Faster computation of Heegner points on elliptic curves over Q of rank 1

B. Allombert

IMB
CNRS/Université Bordeaux 1

10/09/2014

Lignes directrices

Credits

We are presenting the latest optimisation in our implementation of an algorithm for computing a non-torsion rational point over a rank-1 rational elliptic curve which is due to J.H. Silverman J. Cremona and C. Delaunay, with improvements by N. Elkies, and M. Watkins. The survey "Some remarks on Heegner point computations" by M. Watkins is a great resource.
This work was done with the help of P. Molin.
Our optimisation mostly concern the practical computation of points with very large heights.

Introduction

Let E be an elliptic curve défined over $\mathbb{Q}$ of (analytic) rank 1.
We want to compute a non-torsion point of $E(\mathbb{Q})$.
More precisely under the Birch and Swinnerton-Dyer conjecture

Conjecture (Birch and Swinnerton-Dyer)

$$L'(E,1) = \frac{\Omega_{re}\left(\prod_{p|N\infty} c_p\right)|Ш_E|R_E}{{E(\mathbb{Q})_{tors}}^2} \quad .$$

where L is the L-function associated to E, the c_p are the local Tamagawa numbers, $Ш_E$ is the analytic Ш and R_E is the elliptic regulator.

We want to compute a rational point P of height $|Ш_E|R_E$ (unique up to torsion and inverse).

Quadratic surd

A complex number $\tau \in \mathbb{C}$ is an imaginary quadratic surd if $\Im\tau \neq 0$ and $\dim_{\mathbb{Q}}(1, \tau, \tau^2) = 2$. We associate to it

1. The minimal polynomial of τ is $P_\tau = a(x - \tau)(x - \overline{\tau})$, where a is such that the content of P is 1.
2. The discriminant $\mathrm{Disc}(\tau) = \mathrm{Disc}(P_\tau)$.

Heegner points

An imaginary quadratic surd is an Heegner point of level N if $\Im\tau > 0$ and $\mathrm{Disc}(\tau) = \mathrm{Disc}(N\tau)$.

Theorem

The set $\mathcal{H}_N^D$ of Heegner points of level N and of discriminant D is invariant by $\Gamma_0(N)$ acting by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}.\tau \mapsto \frac{a\tau+b}{c\tau+d}$

Theorem

Let $\mathcal{H}_N^D$ be the set of Heegner points of level N and of discriminant D, and $S(D,N)$ be the set of square roots modulo $2N$ of $D \pmod{4N}$, then

$$\mathcal{H}_N^D/\Gamma_0(N) \cong S(D,N) \times \mathcal{C}\ell(\mathbb{Q}(\sqrt{D})) \ .$$

This result allow to compute a set of representative of $\mathcal{H}_N^D/\Gamma_0(N)$ from the class group of $\mathcal{C}\ell(\mathbb{Q}(\sqrt{D}))$.

Shimura Reciprocity

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N and of Manin constant equal to 1. Let Λ be its associated period lattice, $\wp$ its associated Weierstraß function and $\mathcal{P}(z) = (\wp(z), \wp'(z))$ the map $\mathbb{C}/\Lambda \mapsto E(\mathbb{C})$. Let $q(\tau) = \exp(2i\pi\tau)$, and

$$\phi(\tau) = \sum_{n\geq 1} \frac{a_n}{n} q(\tau)^n$$

.

Theorem

If $\tau \in \mathcal{H}_N^D$, then $\mathcal{P}(\phi(\tau))$ belongs to the Hilbert class field of $\mathbb{Q}(\sqrt{(}D))$.

Theorem

Let $b \in S(D, N)$ and set

$$H_N^D(b) = \{\tau \in H_N^D | \mathrm{Tr}\tau / \mathrm{Norm}\tau = b\} \backslash \Gamma_0(N) \quad ,$$

then $P_D = \mathcal{P}(\sum_{\overline{\tau} \in \mathcal{H}_N^D(b)} \phi(\tau)) \in E(\mathbb{Q})$.

Note that this formula gives a lots of choice: D, b and each representatives τ.

Lifting the imaginary part of τ

It is important to choose representative quadratic surds τ modulo $\Gamma_0(N)$ such that $|\exp(2IPi\tau)|$ be as small as possible, so that the series ϕ converges faster.
If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, then $\Im \frac{a\tau+b}{c\tau+d} = \frac{2a}{|c\tau+d|^2}$. Thus maximizing $\Im \frac{a\tau+b}{c\tau+d}$ with $N|c$ is equivalent to minimizing the binary integral quadratic form $f(X,Y) = |NX\tau + Y|^2 = \mathrm{Norm}\tau N^2X^2 - \mathrm{Tr}\tau NXY + Y^2$. under the condition that Y is coprime to N which can be solved by enumerating the short vectors of f

Atkin-Lehner Involution

Let $Q \| N$, and u, v so that $uQ^2 - vN = Q$. The Atkin-Lehner involution W_Q is defined by $W_Q(\tau) = \frac{uQ\tau+v}{N\tau+Q}$.

Theorem

$$\phi(\tau) = \epsilon_Q \phi(W_Q(\tau)) + \phi(W_Q(i\infty))$$

where $\epsilon_Q = \prod_{p|Q} \epsilon_p$. $\mathcal{P}(\sum_{\tau \in \mathcal{H}_N^D(b)} \phi(W_Q(\tau))) = P +$ *torsion.*

The use of Atkin-Lehner involutions allows yet more choice for the values of τ. In particular it allows to ensure that $\Im\tau > \frac{1}{N}$.

Theorem of Gross-Zagier

Theorem (Gross-Zagier)

Let $D < -4$ be a fundamental discriminant such that D is an invertible square modulo $4N$, then

$$h(P_D) = \frac{\sqrt{-D}}{4\Omega_{vol}} L'(E,1)L(E_D,1) \quad .$$

Gross-Hayashi conjecture

More generally, it is expected that

Conjecture (Gross-Hayashi)

Let $D < 0$ be a fundamental discriminant such that D is a square modulo $4N$, then

$$h(P_D) = \frac{\sqrt{-D}}{4\Omega_{vol}} L'(E,1)L(E_D,1)2^{\omega(pgcd(D,N))}\frac{w(D)^2}{4} \quad .$$

This allows more choice for D.

Consequences

- P_D is torsion if and only if $L(E_D, 1) = 0$.
- The index $\ell^2 = h(P_D)/h(P)$ is computable.

Thus we chose D in some finite set and b so that $L(E_D, 1) \neq 0$ and the lifting of the τ gives the largest imaginary part.

Cremona-Silverman trick

Let write $P = [x/d^2, y/d^3]$ with x, y and d integers and d minimal then $d = h(P) - h_\infty(P) - \sum_{p|N} h_p(P)$.

Theorem (Cremona-Silverman trick)

The local heights h_p can only take a finite number of values depending on the Kodaira type of E at p.

By trying all the possibilities, we find a relatively small number of candidate values for d. This allows to recover a rational expression for P from an approximate expression for P_D.

The algorithm requires the computation of series of the form $S_i = \Re \sum_{n=1}^{N_i} \alpha_n {q_i}^n$, for $1 \leq i \leq k$, where the q_i are complex numbers with $|q_i| < 1$ and $\alpha_n = a_n$ (for $L'1$) or $\alpha = a_n/n$ (for ϕ).
Estimating the value of N_i needed to get the right accuracy b (in bit) is easy.
There are two tricks that can be used to speed up the computation.

Bulher-Gross iteration

The Bulher-Gross iteration allows to compute all the needed a_n while computing the value a_p for p prime only once but generates them in the lexicographic order of the exponents, e.g. for $n = 20$, the order is
$1, 2, 2^2, 2^3, 2^4, 3, 3 \times 2, 3 \times 2^2, 3^2, 3^2 \times 2, 5, 5 \times 2, 5 \times 4, 5 \times 3, 7, 7 \times 2, 11, 13, 17, 19$
i.e.
1, 2, 4, 8, 16, 3, 6, 12, 9, 18, 5, 10, 20, 15, 7, 14, 11, 13, 17, 19.
The storage requirement is $\sqrt{N}$ entries.

Brent and Kung series evaluation

Brent and Kung fast series evaluation method allow to reduce the number of multiplications by q to $2\sqrt{N}$ instead of N using a baby-step giant-step method. If $M = \lceil \sqrt{N} \rceil$, then

$$S = \sum_{m=0}^{M} \left(\sum_{n=0}^{M-1} \alpha_{n+Mm} q^n \right) q^{mM}$$

The storage requirement is of $\sqrt{N}$ entries.

The problem is to use both methods at once while still using $O(\sqrt{N})$ memory.
Zeroth method: Precompute the baby-step $({q_i}^n)_{n=0}^M$ and the giant-step $({q_i}^{Mn})_{n=0}^M$ for $1 \leq i \leq k$
Generate the a_j using Bulher-Gross iteration. Each time a new a_j is generated, write $j = n + mM$ and add $a_j {q_i}^n {q_i}^{Mm}$. Slow but require $2Mbk$ (if $N = 10^9$, this means 4GB of storage.)

First method

Compute first all the a_n using Bulher-Gross iteration, then apply Brent and Kung summation. Fast but require $N \log_2 N$ bits of storage which might not be practical (if $N = 10^9$, this means 4GB of storage.)

Second method

Precompute the baby-step $({q_i}^n)_{n=0}^M$ for $1 \leq i \leq k$ and maintains an array $(A_{i,n})$ of size $k \times M$ for the giant-step set to 0.
Generate the a_j using Bulher-Gross iteration. Each time a new a_j is generated, write $j = n + mM$ and add $a_j {q_i}^n$ to $A_{i,m}$ for $1 \leq i \leq k$.
At the end returns $S_i = \sum_{m=1}^M A_{i,m} q^{mM}$ for $1 \leq i \leq k$. The storage is $2Mbk$. So this method is better when $2Mbk < N \log_2 N$.