INVERSE POINT COUNTING
STEVENSON

ROBERT C. RHOADES

ABSTRACT. These are my notes from a talk by Stevenson in the Stanford University Number Theory seminar. All mistakes are my own.

The problem we deal with is:

Given \( N \) find a smooth projective variety of type \( X \) with \( N \) points and solve the problem efficiently.

Of course there is a question of what \( F \) is. Here we take only \( N \) and produce \( F \) and \( X \). Furthermore, the genus will be 1 or 2. Schoof showed that for genus 1 you can count the number of points on \( E/F \) in polynomial time.

Before we answer the question of constructing such a genus 1 curve let us consider the issue of existence. A curve over \( F_p \) has between \( q + 1 - 2\sqrt{q} \) and \( q + 1 + 2\sqrt{q} \) points. Let \( H_p = [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}] \). Does \( \cup_{p \text{ prime}} H_p \supseteq \mathbb{Z}_{\geq 0} \)? This is a question about how big the gaps between primes can be. Primes between consecutive squares is beyond the reach of GRH. Note that prime powers are thin and so it doesn’t help to introduce them.

None-the-less there is a naive algorithm of order \( O(N^{1/2+\epsilon}) \). This is a CM-algorithm to construct a CM curve. In such a set up, we know about \( \text{End}(E) \) and we need only to know what \( \text{Frob}_p \) looks like inside \( \text{End}(E) \). The characteristic polynomial of \( \text{Frob}_p \) is

\[
f_{\text{Frob}_p} = x^2 - tx + p
\]

The number of points on the curve is

\[
|E(F_p)| = p + 1 - t
\]

So we need \( N = p + 1 - t \). We know that \( \Delta = t^2 - 4p < 0 \) and that \( \mathbb{Z}[\text{Frob}_p] \simeq \mathcal{O}_\Delta = \mathbb{Z}[(\Delta + \sqrt{\Delta})/2] \). Furthermore, \( \text{Frob}_p \leftrightarrow \pi = t + \sqrt{\Delta} \). Writing down the elliptic curve is almost the same as writing down the \( j \)-invariant. So we need to find a \( j \)-invariant in \( \mathbb{F}_p \) so that \( \mathbb{Z}[\text{Frob}_p] \simeq \mathcal{O}_\Delta \) over \( \mathbb{C} \) one can write down \( E/\mathbb{C} \) up to equivalence having \( \text{End}(E) \simeq \mathcal{O}_\Delta \). This corresponds to an ideal class of \( \mathcal{O}_\Delta \) by CM theory. That is, there is an \( I \subset \mathcal{O}_\Delta \subset \mathbb{C} \), an ideal, and \( \mathbb{C}/I \) is the desired elliptic curve. Furthermore, the Hilbert class polynomial is given by

\[
H_\Delta = \prod_{I \in \text{Pic}(\mathcal{O}_\Delta)} (x - j(\mathbb{C}/I)) \in \mathbb{Z}[x]
\]

Then \( H_\Delta \) splits in \( \mathbb{F}_p[x] \) and any root is the correct elliptic curve up to twisting.

**BUT** \( \deg(H_\Delta) \sim |\Delta|^{1/2} \sim N \) and the coefficients are huge. So algorithmically it seems to be of run time \( O(N^{1+\epsilon}) \) but we are free to pick \( p \). So we may try to make \( \Delta \) small. So that \( \mathbb{Q}(\sqrt{\Delta}) = K \supset \mathcal{O} \supset \mathcal{O}_\Delta \) is small and we replace everything by \( \mathcal{O} \) the maximal guy in \( K \). Then \( \text{disc}(K) \) controls the size.

*Date: July 13, 2010.*
Bröker wrote a thesis saying given $N$, and a prime $p$, such that heuristically $t \Delta_K = O(\log^2(N))$. For the heuristic we consider $N = \nu \varpi$ and $p = \pi \overline{\pi}$ such that $\nu + \pi = 1$ ($1^2 - tp = N$). Then we look for the smallest $\Delta = -3, -4, \cdots$ so that it splits as above. Then we split $N$ in $O_\Delta$. Compute the norm of $1 - \nu$ if norm is $p$ we are done.

During the talk there was a remark asking if this was Cramer’s conjecture. If the norms are random then we expect $\log(N)$ trials but splitting is obstructed by the class numbers. We have

$$\sum_{|\Delta| < X} \frac{1}{h(\Delta)} \approx \int_2^X \frac{dt}{\sqrt{t}} \approx \sqrt{X}.$$ 

So you expect this many to split and expect to go up to $\log(N)$ values to get a prime.

Alternatively one looks for a prime with $p + t - 1 = N$ and $t^2 - 4p$ small. So we need to find the probability of a prime that solves this. The question is: How many primes satisfy a linear constraint and a quadratic constraint?

In genus 2 we have the following: $C : y^2 = g(x)$ with $g$ of degree 5 or 6. $N$ may be $|C(\mathbb{F}_p)| \sim p$ or $|J(\mathbb{F}_p)| \sim p^2$.

$$f_{\text{Frob}} = x^4 - ax^3 + bx^2 - px + p^2$$

with $|a| \leq 4\sqrt{p}$ and $|b - 2p| \leq 4p$. Call $\pi$ a root if $K = \mathbb{Q}(\pi)/K_0 = \mathbb{Q}(\pi + \overline{\pi})$ of degree 2. Write $\Delta_K = f(\Delta_\pi^2) = \Delta_1 \Delta_2$. Genus 2 CM involves Igusa class polynomials and 3 invariants specify $C$. Igusa class polynomials play analog of $H_\Delta$. Coefficients are in $\mathbb{Q}$ not in $\mathbb{Z}$ and so one must bound denominators in addition to problems from before. But the runtime is $O(\Delta_K^{7/2+\epsilon})$.

**Theorem 0.1** (Howe, Lauter, S). CM in genus 2 to produce $J(C)$ of given order is necessarily exponential in $\log(N)$.

$$\limsup_{N \to \infty} \frac{\Delta_{\text{min}}(N)}{\sqrt{N}} = +\infty$$

Can you realize all $N < B$ by CM methods? How many $K$ can you encounter via these methods? But each $K$ yields $O(B^{1/2}/\log(B))$ polynomials. Then the number of $K$ to do all $N < B$ will be $B^{1/2} \log(B)$.

Can do $|C(\mathbb{F}_p)| = N$, but here you cheat a bit since $|C(\mathbb{F}_p)| = p + 1 - a$ and $|J(\mathbb{F}_p)| = f_{\text{Frob}}(1)$. So you see you have so much choice in the parameter $b$ that you can choose $b$ so that $J(C) \simeq E_1 \times E_2$. This implies that $f = (x^2 - t_1 x + p)(x^2 - t_2 x + p)$. Which in turn implies $|C(\mathbb{F}_p)| = p + 1 - t_1 - t_2 = N$. So we can glue $E_1$ with $|E_1(\mathbb{F}_p)| = N$ and a super singular elliptic curve.

$$0 \to \Gamma \to E_1 \times E_2 \to J(C) \to 0$$

and $\Gamma$ is the graph of $E_1(n) \to E_2[n]$ and an antiisomorphism with respect to Weil pairing.