CISS451/MATH451: Cryptography and Computer Security
Assignment 9

The following equation (an elliptic curve)

$$E : y^2 = x^3 - 2$$

has the following solution

$$P = (3, 5)$$

[Check that P is on the curve in your head ... 2 seconds.] That's no big deal. *Here's* the big deal ...

In 1621, Bachet showed that there are in fact a series of solutions. Here's one of them:

$$\left(\frac{30037088724630450803382035538503505921}{30106839828987630717868429937799184 00},\right.$$

$$\left.\frac{1644557217519796256439143766866676956618981558720105932 81}{5223934923525719974563641453744978655831227509874752000}\right)$$

It was discovered later that his formulas for producing the x– and y–coordinates of the series of points on the curve actually give the doubling of points. In other words his formulas compute the points

$$2P, \quad 2(2P), \quad 2(2(2P), \quad 2(2(2(2P)))...$$

from P. [Recall that $2P$ is just $P + P$.] The humongous point above is in fact $8P$.

This quiz involves the computation of addition of rational (i.e. $\mathbb{Q}$) points on E. For all the questions below, P denotes the point $(3, 5)$.

All work must be shown clearly. Answers without justification (i.e. computation) will give you a zero. You need not however show work for simple computations such as addition fractions and simplify fractions. If in doubt, it's your responsibility to ask me.

Q1. Given

$$E : y^2 = x^3 - 2$$

and

$$P = (3, 5)$$

is on E. Compute $2P$. Write clearly. Simplify your answer. Circle the answer. [It's a good idea to check that your $2P$ is on E.]

SOLUTION.

STEP 1: Let L be the equation of the tangent line to the E at P. From

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

we get

$$\begin{aligned} 2y\frac{dy}{dx} &= 3x^2 \\ \therefore \quad \frac{dy}{dx} &= \frac{2y}{3x^2} \\ \therefore \quad \left.\frac{dy}{dx}\right|_P &= \frac{27}{10} \end{aligned}$$

Hence the tangent line of E at P is of the form

$$L : y = \frac{27}{10}x + c$$

where c is a constant. Since P is on L, on substituting P into L we get

$$\begin{aligned} 5 &= \frac{27}{10} \cdot 3 + c \\ \therefore \quad c &= \frac{-31}{10} \end{aligned}$$

Therefore L is

$$L : y = \frac{27}{10}x + \frac{-31}{10}$$

STEP 2: Let R' be the point of intersection of E and L other than P. Furthermore let $R' = (x_3', y_3')$. P and R' are both on E and L and hence satisfies the equation of E and the equation of L:

$$y^2 = x^3 - 2 \tag{1}$$

$$y = \frac{27}{10}x + \frac{-31}{10} \tag{2}$$

Substituting (2) into (1) we get

$$\left(\frac{27}{10}x + \frac{-31}{10}\right)^2 = x^3 - 2$$
$$\therefore \quad 0 = x^3 - 2 - \left(\frac{27}{10}x + \frac{-31}{10}\right)^2$$

Note that we already know two roots of this cubic since P occurs twice on E and L:

$$x^3 - 2 - \left(\frac{27}{10}x + \frac{-31}{10}\right)^2 = (x-3)(x-3)(x-x_3')$$

The coefficient of x^2 on the left of this equation is

$$\frac{-729}{100}$$

The coefficient of x^2 on the right of this equation is

$$-x_3' - 3 - 3$$

Equating the coefficient of x^2 on the left of the equation with the coefficient of x^2 on the right, we get

$$\frac{-729}{100} = -x_3' - 3 - 3$$
$$\therefore \quad x_3' = \frac{129}{100} \tag{3}$$

Substituting (3) into (2) we get obtain the y–coordinate of R':

$$y_3' = \frac{27}{10} \cdot \frac{129}{100} + \frac{-31}{10} = \frac{383}{1000}$$

Therefore

$$R' = \left(\frac{129}{100}, \frac{383}{1000}\right)$$

STEP 3: Reflecting R' about the x–axis, we get

$$2P = \left(\frac{129}{100}, -\frac{383}{1000}\right)$$

□

Q2. You are given another point on E is the following

$$Q = \left(\frac{129}{10^2}, \frac{383}{10^3}\right)$$

Compute $P+Q$. Write clearly. Simplify your answer. Circle the answer. [It's a good idea to check that your $P+Q$ is on E.]

SOLUTION.

STEP 1. Let L be the line through P and Q. The slope of L is

$$\frac{5 - 383/1000}{3 - 129/100} = \frac{27}{10}$$

Hence the equation of L is of the form

$$L : y = \frac{27}{10}x + c$$

where c is a constant. Since P is on L when we substitution P into L we get

$$\begin{aligned} 5 &= \frac{27}{10} \cdot 3 + c \\ \therefore \quad c &= 5 - \frac{27}{10} \cdot 3 = -\frac{31}{10} \end{aligned}$$

Therefore

$$L : y = \frac{27}{10}x - \frac{31}{10}$$

STEP 2: Let R' be the point of intersection of L and E that is not P or Q. Furthermore let $R' = (x_3', y_3')$. Then P, Q, R' are on the equation of E and the equation of L:

$$y^2 = x^3 - 2 \tag{1}$$

$$y = \frac{27}{10}x - \frac{31}{10} \tag{2}$$

Substituting (2) into (1) we get

$$\begin{aligned} \left(\frac{27}{10}x - \frac{31}{10}\right)^2 &= x^3 - 2 \\ \therefore \quad 0 &= x^3 - 2 - \left(\frac{27}{10}x - \frac{31}{10}\right)^2 \end{aligned}$$

Note that the three roots of this cubic polynomial must be the x–coordinates of P, Q, R', i.e. $3, 129/10^2, x_3'$. Hence

$$x^3 - 2 - \left(\frac{27}{10}x - \frac{31}{10}\right)^2 = (x-3)(x - 129/10^2)(x - x_3')$$

The coefficient of x^2 on the left of the above equation is

$$\frac{-729}{100}$$

The coefficient of x^2 on the right of the above equation is

$$-x_3' - 3 - \frac{129}{100}$$

Equating the coefficient of x^2 on the left side of this equation with the coefficient of x^2 on the right side of this equation we get

$$\begin{aligned} \frac{-729}{100} &= -x_3' - \frac{429}{100} \\ \therefore \quad x_3' &= 3 \end{aligned}$$

Substituting $x = x_3'$ into (2), we get the the y–coordinate of R':

$$y_3' = \frac{27}{10} \cdot 3 + \frac{-31}{10} = 5$$

Therefore

$$R' = (3, 5)$$

STEP 3: On reflecting R' about the x–axis, we get

$$P + Q = (3, -5)$$

$\square$

Note. Q2 actually has a much shorter solution. Using the fact that $E(\mathbb{Q})$ is a group, we can compute $P + Q$ algebraically without performing the geometric construction for $+$. How?

First here's a fact that can be deduced quickly from our geometric construction of $+$: If $A = (x, y)$ and $B = (x, -y)$ are points of an elliptic curve $y^2 = f(x)$, i.e. they are reflection of each other about the x–axis, then the geometric construction tells us immediately that

$$A = -B$$

and

$$B = -A$$

In other words

$$-(x, y) = (x, -y)$$

Now look at Q1. $2P$ is the reflection about the x–axis of Q. This means that

$$Q = -2P$$

For Q2, we need to compute $P + Q$. This is then

$$P + Q = P - 2P = -P$$

But $-P$ is just the reflection of P about the x–axis. Therefore we have

$$P + Q = -P = -(3, 5) = (3, -5)$$

Vóila!!!