ELLIPTIC CURVES
POSSIBLE PROJECTS

(1) An elliptic curve over $\mathbb{Q}$ has a minimal Weierstrass equation, but this equation may not be the equation with the smallest coefficients. Explain this, give some examples, and try to find an algorithm (*reduction theory*) which gives an equation requiring the fewest number of bits.

(2) Let E be an elliptic curve over an imaginary quadratic field K of rank 1 with torsion group $T = E(K)_{\text{tors}}$. Let $\phi : E \to E'$ be the isogeny with kernel $\ker \phi = T$. Then E' has rank 1; let P' be a generator. Let $L = K(\phi^{-1}(P'))$ be the extension of K obtained by adjoining all points $P \in E(\overline{K})$ such that $\phi(P) = P'$. Then L/K is an abelian extension with Galois group a subgroup of T. Under what circumstances is L Galois not just over K, but Galois over $\mathbb{Q}$?

(3) Take the tables of Hilbert modular forms over totally real quartic and quintic fields and see if there are any further elliptic curves with *sporadic* torsion subgroups.

(4) Question of Brian Conrad: among ordinary elliptic curves over finite fields:
    (a) When is the endomorphism ring of an elliptic curve a maximal order?
    (b) When is the subring generated by Frobenius the entire endomorphism ring of the elliptic curve?
    (c) When is the subring generated by Frobenius a maximal order?

    "When" is supposed to be in some precise statistical sense—you could either consider all ordinary curves over a fixed $\mathbb{F}_q$, and then let $q \to \infty$; or take a fixed elliptic curve over $\mathbb{Q}$ and let $p \to \infty$. If you know the answers to (i) and (ii), you know the answer to (iii), but an answer to any one of them would be interesting.

Date: August 10, 2016.