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

I.1. For $n, m \in \mathbf{Z}$ with $\gcd(n, m) = 1$, prove that $(n^2 - m^2, 2mn, n^2 + m^2)$ is primitive when n and m have opposite parity and that $\gcd(n^2 - m^2, 2mn, n^2 + m^2) = 2$ for odd n and m.

I.2. (i) Using the base point $(3/5, 4/5)$ on $C = \{u^2 + v^2 = 1\}$, adapt the method of parameterization of C via the base point $(-1, 0)$ to obtain another parameterization of C:

$$(u(t), v(t)) = \left(\frac{3t^2 - 8t - 3}{5(t^2 + 1)}, \frac{-4t^2 - 6t + 4}{5(t^2 + 1)}\right),$$

with $u(t), v(t) \in \mathbf{Q}$ if and only if $t \in \mathbf{Q} \cup \{\infty\}$. Explain geometrically why $(u(0), v(0)) = (-3/5, 4/5)$, $(u(\infty), v(\infty)) = (3/5, -4/5)$, and $(u(-3/4), v(-3/4)) = (3/5, 4/5)$.

(ii) Using (i), deduce the parameterization of nonzero $\mathbf{Z}$-points on $x^2 + y^2 = z^2$:

$$(3m^2 - 8mn - 3n^2, -4m^2 - 6mn + 4n^2, 5(m^2 + n^2))$$

with $m, n \in \mathbf{Z}$ not both zero. Can you describe in terms of n and m when this is primitive?

I.3. (i) Using the base point $(1, 1)$, show that $\{u^2 + v^2 = 2\}$ admits the parameterization

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

and use this to parameterize the nonzero $\mathbf{Z}$-points on $x^2 + y^2 = 2z^2$ (and compute lots of explicit primitive nonzero $\mathbf{Z}$-points). Can you parameterize the primitive solutions?

(ii) Parameterize the $\mathbf{Q}$-points on the hyperbola $u^2 - 7v^2 = 1$ using the base point $(1, 0)$, and the $\mathbf{Q}$-points on the ellipse $3u^2 + 2v^2 = 5$ using the base point $(1, 1)$. Can you describe the $\mathbf{Z}$-points on $u^2 - 7v^2 = 1$ (i.e., $\mathbf{Z}$-points on $x^2 - 7y^2 = z^2$ with $z = \pm 1$)?

I.4. (i) Prove that $x^2 + y^2 = 3z^2$ has *no* nonzero solution in $\mathbf{Z}$ by assuming there is one and passing to a primitive solution and considering it modulo 3 (noting that -1 is not a square mod 3). Deduce that $u^2 + v^2 = 3$ has *no* $\mathbf{Q}$-point.

(ii) Use mod-3 considerations to likewise prove that $7x^2 - 23y^2 = 15z^2$ has no nonzero $\mathbf{Z}$-solution, so $7u^2 - 23v^2 = 15$ has no $\mathbf{Q}$-point.

(iii) If $a, b, c \in \mathbf{Z} - \{0\}$ are pairwise relatively prime and squarefree and $ax^2 + by^2 = cz^2$ has a nonzero $\mathbf{Z}$-point then prove that $-ab$ is a square mod c, ac is a square mod b, and bc is a square mod a. Deduce that these three congruential conditions are *necessary* for $au^2 + bv^2 = c$ to have a $\mathbf{Q}$-point, and verify them for $(a, b, c) = (7, 23, 15)$. (Gauss and Legendre proved that these necessary conditions are *sufficient* when the conic has an $\mathbf{R}$-point; e.g., $a, b, c > 0$.)

I.5. Use our parameterization of $\{u^2 + v^2 = 1\}$ to explain the $\tan(\theta/2)$-substitution converting $\int R(\cos\theta, \sin\theta)\mathrm{d}\theta$ for rational functions $R(x, y)$ into $\int f(t)\mathrm{d}t$ for a rational function $f(t)$.