

claim: f: Z/pZ => Z/pZ

IS a bijection

Widea: show it's injective, since an
injection from a set to itself is a
finite

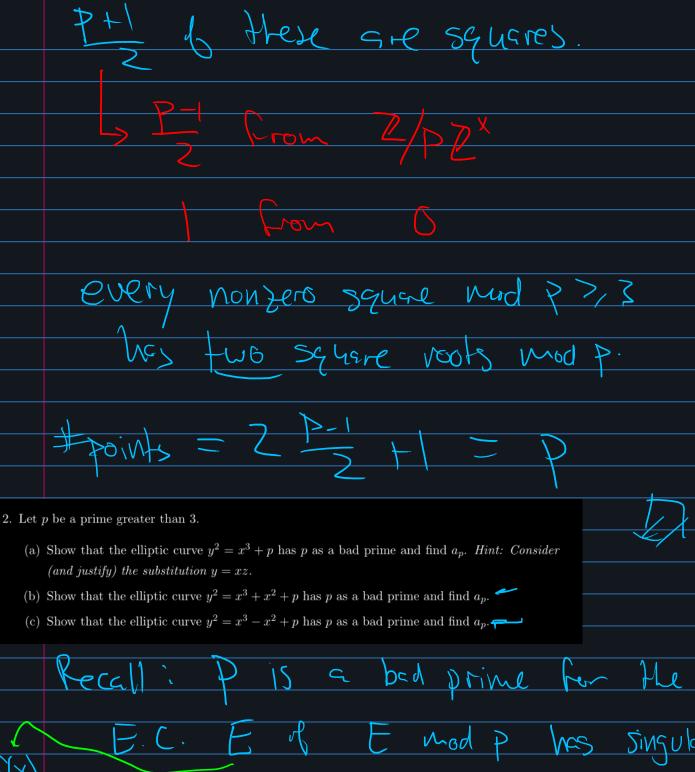
Subjection.

XHON OHOO & X5=0 mod ?

Pour about on Z/77

Let 9 be a primitive root mod ?.

List 3 be a primitive root mod ?.



Recall: P is a bad prime for the

E.C. E of E mod P has singular

Points, re. of f(x) has a reparted root

Mod P.

C)
$$\sqrt{2} = \chi^3 + p = \chi^3$$
 mod p

A triple real at zero.

This could be prime for this curve.

Op = P-Np

Solution on E mod p

(xz)² = x³ mod p

(xz)² = x³ mod p

(xz)² = x³ mod p

Solution come from letting z range over

Ppz set x = z², y = z³

Heal cre c|| different from each other.

The cre c|| different from each other.