Problems are on Canvas.

Work together until ~3:20

1. Let p be a prime with $p \not\equiv 1 \pmod 5$. Prove that the equation $y^2 = x^5 + 1$ has exactly p solutions modulo p.

RHS: $x^5 + 1 \bmod p$

claim: $f: \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is a bijection

idea: show it's injective, since an injection from a set to itself (finite) is a surjection.

$x \mapsto x^5$ $\quad 0 \mapsto 0$ & $x^5 \equiv 0 \bmod p \Rightarrow x \equiv 0$.

how about on $\mathbb{Z}/p\mathbb{Z}^\times$?

Let g be a primitive root mod p.

($f: S \to S$ is injective $\Leftrightarrow$ surjective, $|S| < \infty$)

write $x = g^y$ for some y.

$x \mapsto x^5 \iff g^y \mapsto g^{5y}$

if $g^{5y} \equiv g^{5z} \mod p$

$\iff \bar{5}y \equiv \bar{5}z \mod \mathrm{ord}(g) = p-1$

$\iff 5(y-z) \equiv 0 \mod p-1$

$\iff y - z \equiv 0 \mod p-1$

since $p \not\equiv 1 \mod \bar{5} \iff p-1 \not\equiv 0 \mod \bar{5}$

$\iff \bar{5} \nmid p-1 \iff \gcd(5, p-1) = 1$

$\Rightarrow x \mapsto x^5$ is injective on $\mathbb{Z}/p\mathbb{Z}^\times$

$\Rightarrow$ it's surjective too.

$\Rightarrow x \mapsto x^5$ is a bijection $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$

$\Rightarrow x \mapsto x^5 + 1$ is a bijection too.

$y^2 = x^5 + 1 \mod p$

RHS ranges over all of $\mathbb{Z}/p\mathbb{Z}$.

$\frac{p+1}{2}$ of these are squares.

↳ $\frac{p-1}{2}$ from $\mathbb{Z}/p\mathbb{Z}^\times$

1 from 0

every nonzero square mod $p \geq 3$ has two square roots mod p.

$$\#\text{points} = 2\frac{p-1}{2} + 1 = p$$

2. Let p be a prime greater than 3.

(a) Show that the elliptic curve $y^2 = x^3 + p$ has p as a bad prime and find a_p. *Hint: Consider (and justify) the substitution* $y = xz$.

(b) Show that the elliptic curve $y^2 = x^3 + x^2 + p$ has p as a bad prime and find a_p.

(c) Show that the elliptic curve $y^2 = x^3 - x^2 + p$ has p as a bad prime and find a_p.

Recall: p is a bad prime for the E.C. E if E mod p has singular points, ie. if $f(x)$ has a repeated root mod p.

$y^2 = f(x)$

c) $y^2 = x^3 + p \equiv x^3 \mod p$

↑ triple root at zero.

$\Rightarrow$ p is a bad prime for this curve.

$a_p = p - N_p$

$\hookrightarrow$ # points on E mod p

Find N_p for $y^2 \equiv x^3 \mod p$

Hint: consider $y = xz$

$(xz)^2 \equiv x^3 \mod p$

$\overset{x \neq 0}{\Longleftrightarrow}$ $x^2 z^2 \equiv x^3 \mod p$

$\Longleftrightarrow$ $z^2 \equiv x \mod p$

Solutions come from letting z range over $\mathbb{Z}/p\mathbb{Z}$ set $x = z^2$, $y = z^3$

These are all different from each other.

$\Rightarrow$ $x = z^2 = (-z)^2$ $\Rightarrow$ p points.

$z^3 \neq (-z)^3 = -z^3$ $\Rightarrow a_p = 0$

$\lightning$

□