44.2. Exercise 42.2(c) says that the elliptic curve $E : y^2 = x^3 - x$ has a torsion collection T $\{(0,0), (1,0), (-1,0)\}$ containing three points.

(a) Find the number of points on E modulo p for $p = 2, 3, 5, 7, 11$. Which ones satisfy $N_p \equiv 3 \pmod 4$?

(b) Find the solutions to E modulo 11, other than the solutions in the torsion collection, and group them into bundles of four solutions each by drawing lines through the points in the torsion collection.

say $P \in E_{11}$, $P \notin T$

look at $P + Q_i$, $\forall Q_i \in T$

ie, look at where the line $\{PQ_i\}$ intersects E

$y^2 = x^3 - x \mod 11$

$S = \{\text{squares mod } 11\}$

$= \{0, 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 = 5$

$5^2 = 25 = 3, 6^2 = (-5)^2 = 3 \ldots\}$

$= \{0, 1, 3, 4, 5, 9\}$

$0 : 0^3 - 0 = 0 = 0^2 \checkmark \Rightarrow (0,0)$

$1 : 1^3 - 1 = 0 = 0^2 \checkmark \Rightarrow (1,0)$

$2: 2^3 - 2 = 6 \notin S$

$3: 3^3 - 3 = 24 = 2 \notin S$

$4: 4^3 - 4 = 60 = 5 = 4^2 \Rightarrow (4,4), (4,7)$

$5: 5^3 - 5 = 120 = 10 \notin S$

$6: (-5)^3 - (-5) = -125 + 5 = -120 = -10 = 1$

note $(-x)^3 - (-x) = -(x^3 - x)$!

$(6,1), (6,10)$

$7 = -4: (-4)^3 - (-4) = -60 = -5 = 6$

$8 = -3: (-3)^3 - (-3) = -24 = -2 = 9$

$\Rightarrow (8,3), (8,8)$

$9 = -2: (-2)^3 - (-2) = -8 + 2 = -6$
$= 5$

$\Rightarrow (9,4), (9,7)$

$10 = -1 \quad (-1)^3 - (-1) = 0$

$\Rightarrow (10,0)$

6

look at $(9,4)$ connect this to each point in T, find the intersection.

- connect $(9,4)$ to $(0,0)$

line from $(0,0)$ to $(9,4)$: $y = \frac{9}{4}x$

$m = 9/4$ $\qquad\equiv 3x$

$4^{-1} \bmod 11 \equiv 3$

find where $y = 3x$ intersects E

$y^2 =_{11} x^3 - x$

$(3x)^2 = 9x^2$

$\Rightarrow 0 = x^3 - 9x^2 - x$

Sum of the roots to $= 9$

$\Rightarrow 0 + 9 + x_3 = 9$

$\Longrightarrow x_3 = 0$

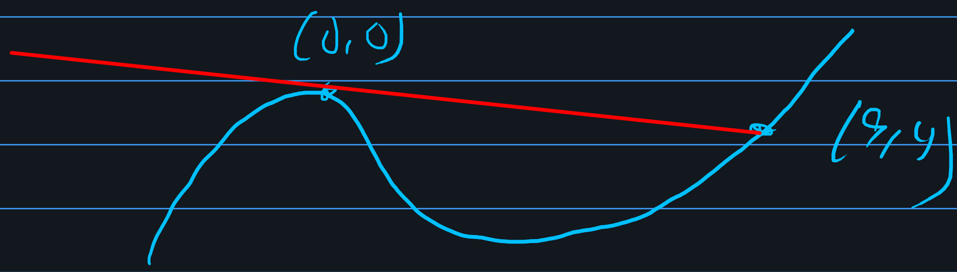
$\Rightarrow y_3^2 = 0^3 - 0 = 0 \Longrightarrow y_3 = 0$

$\Rightarrow$ points of intersection are $\{(0,0), (9,0), (9,4)\}$

R

$(0,0)$ shows up twice

$\Rightarrow$ line thru $(0,0)$ & $(9,4)$ is <u>tangent</u> to E at $(0,0)$



Consider: $x^3+ax^2+bx+c=0$

$$\parallel$$

$$(x-r_1)(x-r_2)(x-r_3)$$

$$\parallel$$

$$x^3+\underline{(-r_1-r_2-r_3)}x^2+\cdots$$

$$-(r_1+r_2+r_3)x^2$$

Connect $(9,4)$ to $(1,0)$

$\Rightarrow$ get new point R_2

$$\{(9,4),\ \underset{R_1}{(0,0)},\ R_2,\ R_3\}$$

The set $\{\underline{(0,0), (1,0), (-1,0)}, \mathcal{O}\}$ = T

$\mathcal{O}$ point at ∞, the identity element

is a subgroup of E

we just computed the coset

$\underline{(9,4) + T}$.

42.4. This exercise guides you in proving that the elliptic curve

$$E : y^2 = x^3 + 7$$

has no solutions in integers x and y. (This special case of Siegel's Theorem was originally proven by V.A. Lebesgue in 1869.)

(a) Suppose that (x, y) is a solution in integers. Show that x must be odd.

(b) Show that $y^2 + 1 = (x + 2)(x^2 - 2x + 4)$.

(c) Show that $x^2 - 2x + 4$ must be congruent to 3 modulo 4. Explain why $x^2 - 2x + 4$ must be divisible by some prime q satisfying $q \equiv 3 \pmod 4$.

(d) Reduce the original equation $y^2 = x^3 + 7$ modulo q, and use the resulting congruence to show that -1 is a quadratic residue modulo q. Explain why this is impossible, thereby proving that $y^2 = x^3 + 7$ has no solutions in integers.

a) say $y^2 = x^3 + 7$

mod 4: $y^2 = x^3 + 3$ $\equiv 3$ (if x even)

if x is even, $x^3 \equiv 0 \bmod 4$

no solns $\Rightarrow x$ not even!

44.1. Suppose that the elliptic curve E has a torsion collection consisting of the t points $P_1, P_2, \ldots, P_t$. Explain why the number of solutions to E modulo p should satisfy

$$N_p \equiv t \pmod{t+1}.$$

T (Think cosets)

If $Q \notin T$, $\tilde{Q}$

look at the "bundle",

$$|\{Q, R_1, R_2, \ldots, R_t\}| = t+1$$

where R_j = third point of intersection of $\overline{QP_j}$ with E.

$$\# \text{ Solns} = \underline{t} + (\text{multiple of } t+1)$$

$$\equiv t \mod t+1.$$