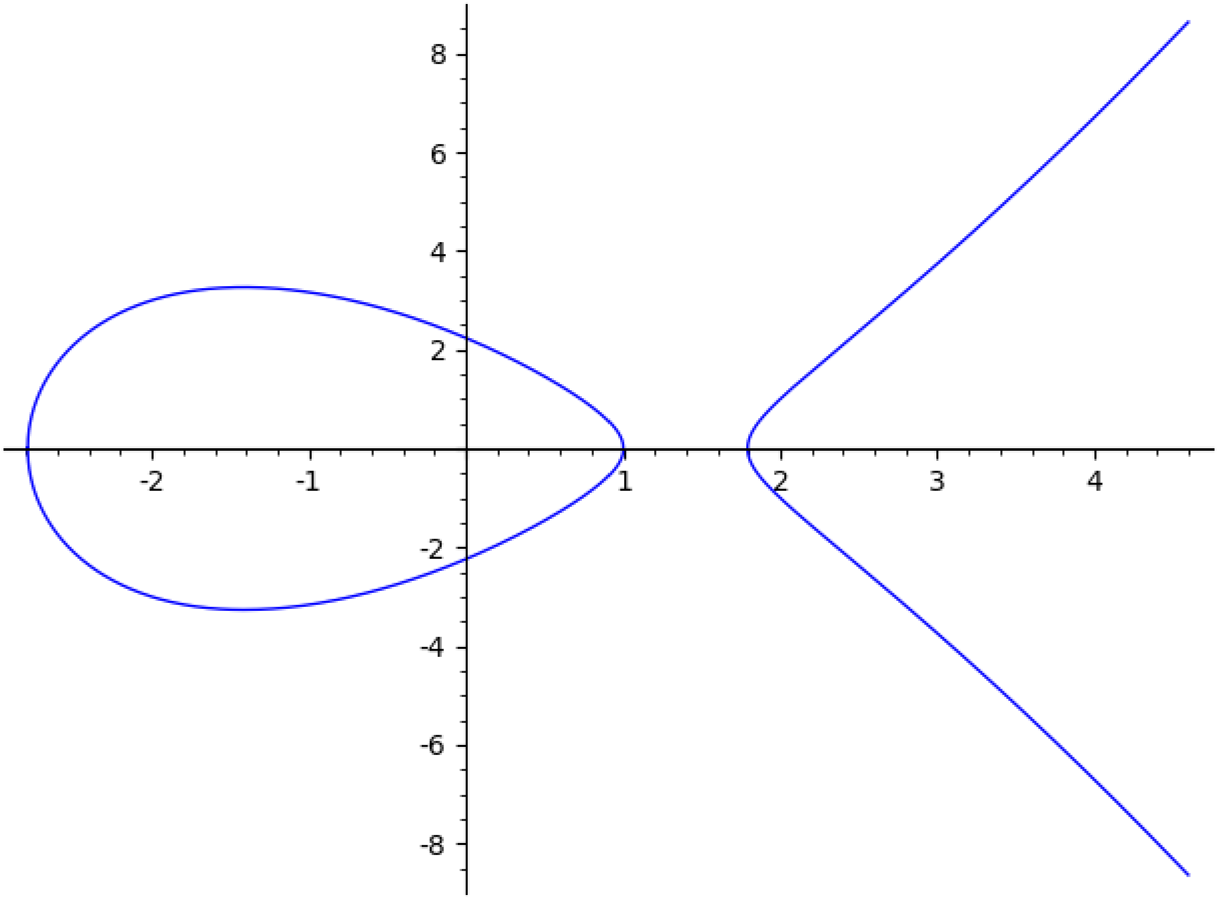
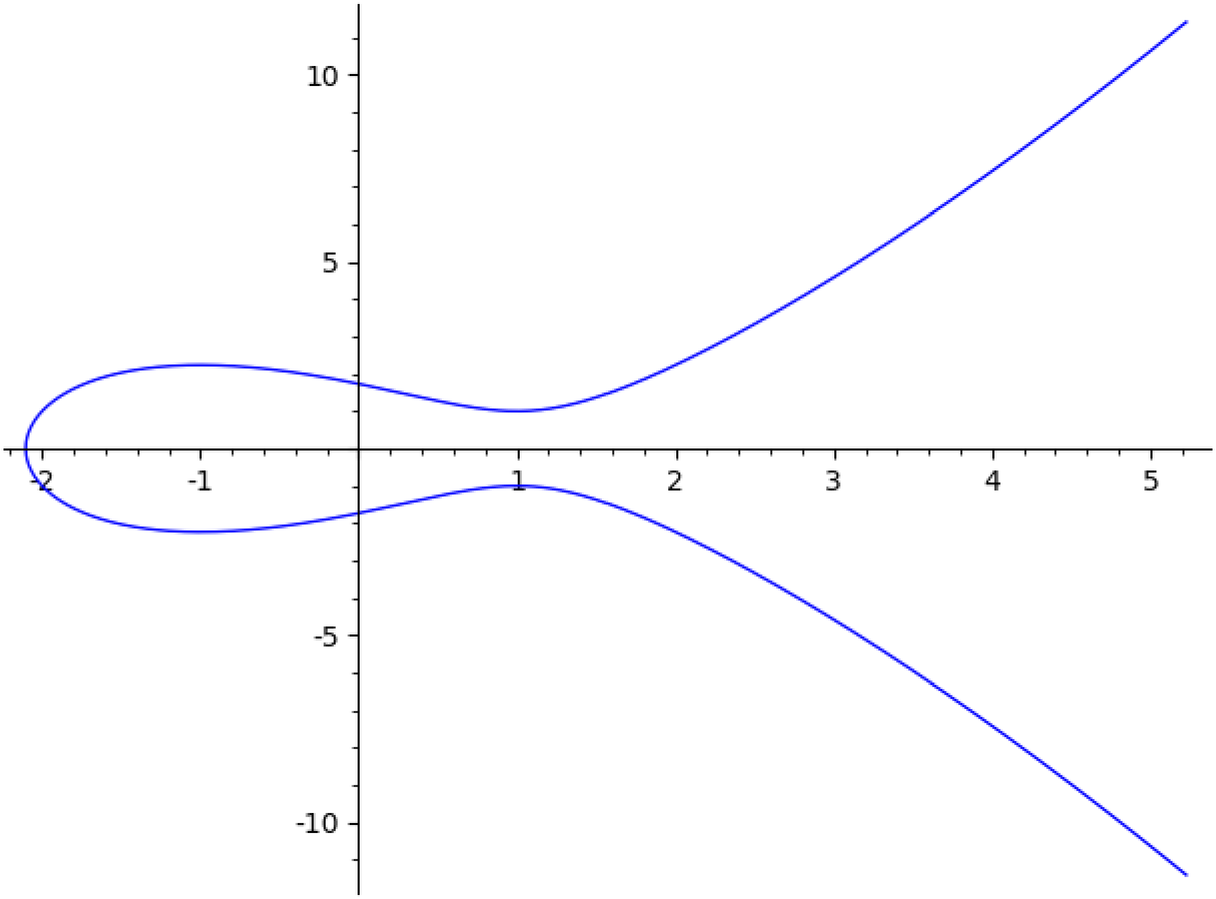
Lecture 11 Elliptic Curves

Def. An **elliptic curve** is a curve with an equation $y^2 = x^3 + Ax + B$ where $4A^3 + 27B^2 \neq 0$. This last condition guarantees that the curve does not have self-intersections or cusps.

Examples:
(1) $y^2 = x^3 - 6x + 5$



(2) $y^2 = x^3 - 3x + 3$



Note: The graphs above were produced in Sage by the commands (we illustrate the second graph).

```
E =EllipticCurve([−3,3])
plot(E)
```

Def: A point (x, y) is said to be a **rational point** if x and y are both rational numbers (i.e., they can be expressed as fractions a/b where a,b are itegers and $b \neq 0$

The use of elliptic curves in cryptography is related to the fact that one can define an addition of rational points on an elliptic curve. This kind of addition is used as the basic operation in elliptic curve cryptography. The following theorem is what justifies the addition of rational points on elliptic curves.

Theorem. If E is an elliptic curve and P, Q are two rational points on E then the line connecting P, Q intersects E at a third point R, which is a rational point.

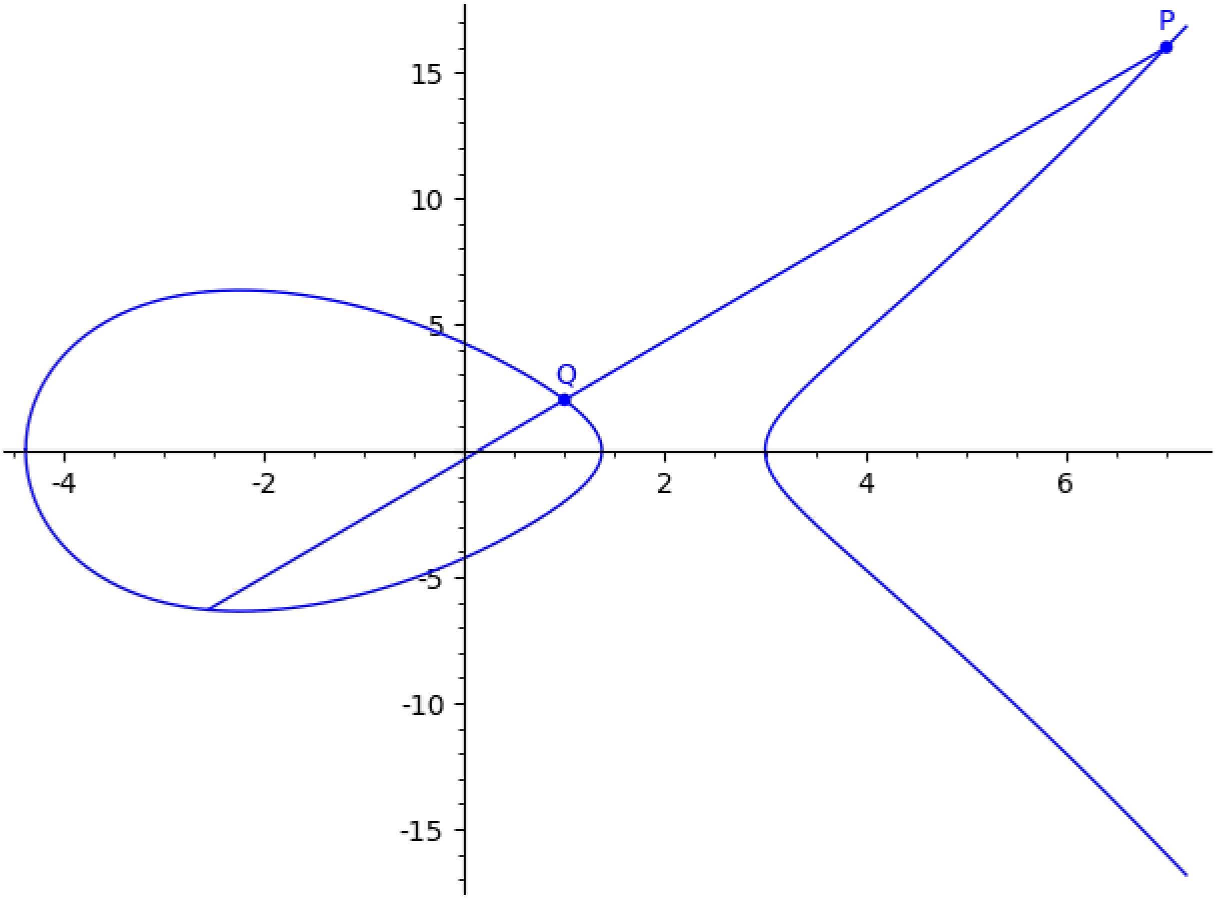
Def. If *E* is an elliptic curve and *P*, *Q* are two rational points on *E* then we define the addition of the points $\boldsymbol{P+Q}$ as follows

Connect *P*, *Q* with a line intersecting *E* at the third point *R*. Let $\boldsymbol{R'}$ be the reflection of *R* across the *x*-axis (if $\boldsymbol{R=(x,y)}$ then $\boldsymbol{R'=(x,-y)}$). Define $\boldsymbol{P+Q=R'}$.

Note there are two special cases:
(1) $\boldsymbol{P+P=2P}$. We draw a tangent line at *P*, and use the other point of intersection *R* of the tangent line and *E*. We then define $\boldsymbol{P+P=R'}$ as in the main case.

(2) $\boldsymbol{P+P'}$. We first introduce what is known as the point at infinity. This point is at the "end" of vertical lines. Call this point *O* (a further use of this point is in the theorem below). Define $\boldsymbol{P+P'=O}$.

Example: Consider $\boldsymbol{y^2=x^3-15x+18}$. Let $\boldsymbol{P=(7,16), Q=(1,2)}$ be rational points on the curve (it is easy to check that the points are in fact on the curve).



Note: I have shown the line connecting the two points and the third point of intersection between the line and the elliptic curve.

Here is the hard way to compute the sum (the easy way is in the theorem below).

The line connecting *P*, *Q* has the equation $y = \frac{7}{3}x - \frac{1}{3}$ (use the point-slope formula $y - y_0 = \frac{y_1 - y_0}{x_1 - x_0}(x - x_0)$).

Find the intersection of this line and the elliptic curve.

$$\left(\frac{7}{3}x - \frac{1}{3}\right)^2 = x^3 - 15x + 18$$

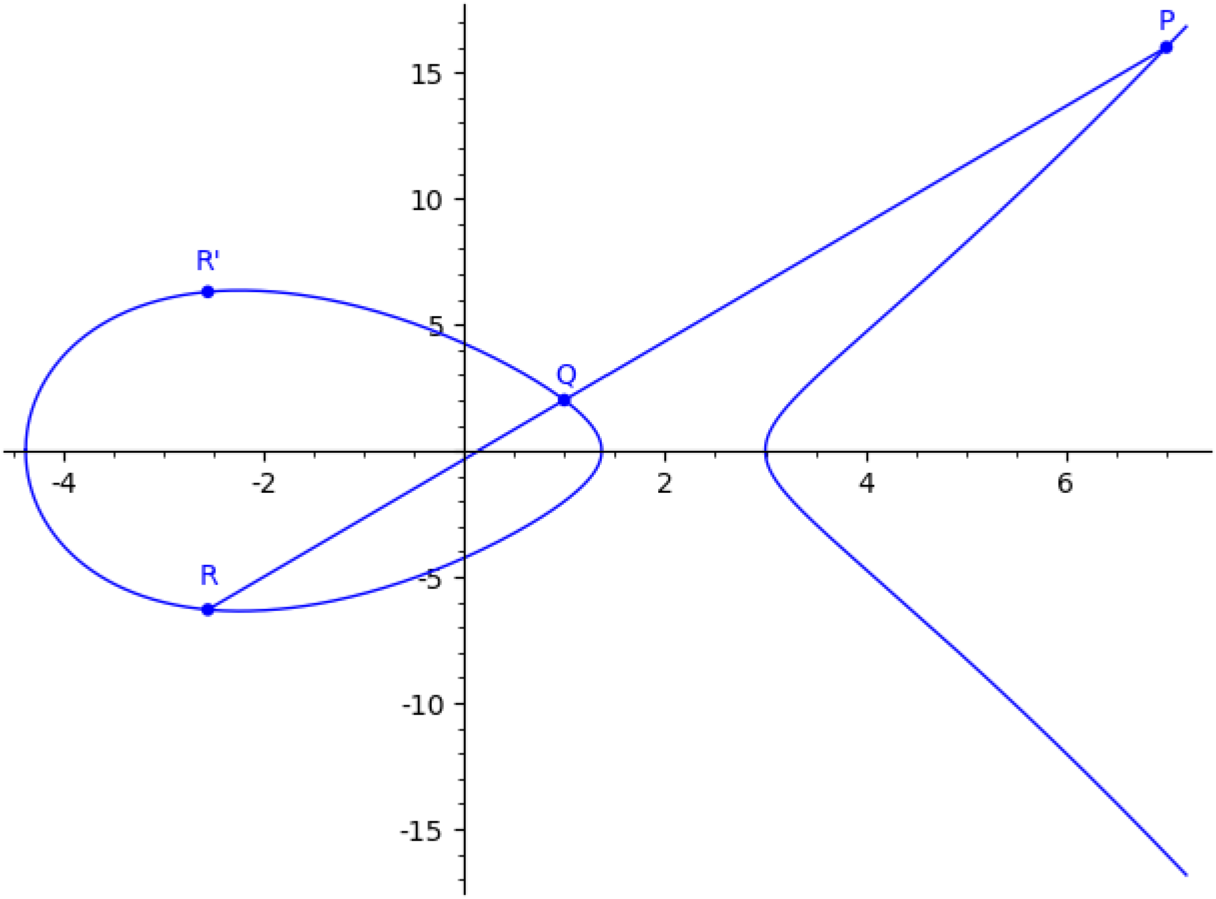
$$\frac{49}{9}x^2 - \frac{14}{9}x + \frac{1}{9} = x^3 - 15x + 18$$

$$x^3 - \frac{49}{9}x^2 - \frac{121}{9}x + \frac{161}{9} = 0$$

$$(x-7)(x-1)\left(x + \frac{23}{9}\right) = 0$$

The last equation comes from the fact that we know *P*, *Q* are two of the three points of intersection. So the point of intersection *R* has *x*-coordinate $x = \frac{23}{9}$. The *y*-coordinate can be computed $y = \frac{7}{3}x - \frac{1}{3} = \frac{7}{3}\left(\frac{-23}{9}\right) - \frac{1}{3} = -\frac{170}{27}$.

Hence $R = \left(-\frac{23}{9}, -\frac{170}{27}\right)$, $P + Q = R' = \left(-\frac{23}{9}, \frac{170}{27}\right)$



Here are the Sage commands that gave the above graph

```
E1=EllipticCurve([-15,18])
g1 = plot(E1)
g2 = line([(7,16),(-23/9,-170/27)])
P = point((7,16), size = 22)
g3 = plot(P)
g4 = text("P", (7,17))
Q = point((1,2), size = 22)
g5 = plot(Q)
g6 = text("Q", (1,3))
R = point((-23/9,-170/27), size = 22)
g7 = plot(R)
g8 = text("R", (-23/9, -5))
R_prime = point((-23/9,170/27), size = 22)
g9 = plot(R_prime)
g10 = text("R'", (-23/9, 7.5))
show(g1+g2+g3+g4+g5+g6+g7+g8+g9+g10)
```

Now let’s compute $\boldsymbol{P+P=2P}$

We first need to compute the equation of the tangent line at *P*. Start with the equation of the elliptic curve and use implicit differentiation to find the slope of the tangent line.

$$y^2 = x^3 - 15x + 18$$

$$2y\frac{dy}{dx} = 3x^2 - 15 \Rightarrow \frac{dy}{dx} = \frac{3x^2-15}{2y}$$

Substituting $(x, y) = (7,16) \Rightarrow \frac{dy}{dx} = \frac{33}{8}$

Using the point slope formula gives the following equation for the tangent line.

$$y = \frac{33}{8}x - \frac{103}{8}$$

Find the intersection of this line and the elliptic curve.

$$\left(\frac{33}{8}x - \frac{103}{8}\right)^2 = x^3 - 15x + 18$$

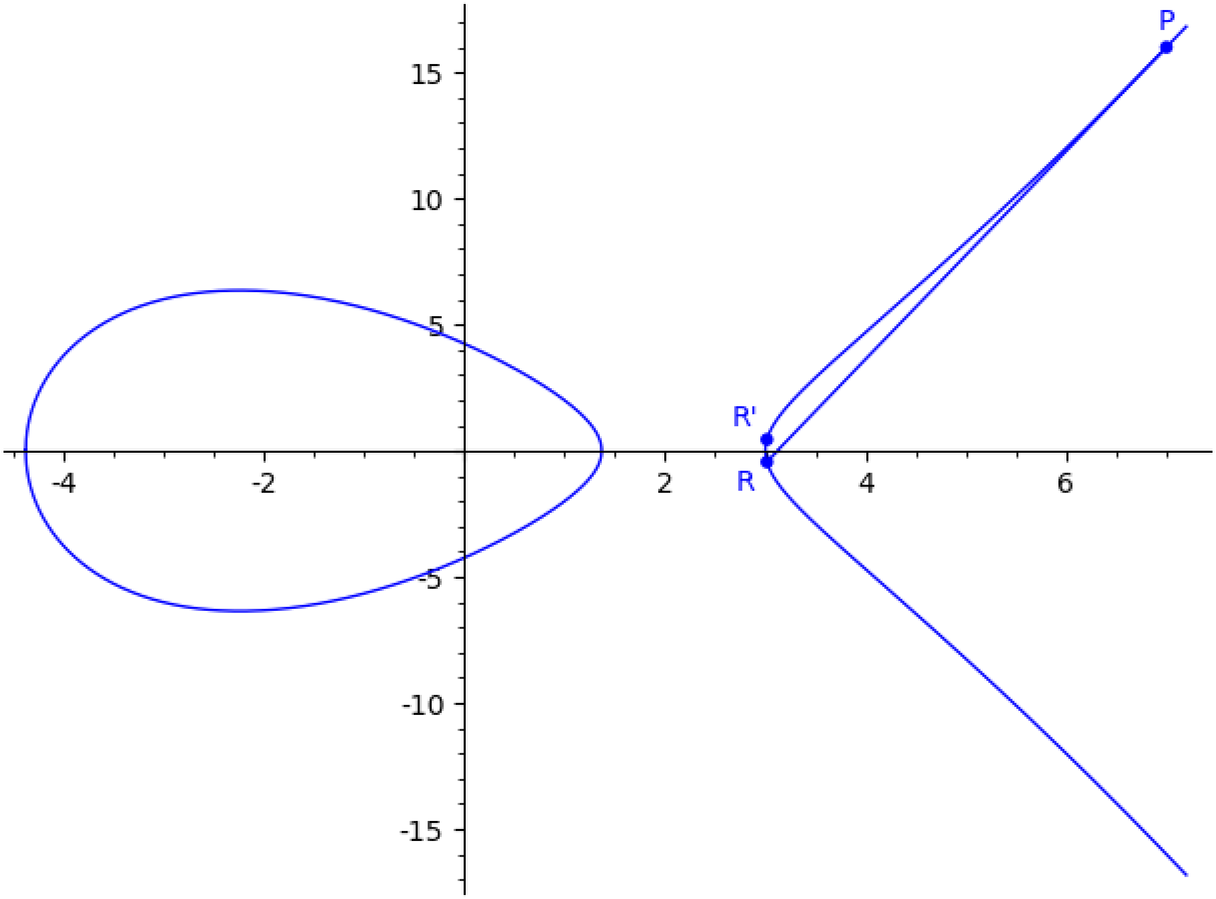
$$(x-7)^2\left(x - \frac{193}{64}\right) = 0$$

So the point of intersection *R* has *x*-coordinate $x = \frac{193}{64}$. The *y*-coordinate can be computed

$$y = \frac{33}{8}x - \frac{103}{8} = \frac{33}{8}\left(\frac{193}{64}\right) - \frac{103}{8} = -\frac{223}{512}$$

$$R = \left(\frac{193}{64}, -\frac{223}{512}\right),\ P + P = R' = \left(\frac{193}{64}, \frac{223}{512}\right).$$

Hence $R = \left(\frac{193}{64}, -\frac{223}{512}\right),\ P + P = R' = \left(\frac{193}{64}, \frac{223}{512}\right)$



Here are the Sage commands for the above graph

```
E1=EllipticCurve([-15,18])
g1 = plot(E1)
g2 = line([(7,16),(193/64, -223/512)])
P = point((7,16), size = 22)
g3 = plot(P)
g4 = text("P", (7,17))
R = point((193/64, -223/512), size = 22)
g5 = plot(R)
g6 = text("R", (2.8,-1.3))
R_prime = point((193/64,223/512), size = 22)
g7 = plot(R_prime)
g8 = text("R'", (2.8, 1.3))
show(g1+g2+g3+g4+g5+g6+g7+g8)
```

Theorem: Let E elliptic curve $y^2 = x^3 + Ax + B$. Let O be the point at infinity.
(a) Let P be a rational point on E. Then $P + O = O + P = P$
(b) Let P be a rational point on E. Then $P + P' = O$
(c) If $P = (x_1, y_1), Q = (x_2, y_2)$, define

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + A}{2y_1} & \text{if } P = Q \end{cases}$$

Let $x_3 = \lambda^2 - x_1 - x_2,\ y_3 = \lambda(x_1 - x_3) - y_1$. Then $P + Q = (x_3, y_3)$

Example
(1) As before let $y^2 = x^3 - 15x + 18$. Let $P = (7,16), Q = (1,2)$. Compute $P + Q$
We then have:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{2-16}{1-7} = \frac{7}{3}$$

$$x_3 = \lambda^2 - x_1 - x_2 = \left(\frac{7}{3}\right)^2 - 7 - 1 = -\frac{23}{9},\ y_3 = \lambda(x_1 - x_3) = \left(\frac{7}{3}\right)\left(7 + \frac{23}{9}\right) = \frac{170}{27}$$

$$P + Q = \left(-\frac{23}{9}, \frac{170}{27}\right)$$

This is the same answer as before.

(2) Let us compute $P + P$, note that in this case we must adjust the formulas as follows:
$(x_1, y_1) = (x_2, y_2) = (7,16)$

$$\lambda = \frac{3x_1^2 + A}{2y_1} = \frac{33}{8}$$

$$x_3 = \lambda^2 - x_1 - x_2 = \frac{193}{64},\ y_3 = \lambda(x_1 - x_3) - y_1 = \frac{223}{512}$$

$$P + P = \left(\frac{193}{64}, \frac{223}{512}\right)$$

This is the same answer as before.