1. Consider the equation

$$x^3 - y^2 = 7. \tag{1.1}$$

While studying the group law on a smooth cubic we noted that if the cubic has coefficients in $\mathbb{Q}$, then any line through two rational points of the curve (or tangent to one rational point of the curve) would meet the curve in another rational point.

The point $(x, y) = (2, 1)$ is a solution to the equation. Let's use the idea above to find another.

(a) Find the equation of the tangent line to $x^3 - y^2 = 7$ at the point $(2, 1)$. (The technique of implicit differention from first-year calculus is a good method to use.)

(b) Substitute the equation of the line into (1.1) to get a cubic equation in x.

(c) Factor the equation in (b) and use the new root to find a new point on the curve. (Be sure to test the point you found to ensure that it satisfies (1.1).)

Solution.

(a) Implicit differentiation of the equation $x^3 - y^2 = 7$ gives

$$3x^3\,dx - 2y\,dy = 0$$

so that at a point (x_0, y_0) of the curve the slope of the tangent line is

$$\frac{dy}{dx} = \frac{3x_0^2}{2y_0}.$$

For $(x_0, y_0) = (2, 1)$ the slope is then $\frac{dy}{dx} = \frac{3\cdot 2^2}{2\cdot 1} = 6$. The equation of the line of slope 6 passing through $(2, 1)$ is $y = 6x - 11$.

(b) Substituting the equation of the line from (a) into $x^3 - y^2 - 7 = 0$ gives

$$0 = x^3 - (6x - 11)^2 - 7 = x^3 - (36x^2 - 132x + 121) - 7 = x^3 - 36x^2 + 132x - 128.$$

(c) The cubic polynomial in (b) factors as $(x - 2)^2(x - 32)$. Plugging the solution $x = 32$ into the equation of the line gives $y = 6 \cdot 32 - 11 = 181$, and thus the point $(32, 181)$ must be on the curve. We check by plugging into the equation:

$$32^3 - 181^2 = 32768 - 32761 = 7.$$

2. We can use a similar method of intersecting with lines to find an algebraic parameterization of points on the circle.

(a) Write down the equation of the line passing through the points $(-1, 0)$ and $(0, t)$.

(b) The line from (a) intersected with the conic $x^2 + y^2 = 1$ will have two points of intersection. One of them is $(-1, 0)$. Find the other one as a function of t.

(c) Check that your solution from (b) satisfies $x^2 + y^2 + 1$.

Integer solutions to $X^2+Y^2 = Z^2$ are called *Pythagorean triples*. The equation $X^2+Y^2 = Z^2$ is the homogenization of $x^2 + y^2 = 1$, and hence rational points on the circle give rise to Pythagorean triples.

(d) Evaluate your solution in (b) at $t = 4$, 5, and 6. For each of your points write it as $[x : y : 1]$ in $\mathbb{P}^2$ and clear denominators to get a different representation of that point as $[X : Y : Z]$ with X, Y, and Z relatively prime integers.

(e) Which Pythagorean triples did you find?

Solution.

(a) The line connecting $(-1, 0)$ to $(0, t)$ has slope t and equation $y = tx+t = t(x+1)$.

(b) Substituting into $x^2 + y^2 - 1 = 0$ gives

$$0 = x^2 + (t(x+1))^2 - 1 = x^2 + t^2(x^2 + 2x + 1) - 1 = (1 + t^2)x^2 + (2t^2)x + (t^2 - 1).$$

We already know that $x = -1$ is a root, and so we see that we can factor the polynomial as

$$(x + 1)((1 + t^2)x + (t^2 - 1)),$$

with root $x = \frac{1-t^2}{1+t^2}$. Plugging this into the equation of the line gives the y coordinate as $y = t\left(\frac{1-t^2}{1+t^2} + 1\right) = t \cdot \frac{2}{1+t^2} = \frac{2t}{1+t^2}$, so that as a function of t the other the point is

$$(x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right).$$

(c) We have

$$\left(\frac{1 - t^2}{1 + t^2}\right)^2 + \left(\frac{2t}{1 + t^2}\right)^2 = \frac{1 - 2t^2 + t^4}{(1 + t^2)^2} + \frac{4t^2}{(1 + t^2)^2} = \frac{1 + 2t^2 + t^4}{(1 + t^2)^2} = \frac{(1 + t^2)^2}{(1 + t^2)^2} = 1,$$

so the point given in (b) is certainly on the circle $x^2 + y^2 = 1$.

(d) For $t = 4, 5, 6$ the points are given by the following table

t	Point in $\mathbb{A}^2$	Point in $\mathbb{P}^2$		
4	$\left(-\frac{15}{17}, \frac{8}{17}\right)$	$\left[-\frac{15}{17} : \frac{8}{17} : 1\right]$	=	$[-15 : 8 : 17]$
5	$\left(-\frac{12}{13}, \frac{5}{13}\right)$	$\left[-\frac{12}{13} : \frac{5}{13} : 1\right]$	=	$[-12 : 5 : 13]$
6	$\left(-\frac{35}{37}, \frac{12}{37}\right)$	$\left[-\frac{35}{37} : \frac{12}{37} : 1\right]$	=	$[-35 : 12 : 37]$

(e) Above we have found the Pythagorean triples

$$(-15)^2 + 8^2 = 17^2, \ \ (-12)^2 + 5^2 = 13^2, \ \text{ and } \ (-35)^2 + 12^2 = 37^2.$$

Of course, we can also multiply the x-coordinate by -1 and get the corresponding Pythagorean triples where every integer is positive:

$$15^2 + 8^2 = 17^2, \ \ 12^2 + 5^2 = 13^2, \ \text{ and } \ 35^2 + 12^2 = 37^2.$$

NOTE: This process can be reversed to show that every primitive Pythagorean triple (those where $\gcd(X, Y, Z) = 1$) occur this way.

3. In this problem we will compute in the group law of the elliptic curve E given by $ZY^2 - X^3 - 17Z^3 = 0$ in $\mathbb{P}^2$ (or its dehomogenized form: $y^2 = x^3 + 17$). Even though not precisely in Weierstrass form, the identity is still at $[0 : 1 : 0]$, and we still compute in the group law by intersecting with lines as before.

Before doing any specific computations, let us work out some general formulae for addition. Recall that the additive inverse of a point $[X : Y : Z]$ on E is $[X : -Y : Z]$. In the affine chart U_2, this means that the inverse of (x, y) is $(x, -y)$.

(a) Suppose that $y = mx + b$ is the equation of a line joining two points (x_1, y_1) and (x_2, y_2) of E. Show that the x-coordinate of $(x_1, y_1) + (x_2, y_2)$ is $m^2 - x_1 - x_2$, and that the y-coordinate is $-m(m^2 - x_1 - x_2) - b$. (SUGGESTION: For the x-coordinate, substitute $y = mx + b$ into the equation of E, and use the relationship between the coefficient of x^2 and the sum of the roots, see for example Homework 5, Question 6(c).)

(b) Suppose that $y = mx + b$ is the equation of the tangent line to the curve E at a point $P = (x_1, y_1)$. Give formulae as in (a) for the x and y coordinates of $P + P$.

(c) Let (x_1, y_1) be a point of E. Use implicit differentiation to compute the slope m of the tangent line to E at (x_1, y_1).

Let $P = (-2, 3)$ and $Q = (2, 5)$. Both are points of E.

(d) Compute $2Q - P$.

(e) Compute $3P - Q$.

Solution.

(a) If α, β, and γ are any numbers then

$$(x-\alpha)(x-\beta)(x-\gamma) = x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\beta\gamma+\alpha\gamma)x - \alpha\beta\gamma.$$

In particular, the coefficient of x^2 is the negative of the sum of the roots.

Substituting the equation $y = mx + b$ into the equation for E we get

$$0 = x^3 - y^2 - 17 = x^3 - (mx+b)^2 - 17 = x^2 - m^2x^2 - 2mbx - (b^2+17).$$

If x_1, x_2, and x_3 are the roots, then our argument above shows that $m^2 = x_1 + x_2 + x_3$. Thus $x_3 = m^2 - x_1 - x_2$.

To find the y-coordinate of the third point where the line intersects E we put x_3 into the equation of the line to get $m(m^2 - x_1 - x_2) + b$. In the group law of E the sum of (x_1, y_1) and (x_2, y_2) is the inverse of the point $(m^2 - x_1 - x_2, m(m^2 - x_1 - x_2) + b)$ on the line. By the rule for taking the inverse, this point is $(m^2 - x_1 - x_2, -m(m^2 - x_1 - x_2) + b)$.

(b) The argument for (b) is the same as (a), except now that x_1 is a double root of the polynomial $x^3 - (mx+b)^2 - 17$. This means that $x_3 = m^2 - 2x_1$. Substituting this x-value into the equation of the line, and taking the inverse in the group law of E we find that $y_3 = -m(m^2 - 2x_1) - b$.

(c) Implicit differentiation of the equation $x^3 - y^2 = 17$ gives

$$3x^3\,dx - 2y\,dy = 0$$

so that at a point (x_0, y_0) of the curve the slope of the tangent line is

$$\frac{dy}{dx} = \frac{3x_0^2}{2y_0}.$$

(d) From (c) the slope of the tangent line to E at Q is $m = \frac{3(-2)^2}{2(5)} = \frac{6}{5}$. The line with slope $\frac{6}{5}$ containing Q is given by the equation $y = \frac{6}{5}x + \frac{13}{5}$. By the formula in part (b), this lets us compute that

$$2Q = Q + Q = \left(\left(\tfrac{6}{5}\right)^2 - 2\cdot 2, -\tfrac{6}{5}\left(\left(\tfrac{6}{5}\right)^2 - 2\cdot 2\right) - \tfrac{13}{5}\right) = \left(-\tfrac{64}{25}, \tfrac{59}{125}\right).$$

From the formula for the inverse, $-P = (-2, -3)$. The line joining $(-2, -3)$ and $(-\frac{64}{25}, \frac{59}{125})$ has slope $m = -\frac{31}{5}$ and equation $y = -\frac{31}{5}x - \frac{77}{5}$.

By the formula in part (a), this means that

$$\begin{aligned} 2Q - P &= \left(\left(-\tfrac{31}{5}\right)^2 - \left(-\tfrac{64}{25}\right) - (-2),\ -\tfrac{31}{5} \cdot \left(\left(-\tfrac{31}{5}\right)^2 - \left(-\tfrac{64}{25}\right) - (-2)\right) + \tfrac{77}{5}\right) \\ &= (43, 282). \end{aligned}$$

(e) The line tangent to E at P has slope $m = \frac{3(-2)^2}{2 \cdot 3} = 2$ and equation $y = 2x + 7$. By the formula from part (b) we compute that

$$2 \cdot P = \left(2^2 - 2 \cdot (-2), -2 \cdot (2^2 - 2 \cdot (-2)) - 7\right) = (8, -23).$$

The line connecting $2P = (8, -23)$ and $P = (-2, 3)$ has slope $m = -\frac{13}{5}$ and equation $y = -\frac{13}{5}x - \frac{11}{5}$. By the formula from (b) we compute that

$$3P = \left(\left(-\tfrac{13}{5}\right)^2 - 8 - (-2), -\left(-\tfrac{13}{5}\right) \cdot \left(\left(-\tfrac{13}{5}\right)^2 - 8 - (-2)\right) + \tfrac{11}{5}\right) = \left(\tfrac{19}{25}, \tfrac{522}{125}\right).$$

Finally, since $-Q = (2, -5)$, the line connecting $-Q$ and $3P$ is $y = -\frac{37}{5}x + \frac{49}{5}$, part (b) gives

$$3P - Q = \left(\left(-\tfrac{37}{5}\right)^2 - 2 - \tfrac{19}{25}, \tfrac{37}{5} \cdot \left(\left(-\tfrac{37}{5}\right)^2 - 2 - \tfrac{19}{25}\right) - \tfrac{49}{5}\right) = (52, 375).$$

As a check, both points we computed are on the curve:

$$282^2 - 43^3 = 79524 - 79507 = 17 \text{ and } 375^2 - 52^3 = 140625 - 14608 = 17.$$

Of course, there are other ways of evaluating this additions, for example in (d) we could compute $Q - P$ first and then add Q. In order to help check these other ways, here is a small table of additions of the points. The identity of E (the point $[0 : 1 : 0]$) is included in the table as a means of displaying the coordinates of P, $2P$ and all the rest. (I.e., $2P + [0 : 1 : 0] = (8, -23)$ is a way of recording that $2P = (8, -23)$.)

$+$	$[0:1:0]$	P	$2P$	$3P$	Q	$2Q$	$-P$	$-Q$
$[0:1:0]$	$[0:1:0]$	$(-2,3)$	$(8,-23)$	$\left(\frac{19}{25},\frac{522}{125}\right)$	$(2,5)$	$\left(-\frac{64}{25},\frac{59}{125}\right)$	$(-2,-3)$	$(2,-5)$
P	$(-2,3)$	$(8,-23)$	$\left(\frac{19}{25},\frac{522}{125}\right)$	$\left(\frac{752}{529},-\frac{54239}{12167}\right)$	$\left(\frac{1}{4},-\frac{33}{8}\right)$	$\left(\frac{1222}{49},-\frac{42741}{343}\right)$	$[0:1:0]$	$(4,9)$
$2P$	$(8,-23)$	$\left(\frac{19}{25},\frac{522}{125}\right)$	$\left(\frac{752}{529},-\frac{54239}{12167}\right)$	$\left(\frac{174598}{32761},\frac{76943337}{5929741}\right)$	$\left(\frac{106}{9},\frac{1097}{27}\right)$	$\left(-\frac{967}{1936},\frac{349933}{85184}\right)$	$(-2,3)$	$(-1,-4)$
$3P$	$\left(\frac{19}{25},\frac{522}{125}\right)$	$\left(\frac{752}{529},-\frac{54239}{12167}\right)$	$\left(\frac{174598}{32761},\frac{76943337}{5929741}\right)$	$\left(-\frac{4471631}{3027600},-\frac{19554357097}{5268024000}\right)$	$\left(-\frac{2228}{961},-\frac{63465}{29791}\right)$	$\left(\frac{524374}{172225},-\frac{480655443}{71473375}\right)$	$(8,-23)$	$(52,375)$
Q	$(2,5)$	$\left(\frac{1}{4},-\frac{33}{8}\right)$	$\left(\frac{106}{9},\frac{1097}{27}\right)$	$\left(-\frac{2228}{961},-\frac{63465}{29791}\right)$	$\left(-\frac{64}{25},\frac{59}{125}\right)$	$\left(\frac{5023}{3249},-\frac{842480}{185193}\right)$	$(4,-9)$	$[0:1:0]$
$2Q$	$\left(-\frac{64}{25},\frac{59}{125}\right)$	$\left(\frac{1222}{49},-\frac{42741}{343}\right)$	$\left(-\frac{967}{1936},\frac{349933}{85184}\right)$	$\left(\frac{524374}{172225},-\frac{480655443}{71473375}\right)$	$\left(\frac{5023}{3249},-\frac{842480}{185193}\right)$	$\left(\frac{38194304}{87025},-\frac{236046706033}{25672375}\right)$	$(43,282)$	$(2,5)$
$-P$	$(-2,-3)$	$[0:1:0]$	$(-2,3)$	$(8,-23)$	$(4,-9)$	$(43,282)$	$(8,23)$	$\left(\frac{1}{4},\frac{33}{8}\right)$
$-Q$	$(2,-5)$	$(4,9)$	$(-1,-4)$	$(52,375)$	$[0:1:0]$	$(2,5)$	$\left(\frac{1}{4},\frac{33}{8}\right)$	$\left(-\frac{64}{25},-\frac{59}{125}\right)$

Note that while the sum of rational points is always rational, the sum of integer points is usually not an integer point. In fact, a theorem of Axel Thue from 1908 shows that equations of the form $y^2 = x^3 + c$ (for any integer constant c) can have only finitely many integer solutions.