

**Exercise 1** Recall the expression for the discriminant of an elliptic curve  $E$  for  $\text{char} \neq 2, 3$ .

- (a) Prove that indeed  $\Delta = -(4A^3 + 27B^2)$
- (b) Conversely, prove that  $4A^3 + 27B^2 = 0$  if and only if  $E$  has at least one multiple root

**Exercise 2** Show that, if the characteristic of the field is  $\neq 2$ , the generalized Weierstrass equation can be reduced to  $y^2 = x^3 + Cx^2 + Ax + B$ . Then, show that, if it is also  $\neq 3$ , we obtain the usual form for the Weierstrass equation.

**Exercise 3** Verify that, for an elliptic curve given by a generalized Weierstrass equation, we have  $-P = (x, -a_1x - a_3 - y)$ .

**Exercise 4** Let  $E(\mathbb{Q}) = y^2 = x^3 + 73$ .

- (a) Verify that  $P = (2, 9)$ ,  $Q = (3, 10)$  and  $R = (-4, -3)$  are points on  $E$
- (b) Compute  $P + Q$  and then  $(P + Q) + R$
- (c) Compute  $Q + R$  and then  $P + (Q + R)$
- (d) Check that you get the same result. Which of the two computations is the most convenient?

**Exercise 5** Transform the cubic  $x^3 + y^3 = d$  into an elliptic curve in Weierstrass form.

*Hint: Similar to the cubic seen in class.*