ELLIPTIC CURVES PROBLEM SET III
(B. CONRAD, LISBON SUMMER SCHOOL, 2011)

III.1. The rational right triangle $(3/2, 20/3, 41/6)$ with area 5 gives rise to the rational point $(-4, 6)$ on $y^2 = x^3 - 25x$. But in terms of algebra, we can change signs on the numbers 3/2, 20/3, and 41/6 and get *more* such rational points:

(i) Using sign changes, discover the following additional rational points: $(-4, -6)$ and $(25/4, \pm 75/8)$. Graph the picture of these points on the cubic curve.

(ii) Join such pairs not on the same vertical line and find yet more rational points on the curve. Going backwards, produce more impressive rational right triangles with area 6.

III.2. The curve $y^2 = x^3 - 49x$ has the rational point $(25, 120)$. Check it.

(i) Using the formulas, discover the "triangle" $(-24/5, -35/12, 337/60)$. What point on the elliptic curve corresponds to the genuine triangle $(24/5, 35/12, 337/60)$?

(ii) Now you have two points on the curve not on the same vertical line. Compute where their secant line meets the curve, and discover another triangle with area 7. Keep going.

III.3. Generalize Exercise II.2(ii): if $n \geqslant 1$ and $E_n = \{y^2 = x^3 - n^2 x\}$ then for $p \nmid 6n$ (so E_n "makes sense" as an elliptic curve over $\mathbf{F}_p$) then prove that $\#E_n(\mathbf{F}_p) = p + 1$.

III.4. Let $E = \{y^2 = x^3 + ax^2 + bx + c\}$ be an elliptic curve over $\mathbf{Q}$. Although we have not defined a notion of "isomorphism" (or even "map") between elliptic curves, this exercise will convince you that there are some simple coordinate changes which should be regarded as not giving an essentially different elliptic curve.

(i) Making the coordinate change $x \mapsto x - a/3$, convert the given curve E into a new elliptic curve $E' = \{y^2 = x^3 + b'x + c'\}$ over $\mathbf{Q}$. Explain why this coordinate change carries lines to lines, and so respects the group law on $E(\mathbf{Q})$ and $E'(\mathbf{Q})$.

(ii) Consider a coordinate change $(x, y) \mapsto (w, z) = (u^2 x, u^3 y)$ applied to E', with $u \in \mathbf{Q}^\times$. Show that this carries E' over to the elliptic curve $E'' = \{z^2 = w^3 + (u^4 b')w + (u^6 c')\}$. Check that the ratio $j = 108 \cdot (4b'^3)/(4b'^3 + 27c'^2)$ (whose funny constants are motivated by the complex-analytic theory) remains unchanged by such coordinate changes. This is called the *j-invariant* of the elliptic curve. It detects "isomorphism" over an algebraically closed ground field (such as $\mathbf{C}$), but not over $\mathbf{Q}$ (as (iii) will illustrate).

(iii) The elliptic curves $E_k = \{y^2 = x^3 - k\}$ for $k \in \mathbf{Q}^\times$ all have j-invariant 0. For $k, k' \in \mathbf{Q}^\times$, check that E_k can be converted to $E_{k'}$ by some coordinate change of the form

$$(x, y) \mapsto (u^2 x + r, u^3 y)$$

for $u, r \in \mathbf{Q}$ with $u \neq 0$ (the output of the right definition of "isomorphism" for elliptic curves over $\mathbf{Q}$ of the form $y^2 = f(x)$) if and only if $k/k' \in (\mathbf{Q}^\times)^6$. For $k \in \mathbf{Z}$ check that when $p \equiv 2 \bmod 3$ (so $t \mapsto t^3$ is an automorphism of $\mathbf{F}_p^\times$!) and $p \nmid 6k$ then $\#E(\mathbf{F}_p) = p + 1$.