

Math 440: Elliptic Curves Homework.

#1. (i) Prove that any elliptic curve given by  $E_K : y^2 = x^3 + ax^2 + bx + c$  can be transformed into the form  $y^2 = x'^3 + b'x' + c'$  through a translation  $x' = x + t$  for some  $t \in K$ .

(ii) Does this affect the group structure of the curve, i.e. is the group for the new curve isomorphic to the original one?

(iii) Does such a  $t$  always exist in the field  $K$ ?

#2. Find the third intersection point of the line through  $(1, 0)$  and  $(9, 20)$  on the curve  $E_{\mathbb{R}} : y^2 = x^3 - 4x^2 - x + 4$ .

#3. Find all points of order 2 on the following curves

- $E_{\mathbb{R}} : y^2 = x^3 - 9x^2 + 16x - 4$

- $E_{\mathbb{R}} : y^2 = x^3 + x^2 + 6x$

- $E_{\mathbb{Q}} : y^2 = x^3 - 8x^2 + 17x - 10$

- $E_{\mathbb{Q}} : y^2 = x^3 + x^2 - 5x$

#4. Let  $S$  be a set with a binary operation  $*$  satisfying the following two rules:

(a)  $P * Q = Q * P$  for all  $P, Q \in S$

(b)  $P * (P * Q) = Q$  for all  $P, Q \in S$

Fix an element  $\mathcal{O} \in S$ , and define the binary operation  $+$  by the rule

$$P + Q = \mathcal{O} * (P * Q)$$

(i) Prove that  $+$  is commutative and has  $\mathcal{O}$  as identity.

(ii) Show that  $X = P * (Q * \mathcal{O})$  is a solution to  $X + P = Q$ .

(iii) Express  $-P$  (the inverse of  $P$  under  $+$ ) in terms of  $*$ .

#5. Use induction to show

$$1^2 + 2^2 + 3^2 + \dots + x^2 = \frac{x^3}{3} + \frac{x^2}{2} + \frac{x}{6}$$

(Hint:  $\frac{x^3}{3} + \frac{x^2}{2} + \frac{x}{6} = \frac{x(x+1)(2x+1)}{6}$ )

#6. Verify that  $(0, 0) + 2(1, 1) = (24, -70)$  on the elliptic curve  $E_{\mathbb{Q}} : y^2 = \frac{x^3}{3} + \frac{x^2}{2} + \frac{x}{6}$ .

#7. If  $a^2 + b^2 = c^2$  and  $n = \frac{ab}{2}$ . Verify that

$$y^2 = x^3 - n^2x$$

where  $y = \frac{(b^2 - a^2)c}{8}$  and  $x = \frac{c^2}{4}$ .

#8. Double the point  $(-3, 36)$  on  $E_{\mathbb{Q}} : y^2 = x^3 - 441x$  to find an  $a$ ,  $b$ , and  $c$  that show 21 is a congruent number.