8mt3 So n2+2 is odd, so p +2. 1) Assume p'=1 (mod 8) for all plN , N=p'--- pr'

N= 1(mod 8)

p,2... p,2 = 1 (mod 8) N= 1+2=3(mod 8) (ontradicts! Not all PIN are in the form 8mt1. 3 There exists one p=8m+3. P. -- PKYN generate Part 2 : Greatest Common Divisor. Important Fact: O if mln then gcd (n,m)=m 3 There exists unique g and r (920, 05rem) so that n=gntr $\Psi \Theta \operatorname{gcd} \left(\frac{\alpha}{\operatorname{gcd}(k,d)}, \frac{k}{\operatorname{gcd}(k,d)} \right) = \prod_{m=g}^{\infty} \operatorname{gcd}(k,d), n = \frac{k}{m}, n = \frac{k}{m},$ gcd(n.,n2)=1 Op be prime, if plas, then pla or plb ♥ (6) If clab, gcd(b,c)=1, then cla Hint: To prove two numbers are equal alb and bla & a=b To prove dlk @ consider k=9d tr and prove r=0 @ Consider Lagrange Theorem

Since N=pi2p2-- Px+2, pi-fk=3(mod 8)

Practice: prove if a&G, |a|=d. if IK, such that ak=e then dlk (By using 0)

K= qd+r (0 < r < d) Then $a^k = e = a^{id+r} a^{id} \cdot a^r = e$

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

 $q^{d} = e \Rightarrow (q^{d})^{l} = e, \quad q^{r} = e, \quad r > 0 \text{ or } r = 0$ k=9d dlk.

* Euclidean Algorith & Diophantine Equation Euclidean Algorithm : used to find gcd(n,m)

Diophontine Equation: mx+ny=gcd(m,n), find x,y satisfy the equation. Practice: find x,y 5.1. 42823x +6409y=17=gcd(42823,6409)

Solution: 42823 = 6409 × 6 + 4369 Back tracking: 17=2080-289 × 7 6409 = 4369 >1 + 2040

= 6409 × 147 - 42823 x22. 4369 = 2040 x2 + 289 2040 = 289 ×7+17

x=-22, y=147 289 = 11×17+0

Part 3: Group Theorem

To prove G is a group:

O Closure: if aEG. bEG. Qob EG

@ Associative Composition (and) oc = Qo(boc)

3 Identity Element lexisits S.t. 1-9=0-1 = a for YOEG

@ For Yaeq, Ja'st aa'=1 Practice: Given a, bER, define Ta, b: R >R x+>ax+b

1 Closure

Ted. Tabe G, then Ted o Tabe G. Ted oTab = ((ax+b) + d = (ax+cb+d = Tea, cbrd Cx) & G where caer (rd*0)

@ Associative: axtb is associative > 0 composition associative.

3 Identity element Trdo Tab = (ax+(b+d = (x+d)

 $\begin{cases} c = (a) \Rightarrow \begin{cases} a=1 \\ c=0 \end{cases}$

Tho (x), identity element for G. Tho(x) = e.

(4) Inverse $T_{c,d} \circ T_{a,b}(x) = T_{1,o}(x) = x = (ax+cb+d)$ $\begin{cases} ac=1 & c=\overline{a}, d=-\overline{a} \\ (b+1)=0 & T_{a,b}(x)^{-1}=T_{\overline{a}}-\overline{a}(x) \end{cases}$

Theorem if S=az+bz, dz=az+bz, d=ra+sb 1 dla, dlb 2. If ela, elb then eld 3. d=gcd (a,b) Least common multiple mz = aznbz, m= low (a,b) Fout: d=grd(a,b), m=(cm(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 = e /x = d @ order of generator = order of cyclic group |x|= |<x>| 3|x|=n, $x^k=1$, then n|k, useful to prove n|k!

Important Inforems

O $|x| = n \in \mathbb{N} \setminus \{0\}$, $\langle x^k \rangle = \langle x^j \rangle$ O $|x| = n \in \mathbb{N} \setminus \{0\}$, $\langle x^k \rangle = \langle x^j \rangle$ O $|x| = n \in \mathbb{N} \setminus \{0\}$, $\langle x^k \rangle = \langle x^j \rangle$ O $|x| = n \in \mathbb{N} \setminus \{0\}$, $\langle x^k \rangle = \langle x^j \rangle$ O $|x| = n \in \mathbb{N} \setminus \{0\}$, $\langle x^k \rangle = \langle x^j \rangle$ O $|x| = n \in \mathbb{N} \setminus \{0\}$, $\langle x^j \rangle = |x^j| \iff |$

Euler Torient Function Q(n)= | { \$ \$ \$ N | 9 \$ \$ \$ \$ \$ \$ | \$ \$ \$ \$ \$ \$ \$ \$ \$ for pelp, ((p)=p-1, ((pk)=pk-pk-1 Property Q(n) is multiplicative: $\ell(m_1, m_2) = \ell(m_1) \ell(m_2)$ if $gcd(m_1, m_2)=1$ For cyclic group: The number of element of order dis given by ((d). Part 5: Homomorphism Definition: Given groups G.G'f:G>G'st for all x,ytG $f(x \circ G') = f(x) \circ G' f(x)$ 1) Take care: operation of G(°G) and G'(°G') may be different. Property of homomorphism 1 for a, -- ak EG, f(a, -- ak) = f(a,) -- f(ak) 2 f(|g) = |g' 3. $f(a^{-1}) = f(a)^{-1}$ D Image of f: Inf= {xEG' / x=fa), af G} kernal of f: kerf= [a∈G |f(a)=|G']

3 Prove injective of homomorphism: iff kerf = {16} Isomorphism: f is bijective. Prove O kerf= {IG} 4) If f is Isomorphism then f' is also isomorphism. Cosets Oleft Coset aH= {g∈G|g=ah for some h∈H}. H≤G For coset aH a is a fixed element from G. 2 cosets are equivalence classes 3 Index: [G:H] is number of left roset of H in G. Pa (Ounting Formula: |G|= |H|· [G:H] 1 D Lagrange Theorem: 1H1 | 1G1 The order of H divides order of G. Practice: Give a, n=N and a,n>1 show that n/y(a^n-1) Thint: Order of $(z/mz)^{x}$ is $\varphi(m) (z/mz)^{x} = \{\bar{\alpha} \in z/nz \mid gcd(\alpha_{i}n)=1\}$ (m) m= a" -1 (a"-1) = | z/(a"-1)z| for \(d^{n}-1) $q \operatorname{cd}(a, a^n - 1) = 1 \Rightarrow a \in \mathbb{Z}/(a^{n-1})^2$ Then prove order of a, |a| = n, Since $a^{n-1}|a^{n-1}|$ So $a^n = |(mod a^n-1)|$ Also for ocxen ax \$ 1 (mod an-1) ax < an-1. 141/161,50--n/9(a'-1)

Normal Subgroup Definition: if for all a

N and g

G, gag

EN ① if f is homomorphism, then kerf ⊆ G ② Center: Z := {z ∈ G | zx = xz for all x ∈ G} center is normal 3 To prove normal subgroup: 1° prove subgroup (closure) 2° prove the following { 1.9Hg-1 = H for all g & G (2.9H=Hy for all 9&G Part 6 : Modular Arithmetic a mod operation property a=b(mod c) & d=e(mod c) Then a+d=b+e(mod c), ad=be(mod c) @ Fermat's Little Theorem: 1° QPT = 1 (mod p) if gcd (a,p)=1 pffrime, a&Z. 2° al = a(modp) if acz, p∈prine

@ Multiplicative Group $(z/nz)^{x} = \{\overline{a} \in z/nz \mid g(d(a,n)=1)\}$

◆: |(z/nz)* |= \((n)\) by definition of Euler Totient Function

4 Euler Theorem: if gcd (a, m) = 1, a (cm) = 1 (mod m)

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

Part 7: Chinese Remainder Theorem.

O Let m, n EN 1803 and gcd (m,n)=1, then Cm = (m x (n ((n means cyclic group of order n)

@ Z/mnz \ Z/mz x Z/nz if g (d (m,n)=).

3 Solve equation: Find x s.t. x=a(mad m), x=b(modn), gad(m,n)=

1° Find u. V, S.t. mu tnv=1 2° t-bmn tanv is the solution.

$$\begin{array}{ll}
X \equiv 3 \pmod{8} & | \times \times^{2} \times^{3} \\
X \equiv | \pmod{15} & | \times \equiv | \pmod{20} \\
X \equiv | \pmod{20} & | \times \equiv | \pmod{4} & \implies \times \equiv 3 \pmod{4}, \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} & | \times \equiv | \pmod{5}
\end{array}$$

$$\begin{array}{ll}
X \equiv | \pmod{5} & | \times \equiv 3 \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv 3 \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv 3 \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv 3 \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \times \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \pmod{5} \\
X \equiv | \pmod{5} \\
X \equiv | \pmod{5} & | \pmod{5} \\
X \equiv | \pmod{5}$$

$$x = 15y+1 = -29$$

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

Part 8: LSA Condition On=P. P. CP., P. are different primes) @ select arbitratry E st god (E. (cn))=1 Opublish key (n, E) Compute of Private key D st D= E (mod q(n)) or DE = ((mod Q(n))) Decrypt message x=dry) = y cmod n) @ Encrypt message x: y= x E (mod n) Condition n=2077, E=97 2077=31×67 p=31, p=6/ (i) DE = 1(mod ((n)) ((n)) ((p)) + ((p2) = (31-1) x (67-1) = 1780 D. 97= 1 (mod 1980) D. 97- 1980 · k=1 D. 97 - 1980 K=1 1= 6-5×1 =6-(17-6×2)×1 1980=97×20 +40 91= 40x2 +1? 1 = 1980 × 17-97 × 347 40 = 17x2 +6 17 = 6 x 2 + 5 k=-11 D= -341 6=5×1+1 D= 1633 (mod 1980)

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

 $D = 1633$, $y = 279$, $x = 279$ (mod 2071)
 $1633 = 2^{10} + 2^{1} + 2^{6} + 2^{5} + 2^{0}$
 $x = 279^{2^{10} + 2^{1} + 2^{6} + \cdots + 2^{0}} \pmod{2071}$

6x=

$$= 279^{2^{10}+2^{1}+2^{6}+\cdots} 2^{0} \pmod{2071}$$

$$= 279^{2^{10}} \cdot 279^{2^{10}} \cdot 279^{2^{10}} \cdot 279^{2^{10}}$$



o mod.

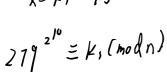
35x+3=124+4

35 x-134 =1

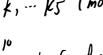


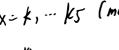


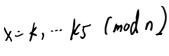
















FTTFTFTFFFFTFFTT