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

IV.1. This exercise uses the Pythagorean parameterization (away from the base point $(-1,0)$!) to "rediscover" the link between the congruent number problem and elliptic curves.

(i) By considering x/z and y/z, explain why triples in $\mathbf{Q}$ satisfying $x^2+y^2=z^2$ with $z \neq 0$ and $x \neq -z$ have the unique form $(x,y,z) = (\lambda(1-t^2), \lambda \cdot 2t, \lambda(1+t^2))$ with $\lambda, t \in \mathbf{Q}$ and $\lambda \neq 0$. (Note that $t=0$ corresponds to triples with $x=z$.)

(ii) Show that imposing $(1/2)xy = n$ (with a fixed $n \neq 0$, which forces $y \neq 0$ and hence $x \neq -z$ and $z \neq 0$) amounts to giving $\lambda, t \in \mathbf{Q}$ such that $\lambda^2 t(1-t^2) = n$.

(iii) Expressing (ii) in the form $(-t)^3 - (-t) = n/\lambda^2$ (to "separate the variables"), multiply through by n^3 on both sides to obtain $(-nt)^3 - n^2(-nt) = (n^2/\lambda)^2$. Voila!

IV.2. Fix a prime $p > 3$, and let E be an elliptic curve over $\mathbf{Q}_p$ defined by $y^2 = f(x)$ for a monic cubic f having coefficients in $\mathbf{Z}_p$ and discriminant in $\mathbf{Z}_p^\times$. Let $\overline{E}$ be the elliptic curve over $\mathbf{F}_p$ defined by $y^2 = \overline{f}(x)$, where $\overline{f} \in \mathbf{F}_p[x]$ is f mod p (i.e., reduce the coefficients of f modulo p). Define a map of sets $E(\mathbf{Q}_p) \to \overline{E}(\mathbf{F}_p)$ by sending $E(\mathbf{Z}_p)$ into $\overline{E}(\mathbf{F}_p) - \{\infty\}$ by coordinate-wise reduction modulo p and sending all other points to ∞.

(i) Show that any line in $\mathbf{Q}_p^2$ (not necessarily through $(0,0)$) has the form $ax+by+c=0$ with $a,b,c \in \mathbf{Z}_p$ and at least one of a,b,c in $\mathbf{Z}_p^\times$, and construct a "reduction mod p" map $L \mapsto \overline{L}$ from lines in $\mathbf{Q}_p^2$ to lines in $\mathbf{F}_p^2$. Check that $\overline{L}$ is vertical if L is vertical.

(ii) For $P \in E(\mathbf{Z}_p)$ with reduction $\overline{P} \in \overline{E}(\mathbf{F}_p) - \{\infty\}$, show that $\overline{T_P(E)} = T_{\overline{P}}(\overline{E})$.

(iii) For distinct $P, Q \in E(\mathbf{Z}_p)$, show that the reduction of the secant line PQ is the secant line $\overline{P}\,\overline{Q}$ when $\overline{P} \neq \overline{Q}$ and is the tangent line $T_{\overline{P}}(\overline{E})$ when $\overline{P} = \overline{Q}$.

(iv) Show that if P lies outside $E(\mathbf{Z}_p)$ then PQ has vertical reduction (treat $Q \in E(\mathbf{Z}_p)$ and $Q \notin E(\mathbf{Z}_p)$ separately), and deduce that $E(\mathbf{Q}_p) \to \overline{E}(\mathbf{F}_p)$ is a *homomorphism*.

IV.3. Dirichlet's theorem on primes in arithmetic progressions says that for any $a, b \in \mathbf{Z}^+$ such that $\gcd(a,b) = 1$, there are infinitely many primes $p \equiv a \bmod b$.

(i) Prove that $\gcd_{p \equiv 2 \bmod 3, p > 1000}(p+1) = 3$. (Hint: Pick one such p_0, so $p_0 + 1 = 3k$ for $k \in \mathbf{Z}$. Seek $p \equiv 2 \bmod 3$ with $p > 1000$ so that $p+1 = 3k'$ with $\gcd(k', k) = 1$; first assume $\gcd(3,k) = 1$ and apply Dirichlet's theorem for the modulus $3k$.)

(ii) Fix an integer $N > 0$. Prove that as we vary through all primes $p \equiv 3 \bmod 4$ with $p > N$, the gcd of the numbers $p+1$ is exactly 4. Can you generalize further?

IV.4. In Lecture IV we saw that for the elliptic curve $E_n = \{y^2 = x^3 - n^2 x\}$ and any prime $p \nmid 6n$, the reduction map $E_n(\mathbf{Q})_{\mathrm{tors}} \to E_n(\mathbf{F}_p)$ is injective on prime-to-p torsion. Using IV.2(iv), prove that $\#E_n(\mathbf{Q})_{\mathrm{tors}}$ divides $\gcd_{p \equiv 3 \bmod 4, p > N}(p+1)$ for some $N > 0$, and use IV.3(ii) to deduce that $E_n(\mathbf{Q})_{\mathrm{tors}} = E_n[2]$.