**Problem.** Given an integer $N \geq 1$, find a finite field $\mathbb{F}_q$ and an elliptic curve $E/\mathbb{F}_q$ such that

$$|E(\mathbb{F}_q)| = N.$$

Necessary condition: there is a prime power $q$ such that

$$N \in \mathcal{H}(q) = [q - 2\sqrt{q} + 1, q + 2\sqrt{q} + 1].$$

We can (and will) restrict to *primes* $q$. The condition above is then also sufficient.

Needed: gap between primes is $O(\sqrt{q})$.
Known:

- $O(q^{0.55})$;
- GRH $\Rightarrow O(\sqrt{q}\log^2(q))$.

Heuristically: $O(\log(q))$.

# Naïve algorithm

- find a prime $q$ such that $N \in \mathcal{H}(q)$;
- let $a$ run over $\mathbb{F}_q$ and test whether

  $$E_a : y^2 = x^3 + ax - a$$

  has $N$ points.
  Fast check: test whether $P = (1, 1) \in E_a(\mathbb{F}_q)$ is annihilated by $N$;
- running time: $O(N^{1/2+\varepsilon})$.

  In example:
  $N = 1425091215750802$,
  $q = 1425091215750803$,
  first $a = ???$

## CM-approach

The desired curve $E/\mathbb{F}_q$ has Frobenius

$$F_q : E \to E \qquad (x, y) \mapsto (x^q, y^q).$$

Write $N = q + 1 - t$, then $F_q$ satisfies

$$F_q^2 - tF_q + q = 0 \in \mathrm{End}(E)$$

of discriminant $\Delta = t^2 - 4q < 0$.

Specifying $N$ is prescribing the *trace* of Frobenius $t$.

If $t \neq 0$, then $\mathrm{End}(E) \supseteq \mathcal{O}_\Delta \subset \mathbb{Q}(\sqrt{\Delta})$.

We want an elliptic curve with endomorphism ring $\mathcal{O} \supseteq \mathcal{O}_\Delta$.

## Deuring lifting theorem

Given $E/\mathbb{F}_q$ with $q+1-t$ points ($t \neq 0$), there exists a number field $H \supset K$ and an elliptic curve $\tilde{E}/H$ such that:

- there exists $\phi_q \in \mathrm{End}(\tilde{E})$ satisfying

$$\phi_q^2 - t\phi + q = 0 \in \mathrm{End}(\tilde{E});$$

- $q$ splits completely in $H$ and

$$\forall \mathfrak{q} | q : \mathrm{End}(\tilde{E} \bmod \mathfrak{q}) \cong \mathrm{End}(E).$$

We can lift $E$ *with* its endomorphism ring.

The lift $\tilde{E}$ is a CM-curve and CM-theory tells us how to compute $\tilde{E}$.

## CM-theory

$\mathcal{O}$ is a lattice in $K = \mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{C}$.

- $j(E_{\mathcal{O}}) \in H(K)$;
- $j(E_{\mathcal{O}})^{(\mathfrak{a},H/K)} = j(E_{\mathcal{O}\mathfrak{a}^{-1}})$;
- $[\mathbb{Q}(j(E_{\mathcal{O}})) : \mathbb{Q}] = h_K$;
- $H_{\mathcal{O}} = \prod_{\mathfrak{a} \in \mathrm{Cl}(D)} (X - j(\mathfrak{a})) \in \mathbb{Z}[X]$.

Moreover, $H_{\mathcal{O}} \in \mathbb{F}_q[X]$ splits completely. Its roots are the $j$-invariants of the curves having $q + 1 \pm t$ points.

## Selecting the discriminant

We want to have the discriminant of $K = \mathbb{Q}(\sqrt{t^2 - 4q})$ as small as possible.

Picking a prime $q$ for which $N$ is 'at the end' of $\mathcal{H}(q)$ yields $\mathrm{disc}(K) \approx N^{1/2}$.
In practice, we can also pick $q$ such that $\Delta = \Delta(q) = (q - 1 - N)^2 - 4N$ has a large square factor.

In the example:
$N$= 1425091215750802;
$q$ = 1425091291226311;
$t$ = 75475510;
$\Delta = t^2 - 4q = -3812555145144$;
$\Delta = -2^3 \cdot 3 \cdot 101 \cdot 39659^2$;
$D = -2^3 \cdot 3 \cdot 101 = -2424$.

# Computing $H_{\mathcal{O}}$

Classically:

- compute a list of reduced binary quadratic forms $[a, b, c]$ of discriminant $D$;

- approximate $j((-b+\sqrt{D})/2a)$ in some way and expand

$$H_{\mathcal{O}} = \prod_{[a,b,c] \in \mathrm{Cl}(D)} \left( X - j\left( \frac{-b+\sqrt{D}}{2a} \right) \right) \in \mathbb{Z}[X].$$

**Problems:**

- working over $\mathbb{C}$ yields *rounding errors*;

- the $j$-function is 'huge'. As example:

$$H_{\mathbb{Z}[\frac{-1+\sqrt{-163}}{2}]} = X + 262537412640768000.$$

## Solution to first problem

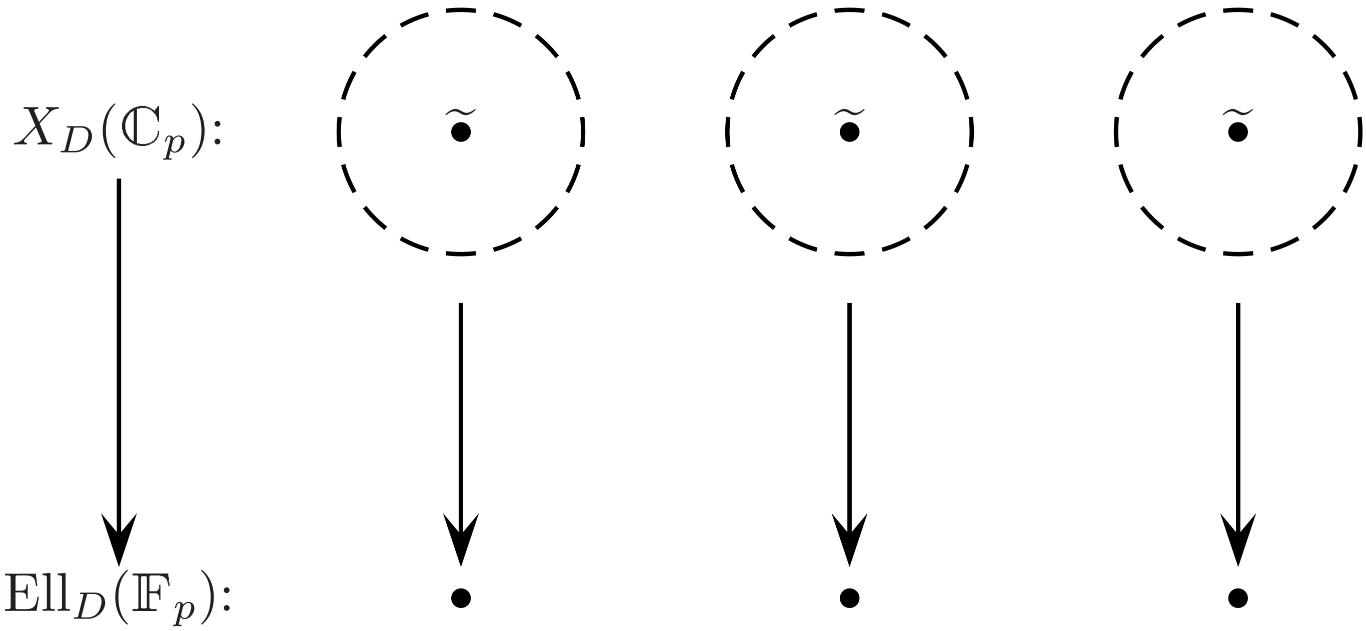
Work over the $p$-adics instead of over $\mathbb{C}$, i.e. embed $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$ for some $p$!

We now want: $\tilde{E}_p/\mathbb{C}_p$ with $\mathrm{End}(\tilde{E}_p) \cong \mathcal{O}_D$.

- find $(t, p)$ such that $t^2 - 4p = D$;
  in example: $t = 2$, $p = 607$;

- apply naïve algorithm to find $E_p/\mathbb{F}_p$ with trace $t$; this ensures $\mathrm{End}(E_p) \cong \mathcal{O}_D$.
  in example: $y^2 = x^3 + x + 67$

- 'Deuring lift' $E_p$ to its *canonical lift* $\tilde{E}_p$. In fact, $\tilde{E}_p$ has a model which is defined over $\mathbb{Z}_p$!




$$\mathrm{Ell}_D(\mathbb{F}_p) = \{E/\mathbb{F}_p : \mathrm{End}(E) = \mathcal{O}_D\}/_{\cong_{\overline{\mathbb{F}}_p}}$$

$$\#\mathrm{Ell}_D(\mathbb{F}_p) = h_K < \infty$$

$$X_D(\mathbb{C}_p) = \{E/\mathbb{C}_p : [\overline{E}] \in \mathrm{Ell}_D(\mathbb{F}_p)\}/_{\cong}$$

$$X_D(\mathbb{C}_p) \underset{j}{\hookrightarrow} \mathbb{C}_p$$

## Galois conjugates over $\mathbb{F}_p$

Let $I \subset \mathcal{O}_D$ be an $\mathcal{O}_D$-ideal prime to $p$. Define

$$E[I] = \{P \in E(\overline{\mathbb{F}}_p) \,|\, \forall \alpha \in I : [\alpha](P) = O_E\},$$

the group of $I$-torsion points.

Given $E$ and $S \subseteq E(\overline{\mathbb{F}}_p)$, there is an elliptic curve $E_S$ and a separable isogeny

$$\phi : E \to E_S \quad \text{with} \quad \ker \phi = S.$$

We obtain a bijection:

$$\overline{\rho}_I : \mathrm{Ell}_D(\mathbb{F}_p) \to \mathrm{Ell}_D(\mathbb{F}_p), \qquad [E] \mapsto [E_I].$$

Since principal ideals act trivially, we get an action of $\mathrm{Cl}(D)$ on $\mathrm{Ell}_D(\mathbb{F}_p)$.

# Lifting

**Couveignes & Henocq:** this action admits a natural lift to $X_D(\mathbb{C}_p)$!

Explicitly, there is a $p$-adic analytic map

$$\rho_I : X_D(\mathbb{C}_p) \to X_D(\mathbb{C}_p)$$

that induces the Galois action of $[I]$ on $\mathrm{Ell}_D(\mathbb{Q}_p)$.

If $I = (\alpha)$, with $\alpha \notin \mathbb{Z}$, then $\rho_\alpha$ stabilizes each disc and the CM-points are its *fixed points*.

Conclusion: we can use Newton iteration to converge to the canonical lift $\tilde{E}$!

# Explicit computation over $\mathbb{F}_p$

We want $(\alpha)$ to be smooth; in the example:

$$(\alpha) = (\phi+12) = (5, 2+\phi)^2 \cdot (31, 12+\phi) = L_5^2 \cdot L_{31}.$$

Of course $E_p/(\alpha) \cong E_p$, but for the lift we also need to know the action of the prime ideals $L_i$.

For any prime $l$, the $l$th modular polynomial $\Phi_l \in \mathbb{Z}[X, Y]$ parametrizes $l$-isogenies between elliptic curves.

Usually, $\Phi_l(X, j(E)) \in \mathbb{F}_p[X]$ has two roots if $l$ splits in $\mathrm{End}(E)$.

Roots of $\Phi_5(X, 46)$ : 68 and 377.

# Choosing the root

We *guess* that the correct $j$-value is 377.

The corresponding Frobenius eigenspace $S$ can be computed with 'Elkies techniques'. We get the $x$-coordinates of the points in $S$ as zeroes of

$$\overline{f}_5 = X^2 + 524X + 93 \in \mathbb{F}_p[X].$$

Since we know that the eigenvalue for $(5, 2 + \phi)$ is $-2 \in \mathbb{F}_5$, we just test whether

$$(X^p, Y^p) = -2 \cdot (X, Y)$$

holds for points in $S$, i.e. we compute $(X^p, Y^p)$ and $-2 \cdot (X, Y)$ in the ring

$$\mathbb{F}_p[X, Y]/(\overline{f}_5(X), Y^2 - X^3 - X - 63).$$

Our guess was incorrect, so now we *know* that the correct $j$-value is $68 \in \mathbb{F}_p$.

## Lifting the isogenies

We have constructed the lower line of the following diagram.

$$
\begin{array}{ccccccc}
E^* & \xrightarrow{\widetilde{\cdot/C_5}} & E_1^* & \xrightarrow{\widetilde{\cdot/C_5}} & E_2^* & \xrightarrow{\widetilde{\cdot/C_{31}}} & E_3^* \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
E & \xrightarrow{\cdot/C_5} & E_1 & \xrightarrow{\cdot/C_5} & E_2 & \xrightarrow{\cdot/C_{31}} & E_3 \cong E
\end{array}
$$

$E^*$ is just a 'stupid' lift of $E$.

In theory we can use Hensel/Vélu to lift the isogenies.

In practice: we know $j(E_1^*) \bmod p$ so we just Hensel lift it to a root of

$$\Phi_5(X, j(E^*)) \in \mathbb{Z}_p[X].$$

# Newton iteration

We know that $j(E^*)^{(\alpha)} = 46 - 22 \cdot 607$. To apply Newton iteration we also need the derivative at the CM-points:

**Lemma.** Write
$$[\alpha](j - j(\tilde{E})) = \sum_{i \geq 1} c_i (j - j(\tilde{E}))^i,$$
then $c_1 = I/\bar{I}$.

We now 'update' $j(E^*)^{(\alpha)}$ according to Newton's formula:
$$j(E_{k+1}) = j(E_k) - \frac{j(\rho_\alpha(E_k)) - j(E_k)}{(\alpha/\bar{\alpha}) - 1} \quad k \in \mathbb{Z}_{\geq 1}.$$

We find that $j(\tilde{E}) \bmod p^2 = 46 - 199 \cdot 607$.

## The $j$-invariant of the canonical lift

The constant term (usually the biggest in size) of $H_{\mathcal{O}_D}$ is relatively close to $10^k$ with

$$k = \frac{\pi\sqrt{|D|}}{\ln(10)} \sum_{[a,b,c]\in \mathrm{Cl}(D)} \frac{1}{a}.$$

So we need to know $j(\tilde{E})$ upto 188 decimals, i.e. 68 $p$-adic digits.

$$\begin{aligned}
j(\tilde{E}) =& 46 + O(p)\\
=& 46 - 199p + O(p^2)\\
=& 46 - 199p + 77p^2 + 104p^3 + O(p^4)\\
=& 46 - 199p + 77p^2 + 104p^3 - 228p^4\\
& -144p^5 - 82p^6 + 21p^7 + O(p^8)\\
=& 46 - 199p + 77p^2 + 104p^3 - 228p^4\\
& -144p^5 - 82p^6 + 21p^7 - 51p^8\\
& +215p^9 - 71p^{10} - 238p^{11} + 171p^{12}\\
& +237p^{13} + 53p^{14} - 219p^{15} + O(p^{16}).
\end{aligned}$$

# Finally, $H_{\mathcal{O}}$

Remains to compute conjugates of $j(\tilde{E})$ under $\mathrm{Cl}(D)$.

We can use modular polynomials once more.

Bach bound: $\mathrm{Cl}(D)$ is generated by primes of norm less than $6\log^2(|D|)$.
In our case: $\mathrm{Cl}(D) = \langle L_3, L_5 \rangle$.

We get the class polynomial of degree 12, whose constant term is:

18031573419817116858674171012408922759775929838844297957252172833044967272386907152455393320194706354169351394942608003785949965858286598001906443231847457556807519764679614103825149853696.

# Obtaining the desired curve

- reduce $H_{\mathcal{O}}$ mod $q$ and compute a root $j$;
- put $k = 27j/(4(j-1728))$, then
  $$E_j : y^2 = x^3 - kx - k$$
  has $j$-invariant $j$;
- we only know that $\mathrm{Tr}(F_q) = \pm t$, so we test if
  $$(q+1+t)P \neq O_E = (q+1-t)P$$
  for a random point $P \in E_j(\mathbb{F}_q)$.
- if this holds, we are done; otherwise we test again with a random point of the *quadratic twist* of $E_j$.

The elliptic curve defined by

$$y^2 = x^3 + 796497089509840x + 964399977303209$$

over $\mathbb{F}_{1425091291226311}$ has exactly

$$1425091215750802$$

points.

## Solution to second problem?

The class polynomial is huge…

- don't use $j$, but smaller functions. Examples: $\gamma_2$, a cube root of $j$, or the classical Weber $\mathfrak{f}$, a root of

$$(X^{24} - 16)^3 - X^{24} j;$$

- approach goes back to Weber and is now well understood (Shimura's reciprocity law) *over the complex numbers*;

- need to adapt things for $\mathbb{C}_p$.