Algorithm 8.1

Input: A problem

Output: An elliptic curve E over $\mathbb{F}_q$ with known cardinality providing a solution to the problem

1. Choose D, $q = p^f$ such that $4p^f = t^2 - v^2 D$ for some $t, v \in \mathbb{Z}$ (and there is no solution with a smaller f), and suitable $|E| = q + 1 - t$.
2. Compute
$$H_D(X) = \prod_{\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})} \big(X - j(\mathfrak{a})\big) \in \mathbb{Z}[X]$$
by Algorithm 8.2.
3. Compute a root $\bar{j} \in \mathbb{F}_q$ of H_D mod p.
4. $k = \frac{\bar{j}}{1728 - \bar{j}}$, γ quadratic non-residue in $\mathbb{F}_q$
5. **return** the one of
$$E : Y^2 = X^3 + 3kX + 2k \qquad E' : Y^2 = X^3 + 3k\gamma^2 X + 2k\gamma^3$$
with $|E| = q + 1 - t$ (for $D < -4$)

Algorithm 8.2

```
Input: $D < 0$ a quadratic discriminant
Output: $H_D \in \mathbb{Z}[X]$
Let $h = \#\mathrm{Cl}(\mathcal{O}_D)$.
Compute the reduced system of representatives $[A_k, B_k, C_k]$ of $\mathrm{Cl}(\mathcal{O}_D)$
for $k = 1, \ldots, h$:

    $$D = B_k^2 - 4A_kC_k, \quad \mathrm{gcd}(A_k, B_k, C_k) = 1, \quad |B_k| \leq A_k \leq C_k$$

and $B_k > 0$ if there is equality in one of the inequalities.
for $k = 1, \ldots, h$
        $\tau_k \leftarrow \frac{-B_k+\sqrt{D}}{2A_k} \in \mathbb{C}$
        $j_k \leftarrow j(\tau_k) \in \mathbb{C}$
$H_D \leftarrow \prod_{k=1}^{h}(X - j_k) \in \mathbb{C}[X]$
Drop the imaginary part of $H_D$, and round the coefficients to integers.
```

Siegel's theorem

Theorem (9.1)

$$h \in O\left(|D|^{1/2} \log |D|\right);$$

under GRH,

$$h \in O\left(|D|^{1/2} \log \log |D|\right), h \in \Omega\left(\frac{|D|^{1/2}}{\log \log |D|}\right).$$

Heights

Theorem (9.2, Enge2009,Schoof1991)

$$\mathrm{maxcoeff}(H_D) \leq Ch + \pi\sqrt{|D|} \sum_{k=1}^{h} \frac{1}{A_k} \in O\left(|D|^{1/2} \log^2 |D|\right) \subseteq \tilde{O}\left(|D|^{1/2}\right)$$

with $C = 3.01\ldots$.

Generic complexity

Theorem (10.1)

Called with a precision of $n \in O\left(|D|^{1/2} \log^2 |D|\right)$*, Algorithm 8.2 computes an approximation to* H_D *in time*

$$\begin{aligned} & O\left(h\, E(n) \mathrm{M}(n) + \log h\, \mathrm{M}_X(h,n)\right) \subseteq O\left((h\, E(n) + h \log^2 h) \mathrm{M}(n)\right), \\ \subseteq\ & O\left(E(n) + \log^2 |D|\right) |D| \log^4 |D| \log\log |D| \\ \subseteq\ & \tilde{O}\left(E(n)\, |D|\right) \end{aligned}$$

where $E(n)$ *is the number of floating-point operations needed to evaluate* j *at precision* n*.*

Naive complexity

Corollary (10.2)

Algorithm 8.2 can be carried out in

$$O(h\,n\,\mathrm{M}(n)) \subseteq O\left(|D|^{3/2}\,\log^6|D|\log\log|D|\right) \subseteq \tilde{O}\left(|D|^{3/2}\right).$$

Dedekind η

$$
\begin{aligned}
\eta(z) &= q^{1/24} \prod_{\nu=1}^{\infty} (1 - q^{\nu}) \\
&= q^{1/24} \left(1 + \sum_{\nu=1}^{\infty} (-1)^{\nu} \left(q^{\nu(3\nu-1)/2} + q^{\nu(3\nu+1)/2} \right) \right) \\
f_1(z) &= \frac{\eta(z/2)}{\eta(z)} \\
\gamma_2 &= \frac{f_1^{24} + 16}{f_1^{8}} \\
j &= \gamma_2^3
\end{aligned}
$$

Addition sequences for η

$$
\begin{aligned}
q^{\nu} &= q^{\nu-1} \cdot q \\
q^{2\nu-1} &= q^{2(\nu-1)-1} \cdot q^{2} \\
q^{\nu(3\nu-1)/2} &= q^{(\nu-1)(3(\nu-1)+1)/2} \cdot q^{2\nu-1} \\
q^{\nu(3\nu+1)/2} &= q^{\nu(3\nu-1)/2} \cdot q^{\nu}
\end{aligned}
$$

Smart complexity

Corollary (10.3)

Algorithm 8.2 can be carried out in

$$O\left(h\sqrt{n}\,\mathrm{M}(n)\right) \subseteq O\left(|D|^{5/4}\log^5|D|\log\log|D|\right) \subseteq \tilde{O}\left(|D|^{5/4}\right).$$

Multipoint evaluation

Corollary (10.4)

Algorithm 8.2 can be carried out in

$$O\left((n\log n + h\log^2 h)\mathsf{M}(n)\right) \subseteq O\left(|D|\,\log^6|D|\log\log|D|\right) \subseteq \tilde{O}\left(|D|\right),$$

which is quasi-linear in the output size

$$O\left(|D|\log^3|D|\right).$$

Implementation

- Record (E. 2009) (with class invariants)
  - $D = -2\,093\,236\,031$
  - $h = 100\,000$
  - Precision $264\,727$ bits
  - $260\,000$ s $= 3$ d CPU time
  - 5 GB
- Software
  - GNU MPC: complex floating point arithmetic in arbitrary precision with guaranteed rounding
    - Based on MPFR and GMP
    - LGPL
  - MPFRCX: polynomials with real (MPFR) and complex (MPC) coefficients
    - LGPL
  - `cm`: class polynomials and CM curves
    - GPL

Chinese remaindering idea

- Enumerate curves with CM by D over $\mathbb{F}_p$ for suitable p.
- Write down their j-invariants $j_1, \ldots, j_h \in \mathbb{F}_p$.
- Then

$$H_D(X) \bmod p = \prod_{k=1}^{h} (X - j_k).$$

- Trick: The p can be relatively small.
- Use several p, and lift by Chinese remaindering to $\mathbb{Z}$.

Slow Chinese remaindering

Input: $D < 0$ a quadratic discriminant
Output: $H_D \in \mathbb{Z}[X]$

Compute a set of primes $p_1, \ldots, p_r$ such that $4p_i = t_i^2 - v_i^2 D$ has integer solutions and

$$\sum_{i=1}^{r} \log p_i > Ch + \pi \sqrt{|D|} \sum_{k=1}^{h} \frac{1}{A_k} + \log 2$$

(the bound of Theorem 9.2, the $\log 2$ is for the sign).

Slow Chinese remaindering

```
for $i = 1, \ldots, r$ do
    $J \leftarrow \emptyset$
    for $j = 0, \ldots, p_i - 1 \in \mathbb{F}_{p_i}$ do
        if $E/\mathbb{F}_{p_i}$ with $j$-invariant $j$ has CM by $D$ then
            $J \leftarrow J \cup \{j\}$
        end if
    end for
    $H_D \bmod p_i \leftarrow \prod_{j \in J}(X - j)$
end for
$H_D \leftarrow \mathrm{CRT}(\{H_D \bmod p_i\})$
```

Complexity

Theorem

Assuming that checking the CM type of a curve is fast (polynomial in $\log |D|$*), the complexity of the algorithm is in*

$$\tilde{O}\left(|D|^{3/2}\right).$$

This is the same as the most naive version of the floating point algorithm…

Fast Chinese remaindering

Belding–Bröker–E.–Lauter 2008

```
for $i = 1, \ldots, r$ do
    $J \leftarrow \emptyset$
    for $j = 0, \ldots, p_i - 1 \in \mathbb{F}_{p_i}$ do
        if $E/\mathbb{F}_{p_i}$ with $j$-invariant $j$ has CM by $D$ then
            break
        end if
    end for
    Compute all the conjugates $J$ of $j$.
    $H_D \bmod p_i \leftarrow \prod_{j \in J}(X - j)$
end for
$H_D \leftarrow \mathrm{CRT}(\{H_D \bmod p_i\})$
```

Complexity

Theorem

Under GRH, the expected complexity of the algorithm is in

$$\tilde{O}\left(|D|^{1/2}\right).$$

Record

E.–Sutherland 2010 (with class invariants)

- $D = -1\,000\,000\,013\,079\,299 > 10^{15}$
- $h = 10\,034\,174$
- precision $21\,533\,832$ bits
- $438\,709$ primes of up to 53 bits
- 200 days CPU time
- 13 TB (?)
- 2 PB (?) without class invariants
- 200 MB modulo 255 bit prime

Bordeaux

UNESCO World Heritage Site since 2007

Sütterlin – Sütterlin

a b c d e f g h i j k l m n

o p q r s t u v w x y z ß

A B C D E F G H I J K L M N

O P Q R S T U V W X Y Z