Thursday October 3

Bornole: Consider $f(x) = x^r - x$.

The "converse" is the three for $f(x)$ (wi 1 Thursday, October 3 October 3 then $f(x)-g(x)=x(x-x+x-\frac{1}{6}x)h(x)$ $Example:$ Consider $f(y) = x^p - x$. \equiv $(\chi^p - \chi)$ h(x) (m)p). By Fernos's little theorem, every The "converse" is otro tries residue class (mod p) is a root of Theorem: Let Zp denote the set of $f(x)$ (mo) p). It follows that It follows that residue closes (mod p). Let $f(x) = x(x-1)(x-2) \cdots (x-(p-1)) g(x)$ The "converse" is stoo there!
Theorem: Let 2p denote the sot
residue classes (mod p). Let
f: 2p 3 2p be any function. - but g(x) must be the constant 1 more than there exists a unique polynom
he comparing degrees and Loading coefficients- a(x) (mod p) of degree at most p-1 $f(x) = x(x-1)(x-2) - (x-(p-1))$
but g(x) must be the constant 1 by comparing degrees and Loading coefficientssuch that $f(z) \equiv g(z)$ (modp) for S_{∞} comparing degrees and concerng everyone every ac Zp. Extra s ift: compose coefficients of χ' : $(m\sigma)$ p). The there exists a unique polynomial of uniqueness = Let g(x), h/x) be - $1 = (-1)^{p-1} (p-1)^{1} = (p-1)^{1} (mod p)$ two such polynomials. Then $g(x) = f(x) \in h(x)$ $(m\rightarrow p)$ for $\rightarrow h$ $\rightarrow e$ \mathbb{Z} ; so Same idea gives a stronger statement: $g(x) - h(x) \equiv 2x^p$ $g(X)-h(X)\equiv (x^p-X)h(X)$ (movp); $if f(a) \equiv g(a)$ lonoop) for every axL α
at $\mathbb Z$, by company degrees, we must have kX) is the zero polynomial-

Profest curstone:

(1) Note that for any ∞Z , Corollary (to Exemple): Suppose allowing
 $1 - (y-x)^{2-1} \leq \begin{cases} 0, & \text{if } y \neq x \text{ (mod p)} \\ 0, & \text{if } y \neq x \text{ (mod p)} \end{cases}$, a note (meat).
 b_3 Ferminds With the meature The total (1 Profs of existence: 1 Corollary (to Example): Suppose d/(p-1). rafs of existence:
(1) Note that for any sell , Then $X^{a}-1$ has exactly Note that for any $\geq \frac{Z}{Z}$, Then X^{d-1} has
 $1 - (u - x)^{p-1} \leq 5$, if $y \neq a$ (modp), d roots (modp). $(y - x)^{p-1} \equiv$ 50 , if $y \neq a$ (morp). Then $x^4 - 1$ has exactly
 50 , if $y \neq a$ (morp), d roots (morp).
 $1 \cdot 1$, if $y \neq a$ (morp). Presf \leq $M \leq$ have the factorization
 $1 \cdot 7$ has tobe $x^{p-1} - 1 = 2x^4 - 12(x^{p-1} + x^{p-1-2d} +$ by Ferrot's lite theorem. Then take Fernats little theorem. Then toke $x^{p-1} = (x^d-1)(x^{n-d}+x^{p-1-2d}+1)$
g(x) = $\sum_{x=0}^{p-1} (1-(x-x^2))f(x)$.
 $\sum_{x=0}^{p-1} f(x) = 0$ $g(x) = \sum_{x=0}^{x} (1 - (x - x)^{-1}) f(x)$.

(2) There are pr functions from Z_1 to By lost close, 11) has st most a
 Z_1 There are pr functions from Z_1 to By lost close, 11) has st most a Z_p . There are pr polymonists of the roots one (2) has at most (p-1-d) $F_{nm} = \frac{p-1}{2} q_2 x^k$ where $c_5 = \frac{50!}{3!} - \frac{p-1}{5}$ roots $(mn) = \frac{8pt}{3!} - \frac{1}{2}$ lmds $\sqrt{2}$ $x = 1$ mas B ut each such polynomial represents B B y counting, D and D must \int 40 and 40 must have their runting chy unghaness 5 their maximum number 1 roots. is represented by some polynomia-I $2P$, d roots (mod p).
 $2P$, P roof \leq $M \leq h$ are the foot
 $X^{p-1} = (\sqrt{x^d-1})(X^{p-1-d} + X^p - \sqrt{x^d + X^{d-1}})$.

By both close, (i) has st mot

roots and (2) has st mot

roots and (2) has st mot

roots (i) has st mot
 By both closes, $\frac{1}{10}$ has $\frac{1}{57}$

roots and $\frac{2}{2}$ has $\frac{1}{27}$ must conden $\frac{1}{2}$ and $\frac{1}{2}$ and $\frac{1}{2}$ and $\frac{1}{2}$ and $\frac{1}{2}$
By counting $\frac{1}{2}$ and $\frac{1}{2}$
By counting $\frac{1}{2}$ and \frac Order and primitive roots / 4

Proofs Let h be the order of a Consom). $Decoll: f f z^n = 1 (mod m)$ then $log m = 1$ Write $k=hq+r$ where $0\leqslant r < h$. Definition: Given Co, m) = 1, the Then $a^k = a^{hq+r} = (a^h)^q a^r$ (multiplicative) ander of a consol m) is the smallest KEIN such that $\equiv |^4a = 2$ (and m). $-\mathbb{f}$ $r = 0$, then $h \mid k$ and $s^{\text{th}} \equiv 1$ (mal m). $2^k \equiv 1 \pmod{m}$ \mathcal{F} \cap \circ , then h tk. Also $Expmplez$ $m=ll_0$ $z=3$. $\dot{s} \not\equiv |$ (mod m), because \cap is smaller k | 1 2 3 4 5 6 then h , the order of a . $3^{k} = 22$ (marr) 3 9 27 is iz 3 Proposition- let > have ader r (madin) and so the order of 3 (mod) is 5. Lemmes: Given $(a_0, m) = 1 : a^k \equiv 1 \pmod{m}$ t is the order of ab (mo) m), then frand only of the order of a (modm) $t|\frac{rs}{(r,s)}=|cm[rs],$ and
 $\frac{rs}{(r,s)^2}$;
 $t=\frac{rs}{s}$. then - In particular: the order of a Gurd m) shways divides alm?
Cay Euler's theorem.

Proposition- let > have add r (madin) $rlst$ C_{353} C_{153} t \iff + is the order of ab (mo) m), then $\frac{1}{55}$ + $\frac{1}{1}$ (since $\frac{1}{1}$ (since $\frac{1}{1}$ $\frac{5}{1}$) t $\frac{rs}{(rs)}$ = 1cm $\frac{rs}{(rs)^2}$) t . The symmetric assumed shows $\frac{3}{400}$ 12. Prof- Let's note that $(2b)^{\lfloor cnL^r, 5\rfloor} = (a^{r})^{\frac{5}{2}(r, s)} (b^{s})^{(r, s)}$ Since $(\frac{1}{4}, \frac{5}{4}, \frac{1}{5})$ we $=$ S/z_{5} $\left\lceil \frac{z_{5}}{2} \right\rceil$ $=$ $\left\lfloor \frac{z_{5}}{2} \right\rfloor$ conclude that $\overline{c_{153}}$ $\overline{c_{153}}$ / $\overline{c_{2}}$ by the previous lemme, Icm Ins] is a Lenns' If a has order h (mod m), multiple of t. V then the order of at (mol) m) Also,
 $a^{st} = a^{st}(b^{s})^{t} = (ab)^{t}$ = $(mabm);$ $e^{-\lambda t}$ Everyth: The order of a^2 (mod m)
equals $\begin{cases} h/2, & h/2 \\ h, & h/2 \end{cases}$ is ever. So r (the order of a) mest divide St by the pseulous lemmes But

Lemns' If a has order h (motion), Détinitions a is a primitive root then the order of at (mod m) Convor and if the order of & Consom equals $\frac{h}{(h_0 k_0)}$.
But: The Following statements short j=IN equats plm) Couhich 15 20 large 25 \vec{v} could be). Example: M=11. 4(m) = 10. se equivalent- $\frac{a}{c_{old}}$ 1 2 3 4 5 6 7 8 9 10

order 1 1 0 5 5 5 10 10 10 5 2

(mod ii) Thus 2, 6, 7,8 are all primative $(1)^{n} (a^{k})^{n} \equiv 1 (mod m)$ (2) $h \mid kj$
 (3) $\frac{h}{4j}$ \mid $\frac{k}{4j}$ j roots (mort 11). Nite: $\{2, 2, 2^3, \ldots, 2^{16}\}$ $\begin{array}{c|c|c|c|c|c|c} \hline \text{CD} & \text{L} & \text{J} &$ In particular, the smallest positive $=$ {2,4,8,5,10,9,7,3,6,1} integer j stisting (4) Low hence reduced residue system- (1) as well) $k = \frac{1}{\sqrt{2}} \frac{h}{4h}$.

 $\begin{array}{l} \underline{Lamm*}: \text{If } m \text{ has a primitive rate,} \\ \underline{Hm*}: \text{if } m \text{ has a positive rate,} \\ \underline{Pm*}: \text{if } m \text{ has a positive rate,} \\ \underline{Pm*}: \text{if } m \text{ is the positive rate,} \\ \underline{Pm*}: \text{if } m \text{ is the positive rate,} \\ \underline{Pm*}: \text{if } m \text{ is the positive rate,} \\ \underline{Pm*}: \text{if } m \text{ is the positive rate,} \\ \underline{Pm*}: \text{if } m \text{ is the positive rate,} \\ \underline{Pm*}: \text{if } m \text{ is the positive rate,} \\ \underline{Pm*$ 1 Lemmo: If m has a psimitik roo $\frac{1}{\sqrt{6}}$ then it has exactly to (them) primitive roots. Prof. Let g be a primitive root Consider. Prof. Let 9 be > primitive 1000 cmos m
Then 3 g, g?, ..., g#cm3 forms a By the previous lemmit, the order of reduced residue system (mod m)
By the previous Lemin, the order of
of 13 (4m) in portlands) the order of s^{μ} equals of the precisely the order of S^k equals $\phi(m)$ ps
when $(k, \not\approx m) = |x - x|$ therefore $\phi(\#m)$ such integers
 $1 \leq k \leq \phi(m)$. 4