The red one behavior in the basis of the set 1 Thursday, October 10 Note: 7  $4=2401 \equiv 1 \pmod{25}$ Thursday October 10<br>What do we know about<br>Your primitive roots?<br>- Group Wask Tues What do we know about which moduli  $18^4 \equiv C70^4 \equiv 1$  (mad 25). have primitive roots? Still, we observe! · Group Wask Tues ... Stall, we observe!<br>. every printive pool (mod 25)  $-$  m= $l<sub>j</sub>$ 2 ,  $15$  primitive root (mot 5) is well; - only other possibilities are: . most (but not old) lifts of the  $p^{\mathbf{k}}$ primitive roots (mors) sue also<br>primitive roots (mort 25). ph, 2ph for odd primes P primitive roots Cnots 25).<br>- Mini-lecture The: -primes <sup>p</sup>  $\omega$  have primitive needs  $f$ The Ingeneral. Today: look at p<sup>k</sup> for one p. -  $m = 1, 2, 4$  do have primitive ro<br>- only other possibilities are:<br>-  $M_i$  in lecture Time:<br>-  $M_i$  in lecture Time:<br>- primes p do have primitive<br>-  $\frac{1}{2}$  for only if  $\frac{1}{2}$ <br>Some data when  $p = 5$ .<br>- The p(p(s) = 2 pr  $\frac{1}{\pi}$  (p(p(s)) =2 primitive roots (mod 5) 33 . · The  $H(b(253) = 8$  primitive roots (mod 25)  $ose\{\frac{2}{3},\frac{3}{12},\frac{8}{13}\}\$  $3,17,22,28$  $\frac{12}{17}$ <br>17,  $\frac{1}{7}$  $D = 8$  $m$ isolas  $7$ , 18

Theology of  $\beta$  is  $\alpha$  primitive roof<br>
Comp  $\beta$  than  $\beta$  is  $\alpha$  primitive roof<br>
Comp  $\beta$  than  $\beta$  is also  $\alpha$  primitive of  $\alpha$ <br>
Contribution  $\beta$  is also  $\alpha$  primitive of  $\alpha$ <br>
Contribution  $\alpha$ <br>
Then  $\alpha^{k} - 1 =$ 1 Theorem: If g is > primitive root Lemme: If a has order h (mad m)  $L_{1}$  $(L_{2}$  ( $L_{3}$ ), then g is also a primitive and dim, and  $d|m_{0}|$  then the order of a (mode) Theorem: It g is > primitive root (sermo: It<br>(mod p<sup>2</sup>) then g is also o primitive and d m,<br>root (mod p). nost (un) p).<br>Starting doservation:  $Suppse a^{k} \in (mod p)$ . Prof: a has order h (mod m)  $\frac{1}{\sqrt{2}}\left(\frac{1}{2}n\pi\right)^{2}-\frac{1}{2}\left(\frac{1}{2}n\pi\right)^{2}-\frac{1}{2}\left(\frac{1}{2}n\pi\right)^{2}-\frac{1}{2}\left(\frac{1}{2}n\pi\right)^{2}$ <br>The  $a^{k}P-1=(a^{k}-1)(4a^{k})^{k}+a^{k}P^{2}+\frac{1}{2}\pi\right)^{k}=1$  (mod m)  $\Rightarrow$  a = 1 (unod m)<br>=> a = 1 (mor) d)  $\begin{array}{c} \n\cdot & \lambda^2 - 1 = L\lambda^{-1} \\
\cdot & \pm (L\lambda^2 + \lambda^2 + 1) \n\end{array}$ and look factors  $\Rightarrow$  h is a multiple of the order of Then  $a^{k}P - 1 = (a^{k} - 1)(4a^{k})$   $(a^{k})$   $b^{k}$ <br>...  $+(a^{k})^{2} + a^{k} + 1$  ; and looth factors<br>are multiples of  $P_1$  so  $a^{k} \equiv 1$  (ma)  $p^{2}$ .  $\alpha$  (mot d). Contropositive: if  $a^{k}P \neq 1$  (mot  $\beta^{2}$ ), then<br> $a^{k} \neq 1$  (mot  $\rho$ ). Proof of theorem: Suppose g is a primitive Starting deservation. Suppose<br>Then  $a^{k}P-1=(a^{k}-1)(la^{k})$ <br>are multiples of  $P_1$  as  $a^{k}$ <br>are multiples of  $P_1$  as  $a^{k}$ <br>and multiples of  $P_1$  as  $a^{k}$ <br> $a^{k} \neq 1$  (and  $p^{k}$ . Suppose  $a^{k}$ <br> $P_0$  as  $a^{k}$  and  $p^{k+1$ Proof of theorem: Suppose g is a primitive  $\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\right)^{2}$ , so g has soder  $\frac{1}{2}(\frac{1}{\sqrt{2}})^{2}$  = p(p).<br>Thus  $\frac{1}{3^{2}}$ ,  $\frac{2}{3^{3}}$ , -,  $\frac{1}{3}$ ,  $\frac{1}{3^{4}}$  = 1 (mod p<sup>2</sup>).  $B_{1}$  the observation,  $9.9^3 - 9^{p-2} = 1$ <br> $B_{1}$  the observation,  $9.9^3 - 9^{p-2} = 1$  $\overline{\mathcal{L}}$  $mod$  p), so g  $50$  $\sqrt{2}$ 

 $\begin{array}{ll} \frac{Proposition 2}{Proposition 2} & \text{if } g \text{ is a primitive unit} \\ \frac{Proposition 2}{Proposition 2} & \text{if } g \text{ is a primitive unit} \\ \frac{1}{2}p^2(1-p^2) \neq 1 \pmod{p^2}. \quad (*) & \text{if } g \text{ is a positive unit} \\ \frac{1}{2}p^2(1-p^2) \neq 1 \pmod{p^2}. \quad (*) & \text{if } g \text{ is a positive unit} \\ \frac{1}{2}p^2(1-p^2) \neq 1 \pmod{p^2}. \quad \frac{1}{2}p^2(1-p^2) \neq 1 \pmod{p^2$ 1 position:  $I = \frac{1}{2}$ Thus the order (modp<sup>or</sup>) nivot be  $LengthD$  with  $r=2,$  then  $erthv p^{r-2}(p-1)$  or  $p^{r-1}(p-1)$  $g^{p-2}(p-1) \neq |$  (med p<sup>r</sup>). (\*) (no intermediate divisors since  $\rho$  is prime. Moreover, it 3 is a primitive root Moreover, it s is a primitive root. But it cont be  $p^{n-2}(p-p)$  by  $(k)$ .<br>(mod  $p^{n-1}$ ) and (dr) holds, then then  $\overline{9}$ seaver, it is is a primitive root But it cont be  $p^{n-1}$  by (<br>is also a primitive root (mod  $p^{n}$ ). Theorem Primitive roots exist  $\frac{9!}{2!}$  is  $\frac{1}{2!}$  of  $\frac{1}{2!}$  be  $\frac{1}{2!}$  (word  $\frac{1}{2!}$ ) for every prime prime Theorem Primitive roots exist<br>Conor p<sup>2</sup>) for every prime p.  $then$  g  $\frac{1}{2}$ <br>has order  $\frac{d}{dt}$  $\left( p^2 \right) = p^{1-1} (p-1) > p^{1-2} (p-1)$ then  $g$  has add the  $\gamma$  (1-15 p 4 - Suppose  $g$  is  $p$  primitive root (mov)  $p^{r-1}$ ) au so CAS holds (definition & arder).<br>- Suppose g is a primitive root (mod p<sup>r.)</sup>.<br>and (d) holds. The order of g (mod p<sup>r</sup>):  $divides \phi(p') = p^{-1}(p-1)$  (Euler's thin) · divides  $\frac{p}{p}$  if  $\frac{p}{p-1}$  there:  $\bigcap$  $\begin{array}{l} \n\mathcal{P}(p+1) = p^2 \\ \n\mathcal{P}(p^2) = p^2 \\ \n\mathcal{P}(p^2) = p^2 \end{array}$ 

Proof: Us of the p institute of  $(mod p)$ .<br>
Neill show that of the p titles and it is p in and prime,<br>
extra  $\theta$  then  $\theta$  the p titles<br>
extra of them is sprimitive root (man)  $p$  (man)  $p$  (m i 22. Then<br>
extra of them is s 1 Proofs Let o Theorem: Let plue on oil prime, We'll show that of the p lifes our let o be o primitive root  $g + tp$  (modp<sup>2</sup>) (03-24p-1), sll but  $Conv2p^3$  for  $r22$ . Then are of them is  $\rho$  primitive root (mod  $\rho$ t)  $C$ <br> $C$ <br> $D$  is also a primitive root (mod  $\rho^{(t+1)}$ ). By Proposition ,  $\#$  suffices to show  $\n By Proposition, 72 with the following relation, we have to show that these functions are not always.$ Cosolbry: Let p be on ode prime. pointbe not<br>=2. Thes<br>be on edd prime. that there's a unique offer I such Any printive root (mod p<sup>2</sup>)  $(9 + 1 p)^{p-1}$  $H = 1$  (mod  $p^2$ ). (then)  $is$  a primitive root (mod  $p^k$ )  $(94 + 4)$ <br>Let  $f(x) = x^{p-1} -$ 1. Then g  $is$  toot for every lie M. of  $f(x)$  (mot p); and  $f'(g) = (p-1)g$ p-2  $700$  cms,  $150$  $is$  a nonsingular root. By Hensel's lemme, there is root By Hersel's lemme, the IS<br>|

Profit Theorem: Let  $S$  be  $>$  primitive<br>
rest (and  $p^c$ ). By Prepartion,<br>  $\frac{1}{2}p^c(2p^c-1)^2$ .  $\frac{1}{2}p^c(2p^c-1)^2$ .  $\frac{1}{2}p^c(2p^c-1)^2$ .<br>  $\frac{1}{2}p^c(2p^c-1)^2$ <br>  $\frac{1}{2}p^c(2p^c-1)^2$ <br>  $\frac{1}{2}p^c(2p^c-1)^2$ <br>  $\frac{1}{$ 1 Prof + Theorem: let 3 be a primitive 9 Prof  $x$  Theorem: let  $g_{bc}$  primitive  $g_{bc}^{p-1}(q-1) = (1 + np^{-1})^p$   $\frac{2np}{p} \times p_{bc}$ <br>root (mod  $p^2 - p$ ) By Proposition,  $\frac{p}{p} = \sum_{k=p}^{p} {p \choose k} (np^{-1})^k$ .  $\frac{2np}{p} \times p_{bc}$  $g^{p^{n-2}(p-1)} \neq l$  (mod  $p^{n}$ ); and we • When  $k \ge 3$  $k(r-i) \geq r+1$  (check):<br>-1)<sup>k</sup> 30 (mm) p<sup>r+1</sup>). ry<br>2<br>2  $9^{p^2+q-1} \not\equiv 1$  (me)<br>want to show (\*)  $s \in (l_{k})$  n  $(p^{r-1})^{u}$  so  $(nw)$   $p^{r+1}$ ).  $g^{p^{-1}(p-1)} \not\equiv |$  (anot  $g^{(b)}$ ), -<br>ት ·  $W$  en  $k=2, (2)^{n_{p}-1}$  = require  $\frac{5}{6}$  that  $\frac{5}{6}$ will be a primitive root (not of )  $P^+$ PASSES And \* Theoren: let g be > primitive<br>
root (and p<sup>r</sup>). By Proposition,<br>  $g^{p-2}(p-1) \neq 1$  (and p<sup>r</sup>), and we<br>
so that g will be > psimitive not (and p<sup>re)</sup>),<br>
so that g will be > psimitive not (and p<sup>re)</sup>)<br>
Now  $g^{p-1}(p-1)$   $k(r-1) \ge r+1$  (check)<br>  $(p^{r-1})^k \ge p$  (mod  $p^{r+1}$ )<br>  $(k \ge p)^n$  (mod  $p^{r+1}$ )<br>  $(k \ge p)^n$  (mod  $p^{r+1}$ )<br>  $n^2 p^{2(r-1)} = n^{\frac{p-1}{2}} p^{2r-1}$ )<br>  $\ge r+1$  (check). So  $m<sup>2</sup>$ by Ever's thm, Uner  $k=3, k=1, ..., k$ <br>
(p)  $n^{k}(p^{r-1})^{k} \equiv D$  (ma)<br>
When  $k=2, (\frac{3}{2})(np^{r-1})^{2} =$ <br>  $\sum_{r=1}^{n} (p^{r-1}p^{2}(p^{2(r-1)}) = p\frac{p-1}{2}p^{2(r-1)}$ <br>
(f)  $(n_{0}^{r-1})^{2} \equiv O$  (ma)  $p^{(t)}$ ).  $\begin{array}{lll} \Sigma_{2} & \Sigma_{1} & \Sigma_{2} & \Sigma_{1} & \Sigma$ Therefore  $Now$   $g^{p-2}(p-p) \equiv ($  (nood  $p^{r-1}$ ) by Eule's thing  $\beta^{\mathsf{P}}$  $\frac{c}{\gamma}$  $\mathcal{U}_{(n)} = \sum_{k=p}^{n} {p \choose k} (np^{n-k})^k$  $\int_{0}^{\infty} 1^{p^{n-2}(p-1)} = 1 + np^{n-1}$  for some  $\int_{0}^{\infty} 1 + p \cdot np^{n-1} = 1 + np^{n}$   $\Rightarrow$   $\int_{0}^{\infty} 1 + p \cdot np^{n-1} = 1 + np^{n}$   $\Rightarrow$   $\int_{0}^{\infty} 1 + p \cdot np^{n-1} = 1 + np^{n}$   $\Rightarrow$   $\int_{0}^{\infty} 1 + p \cdot np^{n-1} = 1 + np^{n}$   $\Rightarrow$   $\int_{0}^{\infty} 1 + p \cdot np^{n-1} =$  $p - p = 1 + np^c \nRightarrow (npq)^{(n)}$  $\infty$   $g^{p^{n-2}(p-1)} = 1 + np^{n-1}$  for some<br> $n \neq p$  (mot p). Then by the =  $1 + p \cdot np^{-1} = 1 + np^{2}$  =  $\Rightarrow p$ <br>Since  $n \neq D$  (mod  $p$ ). Thus (sk) holds,

Summary Principle rests exist<br>precisely for the 1,24 p<sup>2</sup>, 2<sup>p</sup> for structure of M<sub>m</sub> for any *in* 2;<br>precisely for the 1,24 p<sup>2</sup>, 2p<sup>2</sup> for structure of M<sub>m</sub> for any *n*<sup>2</sup>2;<br>contribute the precise of  $>$  lives p.<br>Exampl 1 Summary: Primitive roots exist We now know how to find the group precisely for m= 1,2  $\frac{1}{2}$ Summary: Primitive ruots exist We now know how to the g.<br>Dreekely for  $m=1,2,4, p^k, 2p^k$  for structure of  $M_m$  for any  $m=2$ : od primes p. · Chinese remainder theosen - + Exercise Let please. Show that it  $m = p_1^{\prime\prime}p_2^{\prime\prime} \cdots p_{\nu}^{\prime\prime}$ , then Exercise Let phease. Show that if  $L$  m= p<sup>1</sup>.<br>
(s, 2pk), then the coder of  $\delta$  (mod 2pk) Mm = p<sup>1</sup>.  $M_m \cong M_{p_1^{\rho_1}} \times M_{p_2^{\rho_2}} \times \cdots \times M_{p_{k}^{\rho_{k}}}$ . In particular, since  $t(2p^k) = t(2p^k)$ . If p is old, then primitive roads  $=$   $#(p^k)$ , every primitive root (mod  $p^k$ )  $exist$  (mov  $p^2$ ); so  $M_{pk} \cong C_{pkp^k}$ ) = 4(p2), every primitive root und pe Graph), then the order<br>equats the order of a<br>In posticular, since the<br>= 4(p<sup>2</sup>), every primit<br>is also a primitive rate<br>Grapheary formulation?<br>. Comptheary formulation? Group theory formulation. Let When  $p=2$  $\overline{\phantom{0}}$  $E=\int_{0}^{\infty}e^{k-1}(p-1).$ · . Cm be the cyclic group of order m La complette residue system (mot m), under + undert)  $M_{jk} \in \begin{cases} C_1, & \text{if } k=1, \\ C_2, & \text{if } k=2, \\ C_{k-2} \times C_{k-1} \end{cases}$ ·  $M_m$  be the "multiplicative group" (modm):  $C_{2}xC_{2}$   $P E 3$ reduced residue system (modin), under  $x$ . yunne<br>o<sup>n</sup> (modm)<br>under X.  $(sine \notin m)$ ,

- 1 Lemmin: Suppose m has primitive ractis The number of solutions to this<br>and  $G$ , m) =1. The number of solutions like a conservence is known Lemms: Suppose in hus primitive roots<br>and Co,m) = 1. The number of solutions The number of solutions to this<br>likes congruence is known of  $x^n \equiv a$  (mod m) equals<br> $\leq d$ , if  $a^{t(m)/d} \equiv 1$  (mod m), Suppose in list primitive roots The number of solutions 7.<br>  $m$ ) = 1. The number of solutions likes congruence is limited theorem.<br>  $a_3$  of a other d = \ (number), from an earlier theorem.  $x^n \equiv x$  (mod m) equals these can careful is known<br> $\begin{array}{ccc} x^n \equiv x & \text{(mod m)} \\ y^n \equiv x & \text{(mod m)} \\ \text{(mod m)} & \text{(mod m)} \end{array}$  from an earlier theorem. 10, otherwise,  $S$ pecial  $\sigma$ se n $\epsilon_2$ , map old; where  $d = (n, 4/m)$ .  $Cosech 2$  cose:  $f(n, 0) = 1$  then thes Eules coterions Suppose  $p A$ . always exactly 1 solution) The number of solutions of Indis exactly 1 solution.)<br>Prof: Let o be a primitive root (mod m),  $X = 8$  (mm)  $P = X$ and with  $a \equiv \beta^b$  (mod m) and  $X = g$ \*  $(mabn)$   $3\overline{}$  $(1000)$ <br> $(1000)$ <br> $(1000)$ <br> $(1000)$  $= 1$  (modp), and write  $a \equiv a^{b} \pmod{m}$  and  $x = a^{b} \pmod{m}$ .  $\begin{cases} 2, & \text{if } a^{(p-1)/2} \equiv 1 \pmod{p} \ 0, & \text{if } a^{(p-1)/2} \equiv -1 \pmod{p} \end{cases}$  $(L\leq Y\leq t(n))$ . The  $\chi^4\geq G^4$  of  $\chi^4\geq G^5$  (mod m)  $x^{\frac{1}{2}} \geq (w\omega) \approx (8^1) = 8$ <br>  $\Rightarrow y^{\frac{1}{2}} = 1 \quad (w\omega) \approx (8^1) = 9$   $\Rightarrow y^{\frac{1}{2}} = 0 \quad (w\omega) \approx 1$   $\Rightarrow y^{\frac{1}{2}} = 0 \quad (w\omega) \approx 1$   $\Rightarrow y^{\frac{1}{2}} = 0 \quad (w\omega) \approx 1$   $\Rightarrow y^{\frac{1}{2}} = 0 \quad (w\omega) \approx 1$  $m b = 1$  (und  $m$ )  $\Leftrightarrow$   $\frac{1}{m} b = 0$  (und  $\frac{1}{m}$ )  $\Leftrightarrow$   $\frac{1}{2}$   $\L$ Fernats of  $8-1/2=1$  (map).