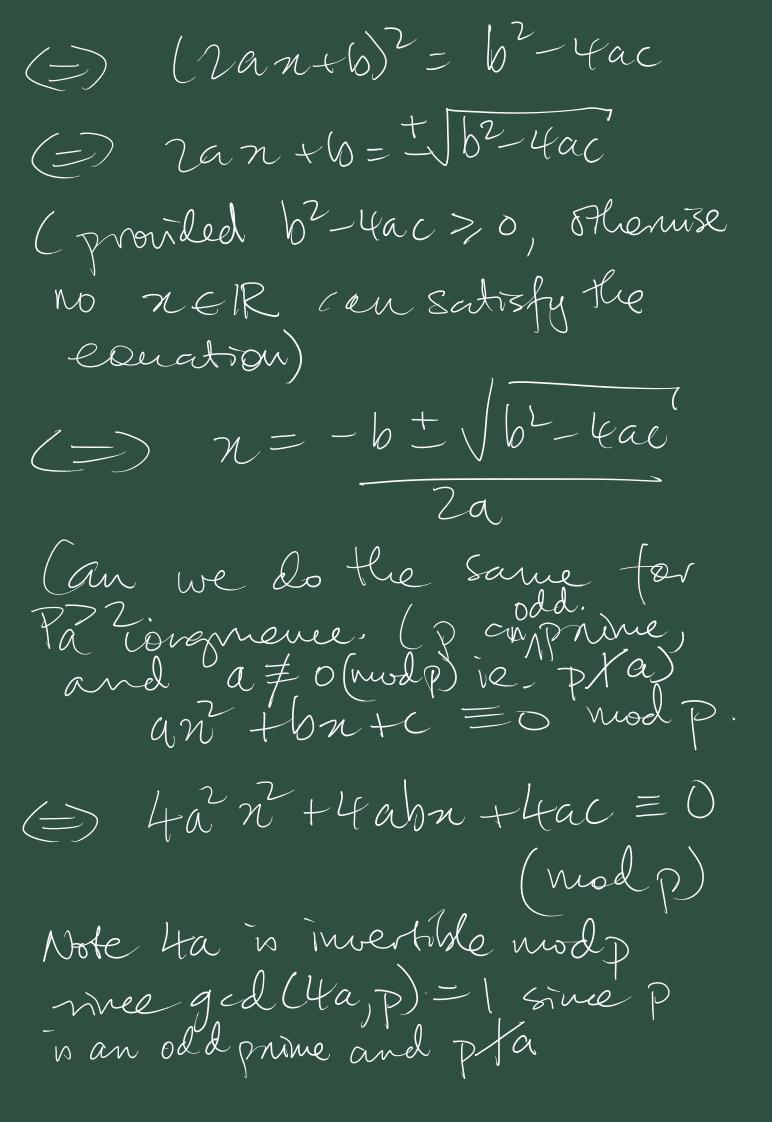
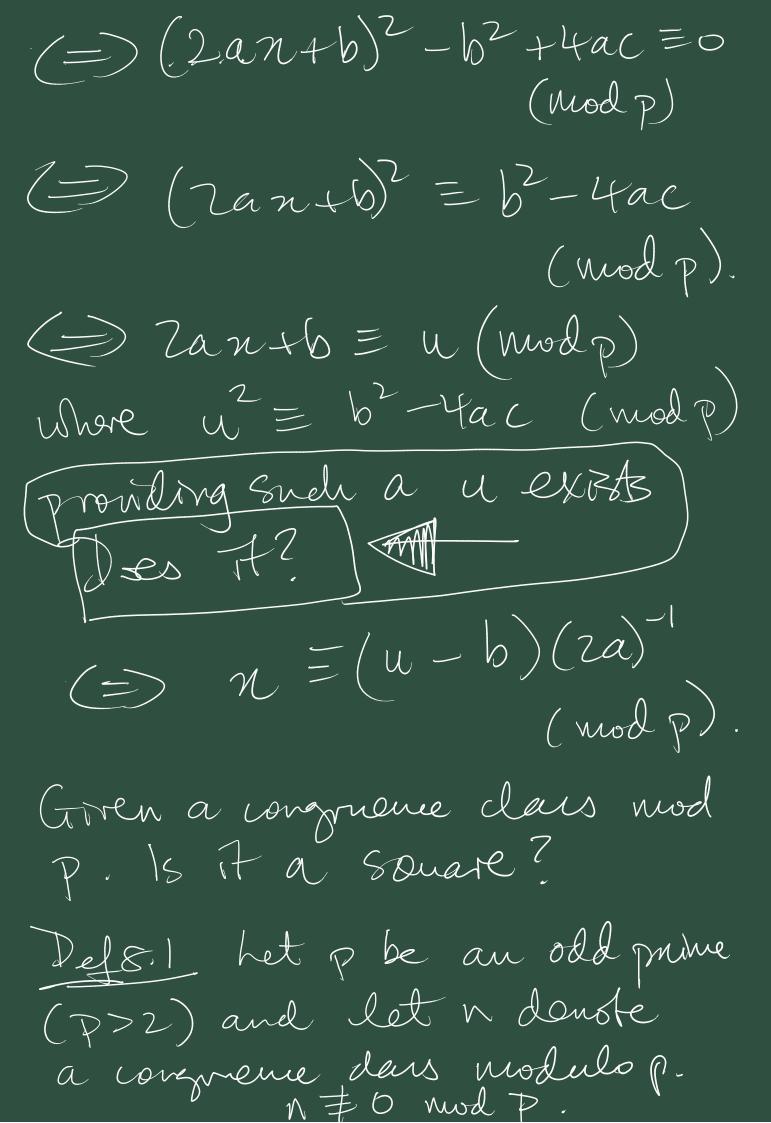
Quadratic Résidues
Concept à souare roots in resdula
antlinetic.
Couriler soluting a Quadratic
Counter solving a anadratic
antbut c = 0.
my the well-known anadratio
Joundar.  N = -6 ± Jb²-4ac
Za
provided that 62-4ac >0
Proof (arruning a to)
antbn+c=o
(=) Harn + 4abn + 4ac =0
$(=) (2au+b)^2 - b^2 + 4ac = 0$

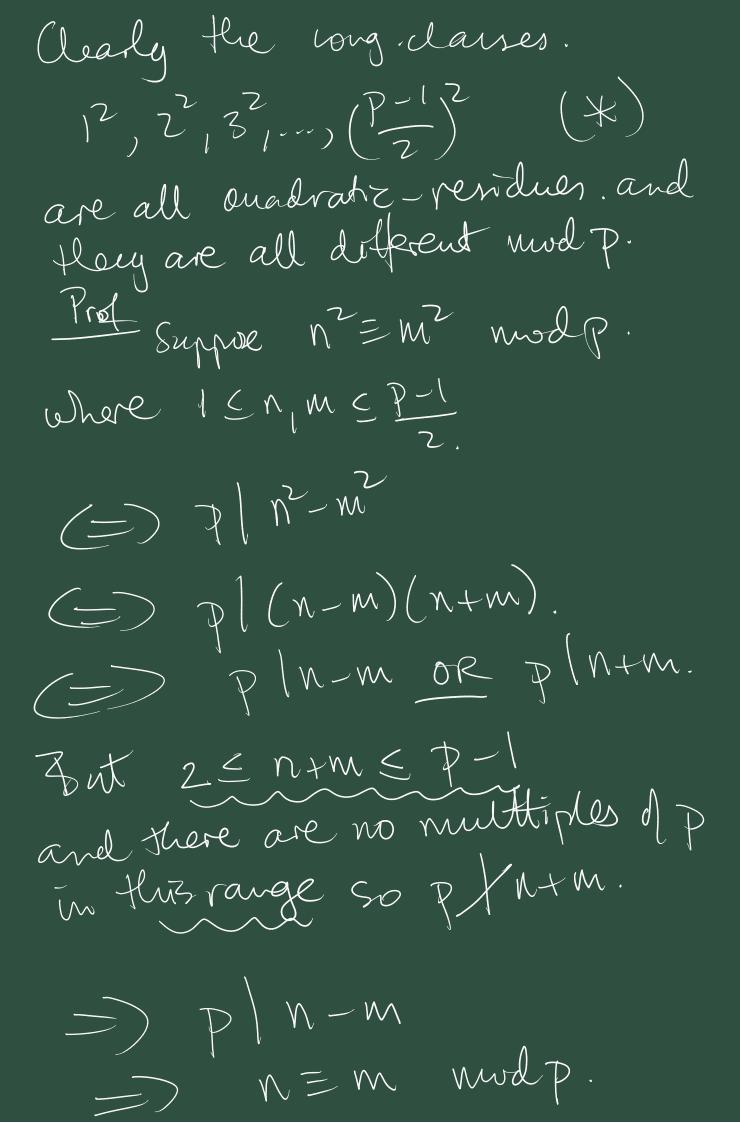




We say n'in a say Quadratiz rundulo p. It there are Solutions to NEN (mudp) n n a Buadvatic non-résidue If There are no solutious to  $n^2 \equiv N \pmod{p}$ . We seek to understand revidues. Examples. What are the residues mud p? n = (1), (2), 3, (4), 5, 6 $1 = 12 \quad 3^2 = 2 \quad 4 = 2^2 \quad (\text{mod } 7).$ So 1,2,4 are residues mod 7

while 3,5,6 are non-regidues mod 7. From Kirs and other examples. Conjedire. For mod p, there are Jan eoual number P-1 8 résidues and non-residues. Observation If m in a somare integer in the usual senese eg. m=1,4,9,16,... Hon m uill be a Quadratir residie mod p. The main lengtion remains. (ls na residue mod p?) Theorem 8.1 There are 7-1 residues and non-regidues mod P.

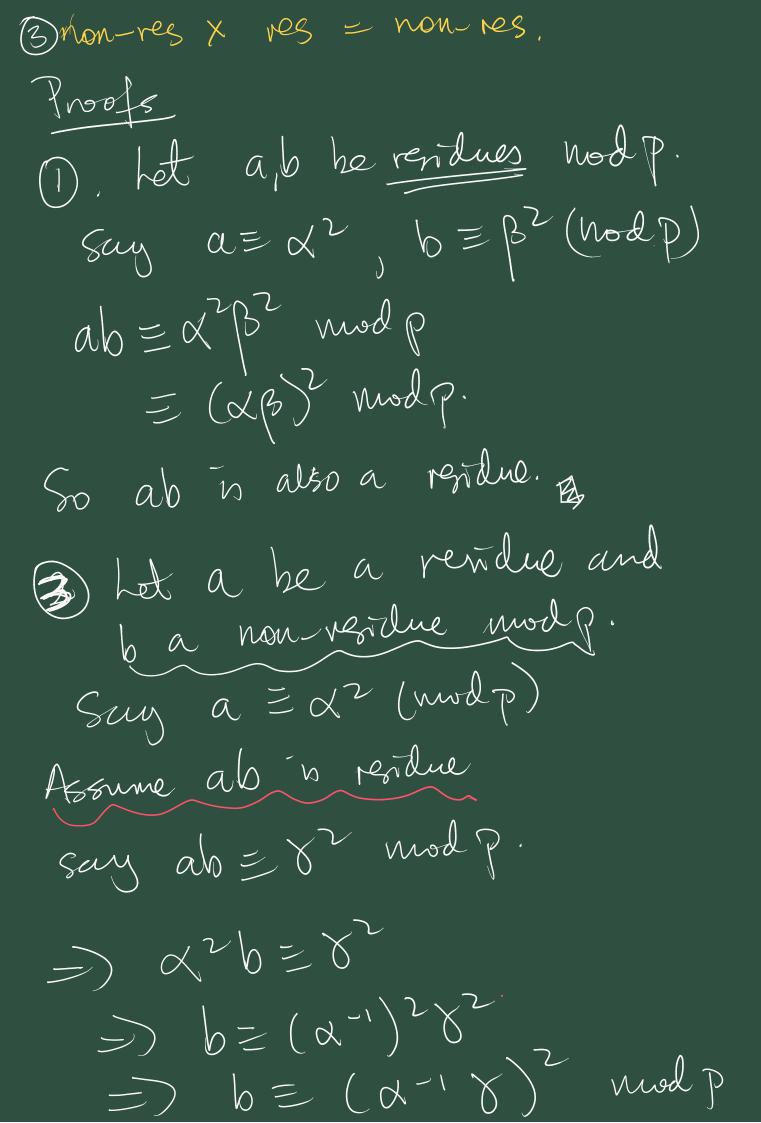
Proof Zp = {1,2,..., P-1}.

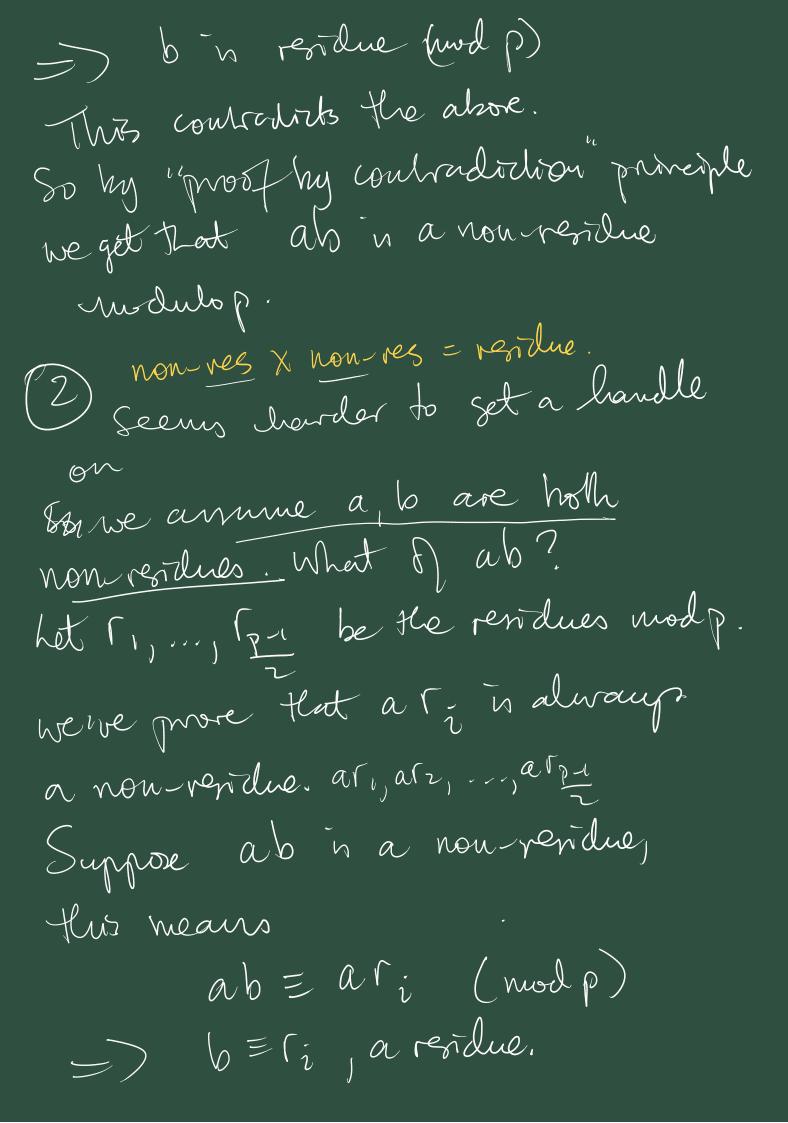


= N=MSo there a least P1 vendues (ree the lost at (x)) Moreover (x) lists all the Konresidues. For suppose j's a repidue with PHI E j E PII. But than i= P-j and 15 15 Pol and  $B_{j} = -i \pmod{p}$ . and so je = 2 (mod p)
and so je already listed m (X)

This proves here are exactly Pt residues mad p and by Implication flore are also P-1 non residues mod of In our mohration we connected the ideas of positive negatives. and having / bant-houng Bridge / non-regidue. a souare root. Now in The Hore in no innediate concept of positive/negative. But we can salvage something. 705/ vegs. behave very systematically under multiplication. 705 × rog= rog pos x pos = pos, reg x reg = pos

Consider an example. Suy modulo P=71. og. 44,46 are holl non residues. 44.46 = 36 mod 71 = 62 Which is a residue 62,63 are non-verduer. 62-63 = 1 mod 71 and In a residul. 38 ha revolve, 47 ha non-revolve 38.47 = 11 md71 which is a non-residue and 40.31 = 33 (mod 71) a non-revolue 24.25 = 32 (mod 71) a residue. So from nepeding examples we can form a conjecture. O res x res = res Oronnes x nonnes = res.





Bout this combradids the feely arruphon that b is a non-residue. ab muit be a residue So therefore vodulo P. Def6.2 Legendre Symbol. Ne define a symbol/notation for n modulo p to indicate whether or not n'in a anadratic regidue. (n/p) = { -1, if nina res.} med P. So 29. (117)=(217)=(417)=+1 (3)7)=(517)=(6)7)=-1Notice that our mosts of the conjectures ou hou revolues /non-revolues

multiply, tells us that (. 17) na multiplicative fernelion of the first a gument. Namelly. (nm|p) = (n|p)(m|p).So let's try and extruit the values for (n/p) haved on the prime feutoriration 1. n= nai for distruct primes.  $= \prod \left( q_i | p \right)$ ) my multiplicative prop.

= <del>|</del> (9i|P) So general problem of deciding In in a residue mod p reduces to the problem of underlanding whether a prime q'n a residue modulo another prime P. Quadrahr Reignouty is a governing principle over the annes to (g/P). act nove unight into evaluating Recall Termetts Littlee Theorem. nP= ( mod P. for n e Zp. ie. n to mod p.

 $\left(=\right) \left(\sqrt{\frac{p-1}{2}}\right)^2 = 1$ (mod p) So NZ na solution to X2 = [ modp. ie.  $X = -1, \pm 1 \mod P$ . the ody two solutions by hagranges theorem from chapter 7.  $= \sum_{n=1}^{\infty} \sum_$ (mod p). 18 Huz connected to (n/p)?? In fact they're the same.  $(np) \equiv n^{\frac{1}{2}} \pmod{p}$ . Thosem 8.4. (Eulers Criterion) 1 vol Assume (n/p)=+1 1e. n'h a Duadratiz regidue mod?

Te. N = u2 (mod p) for rone u. But now.  $N^{\frac{p-1}{2}} = (N^2)^{\frac{p-1}{2}}$ ( mod p). こ ルアー Etl (mod p) hy FLT. So  $(N|P) \equiv N^{-1}$  in this case. Secontly, arrune (np)=-1)
ie. n'is a nonverdue mod P. Let (,..., P-1 he the residues mod?. Here are all volutions to nt = + ( (mod p)
and by Lagrange's theorem there are all the solutions. => n== # +1 (mod p) =  $\sqrt{72} = -1 \pmod{p}$ 

So again in this case (n/p) and n7% holh agree modulo P. So overall  $(N|P) \equiv N^{-1} \pmod{p}$ Two applications.

()  $(-1|P) = (-1)^{P-1}$  (mod P) hy Euler's criterion.

= \( \frac{1}{14} \) \( \frac{1}{2} \) \( \text{is even.} \)

= \( \frac{1}{14} \) \( \frac{1}{2} \) \( \text{is odd.} \)  $=\int +1$ , P-1=0 mod  $\Psi$ . -1, 7-1=2 nod 4. (-1|P). =  $\{-1\}$ , P = 1 mod  $\{4\}$ .

Enter's contenon also ourthy settles.

(2/p)

(an show  $(2/p) = \begin{cases} +1, & p = 1,7 \text{ mod } 8 \end{cases}$   $(2/p) = \begin{cases} -1, & p = 3,5 \text{ mod } 8 \end{cases}$ 

