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

II.1. A $\mathbf{Q}$-point on $y^2 = x^3 - 2$ is $(129/100, 383/1000)$ and a $\mathbf{Q}$-point on $y^2 = x^3 - 11$ is $(9/4, 5/8)$. The denominators in these examples suggest part (i) below.

(i) For each $k \in \mathbf{Z} - \{0\}$, show that every $\mathbf{Q}$-point on $y^2 = x^3 + k$ has the form $(x, y) = (a/c^2, b/c^3)$ for some $a, b, c \in \mathbf{Z}$ with $c \neq 0$ and $\gcd(a, c), \gcd(b, c) = 1$.

(ii) If $f(t)$ and $g(t)$ are monic polynomials with coefficients in $\mathbf{Z}$, does every solution $(x, y) \in \mathbf{Q}^2$ to $f(y) = g(x)$ have the form $(x, y) = (a/c^m, b/c^n)$ where $m = \deg f$ and $n = \deg g$? This would generalize (i) by using $f(t) = t^2$ and $g(t) = t^3 + k$.

II.2. For the elliptic curve $E : y^2 = x^3 - 25x$, $E(\mathbf{Q})$ contains $(0, 0)$, $(\pm 5, 0)$, and $P = (-4, 6)$.

(i) Determine where E meets the line joining P to each of $(0, 0)$, $(5, 0)$, and $(-5, 0)$, and then compute the sum of P with each of these points (don't forget to reflect across the x-axis).

(ii) For $p > 5$ with $p \equiv 3 \bmod 4$, show that when $x \neq 0, \pm 5 \bmod p$ exactly one of $(\pm x)^3 - 25(\pm x) = \pm(x^2 - 25x)$ is a square in $\mathbf{F}_p^\times$. Deduce that $\#E(\mathbf{F}_p) = p + 1$ for such p (don't forget to include the point ∞). For $p = 7$, deduce that $E(\mathbf{F}_p) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ from knowledge of the size and 2-torsion; then find an explicit point of order 4. How about $p = 19$? And $p = 31$?

II.3. In this problem, work with the elliptic curve $y^2 = x^3 + 17$ over $\mathbf{Q}$.

(i) Verify that $(2, 5) \oplus (4, 9) = (-2, 3)$ and $[2](-1, 4) = (137/64, -2651/512)$.

(ii) Verify that $(8, -23) \oplus (-2, 3) \oplus (2, -5) = (52, 375)$ by computing the triple sum in two different ways (i.e., check associativity in this example).

II.4. (i) Verify that $(0, 4)$ has order 3 on $y^2 = x^3 + 16$ by computing the tangent line at this point and checking for a triple root.

(ii) Verify that $P = (0, -4)$ has order 4 on $y^2 = x^3 - 3x^2 - 8x + 16$ by checking that $[2](P)$ lies on the x-axis (and so has order 2).

II.5. Let E be the elliptic curve $y^2 = x^3 - 2$ over $\mathbf{Q}$.

(i) For $P = (3, 5)$, check that $[2](P) = (129/100, 383/1000)$. Then compute $[3](P)$. (Its numerator and denominator will have around 14 digits!)

(ii) Write a computer program to add points on $y^2 = x^3 - k$ (taking care when ∞ intervenes), and set $k = 2$ to compute $[n](P)$ for $n = 3, 4, 5, \ldots$. (Beware that the number of digits in the numerator and denominator grows roughly quadratically in n for points of infinite order.)

(iii) What is the order of P when the elliptic curve E is viewed over $\mathbf{F}_5$? How about $\mathbf{F}_p$ for $p = 7, 11, \ldots$? Can you make sense of a "reduction map" $E(\mathbf{Q}) \to E(\mathbf{F}_p)$ for $p > 3$ (which points should go to ∞?), and is it a homomorphism?