Algebraic construction of the Elkies factor

Christiane Peters

Technische Universiteit Eindhoven

Workshop on Counting Points
CRM Montréal

April 19, 2010

Notation

Given an elliptic curve E over $\mathbf{F}_q$ for q odd.

- Frobenius endomorphism:

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

- Characteristic polynomial of π

$$\pi^2 - t\pi + q = 0.$$

- Call t the trace of the Frobenius.

- $\#E(\mathbf{F}_q) = q + 1 - t$ and t satisfies $|t| \leq 2\sqrt{q}$.

Compute t mod ℓ

Consider a prime ℓ.

- ℓ-torsion $E[\ell] = \{P \in E : [\ell]P = P_\infty\}$
- The restriction π' of the Frobenius endomorphism to $E[\ell]$ satisfies

$$\pi'^2 - t_\ell \, \pi' + q_\ell = 0 \qquad \text{in } \mathbf{F}_\ell$$

  where $t_\ell = t \mod \ell$ and $q_\ell = q \mod \ell$ are uniquely determined.

Schoof (1984): determine t_ℓ for $\mathcal{O}(\log(q))$ primes ℓ such that $\prod \ell > 4\sqrt{q}$. Then the CRT yields

$$t \mod \prod \ell \in [-2\sqrt{q}, 2\sqrt{q}].$$

Division polynomials

Let K be a field of characteristic $\neq 2, 3$.

Let $m \geq 1$. The mth division polynomial $\psi_m \in \mathbf{Z}[A, B, X, Y]$ vanishes in all m-torsion points, i.e., for $P = (x, y)$ in $E(\bar{K})$, $P \notin E[2]$,

$$[m]P = P_\infty \Leftrightarrow \psi_m(x, y) = 0.$$

Theorem

For $m \geq 3$

$$[m](x, y) = \left(x - \frac{\psi_{m-1}\,\psi_{m+1}}{\psi_m^2},\ \frac{\psi_{m+2}\,\psi_{m-1}^2 - \psi_{m-2}\,\psi_{m+1}^2}{4y\,\psi_m^3} \right).$$

Recursion

Given $E : Y^2 = X^3 + AX + B$ over K.

$$\psi_1 = 1,$$
$$\psi_2 = 2Y,$$
$$\psi_3 = 3X^4 + 6AX^2 + 12BX - A^2,$$
$$\psi_4 = 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3)$$

and

$$\begin{array}{rcll} \psi_{2m+1} & = & \psi_{m+2}\psi_m^3 - \psi_{m+1}^3\psi_{m-1} & \text{if } m \geq 2, \\ 2Y\psi_{2m} & = & \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\,\psi_{m+1}^2) & \text{if } m \geq 3. \end{array}$$

- For odd m we have $\psi_m(X,Y) = f_m(X) \in \mathbf{Z}[A,B,X]$ with $\deg f_m = (m^2-1)/2$.
- For even m we have $\psi_m(X,Y) = Y f_m(X)$ with $f_m(X) \in \mathbf{Z}[A,B,X]$ and $\deg f_m = (m^2-4)/2$.

Elkies primes

- Torsion structure: $E[\ell] \cong \mathbf{F}_\ell^2$ for ℓ prime.
- π' acts as a linear operator on $E[\ell]$.
- Call ℓ an Elkies prime if

  $$T^2 - t_\ell T + q_\ell = (T - \lambda)(T - \mu)$$

  with λ, μ in $\mathbf{F}_\ell$.
- In this case the eigenvalues λ and μ of π are defined over $\mathbf{F}_\ell$.
- We get $q_\ell = \lambda \cdot \mu$ and thus

  $$t_\ell = \lambda + \mu = \lambda + q_\ell/\lambda.$$

- Restrict search of $t \mod \ell$ to a subgroup of $E[\ell]$.

Atkin and SEA

If $T^2 - t_\ell T + q_\ell$ does not split over $\mathbf{F}_\ell$ the prime ℓ is called an Atkin prime.

- Determine the rth power of the Frobenius such that there is a π^r-invariant subgroup of $E[\ell]$.
- Then $t \mod \ell$ satisfies

$$t^2 \equiv (\zeta_r + 2 + \zeta_r^{-1})q$$

  for an rth root of unity ζ_r.
- Cannot uniquely determine t_ℓ.

SEA (Schoof-Elkies-Atkin algorithm)

- Use both Elkies's and Atkin's method to determine t_ℓ for primes ℓ until $\prod \ell > 4\sqrt{q}$.

Determine t_ℓ in the Elkies case

- Let P in $E[\ell]$ be an eigenpoint corresponding to an eigenvalue λ, i.e., $\pi(P) = [\lambda]P$.

- The point P generates a π-invariant subgroup $\mathcal{C}$ of order ℓ of $E[\ell]$.

- Since $t_\ell = \lambda + q_\ell/\lambda$ determining t_ℓ in $\mathcal{C}$ means finding an eigenvalue of the Frobenius in $\mathbf{F}_\ell$.

- New 'check equation'. Find $\lambda \in \{1, \ldots, \ell - 1\}$ such that

$$\pi(P) = [\lambda]P$$

for a non-trivial point of a subgroup of $E[\ell]$.

Elkies factor

Let $\mathcal{C}$ be a π-invariant subgroup of $E[\ell]$.

- Determine a factor $f_{\ell,\lambda}(X)$ of $f_\ell(X)$ in $\mathbf{F}_q[X]$ such that

$$(x,y) \in \mathcal{C} \Leftrightarrow f_{\ell,\lambda}(x) = 0.$$

- We get

$$f_{\ell,\lambda}(X) = \prod_{\substack{\pm P \in \mathcal{C} \\ P \neq P_\infty}} (X - x(P)).$$

- Degree: $\deg f_{\ell,\lambda} = (\ell - 1)/2$.

Usual approach with modular forms

- Determine if there is a degree-ℓ isogeny whose kernel is a subgroup $\mathcal{C}$ of $E[\ell]$ by looking at the splitting behaviour of the ℓth modular polynomial $\Phi_\ell(X, j)$ over $\mathbf{F}_q$.

- Compute such an ℓ-isogeny.

- Use Vélu's formulas to compute such an isogenous curve $E' \cong E/\mathcal{C}$.

- Cost for determining $f_{\ell,\lambda}$ is $\mathcal{O}(\ell^{2+o(1)})$.

Cyclic subgroups of $E[\ell]$

- Let P_1 and P_2 generate the ℓ-torsion group $E[\ell]$.
- The $\ell + 1$ cyclic subgroups $\mathcal{C}$ of $E[\ell]$ are given by

$$\mathcal{C}_1 = \langle P_1 \rangle \text{ and } \mathcal{C}_2 = \langle P_2 \rangle$$

and for $k = 3, \ldots, \ell + 1$

$$\mathcal{C}_k = \langle P_1 + [k-2]P_2 \rangle.$$

- The subgroups are pairwise disjoint except for the point P_∞.
- We have

$$E[\ell] = \bigcup_{k=1}^{\ell+1} \mathcal{C}_k.$$

An alternative polynomial

- Consider the polynomial

$$\tilde{U}_\ell = \prod_{P \in E[\ell] \setminus \{P_\infty\}} \left(T - \sum_{1 \le i \le (\ell-1)/2} x([i]P) \right) \text{ in } \overline{\mathbf{F}}_q[T].$$

- If P and Q lie in the same subgroup

$$\sum_{1 \le i \le (\ell-1)/2} x([i]P) = \sum_{1 \le i \le (\ell-1)/2} x([i]Q).$$

- Thus $\tilde{U}_\ell = U_\ell^{\ell-1}$ for a polynomial U_ℓ in $\overline{\mathbf{F}}_q[T]$ of degree $\ell + 1$.

Criterion for finding Elkies primes

Theorem

There is a π-invariant subgroup $\mathcal{C}$ of $E[\ell]$, i.e., the prime ℓ is an Elkies prime if and only if the polynomial U_ℓ has a zero in $\mathbf{F}_q$ of multiplicity 1.

1. Notation and basic Schoof
2. Improvements by Elkies
3. Charlap, Coley, and Robbins's modular equation
4. Algebraic computation of an Elkies factor

Revisiting the multiplication map

Consider an odd prime ℓ which is coprime to q.

- Let $[m](x, y) = (g_m(x, y), h_m(x, y))$. Since g_m is a polynomial in x write $g_m(x)$.
- Note that $g_m(x) = g_{-m}(x)$ for any point (x, y) in E.
- Let

$$p_1(x) = \sum_{1 \leq i \leq \frac{\ell-1}{2}} g_i(x) \mod \psi_\ell.$$

Computing U_ℓ

Lemma (Charlap, Coley, and Robbins (1991))

$$U_\ell^{\frac{\ell-1}{2}} = c^{-1} \cdot \mathrm{Res}_x\left(T - p_1(x), \psi_\ell(x)\right).$$

where $c \in \mathbf{F}_q$.

Proof.

$$\mathrm{Res}_x\left(T - p_1(x), \psi_\ell(x)\right) = c \cdot \prod_{\substack{\pm(x,y)\in E \\ \psi_\ell(x)=0}} \left(T - p_1(x)\right)$$

$$= c \cdot \prod_{j=1}^{\ell+1} \prod_{\substack{\pm(x,y)\in \\ \mathcal{C}_j\setminus\{P_\infty\}}} \left(T - p_1(x)\right) = c \cdot \prod_{j=1}^{\ell+1} \left(T - p_1(x(P_j))\right)^{(\ell-1)/2},$$

where $\mathcal{C}_j = \langle P_j \rangle$ are the $\ell + 1$ subgroups of order ℓ of $E[\ell]$. □

Properties of zeros of U_ℓ

- Let ℓ be an Elkies prime, and $\langle P \rangle$ a π-invariant subgroup of $E[\ell]$.
- So U_ℓ has a zero r in $\mathbf{F}_q$ which corresponds to the sum of points in $\langle P \rangle$.
- Consider

$$h(X) = \sum_{j=1}^{(\ell-1)/2} g_j(X) \mod \psi_\ell.$$

- Let $f_{\ell,\lambda}(X) = \prod_{1 \le i \le (\ell-1)/2}(X - x([i]P))$.
- Then

$$r \equiv h(X) \mod f_{\ell,\lambda}(X) \qquad \text{in } \mathbf{F}_q[X].$$

The Elkies-factor

- It follows that $f_{\ell,\lambda}(X)$ divides $h(X) - r$ in $\mathbf{F}_q[X]$.
- Moreover $f_{\ell,\lambda}$ divides ψ_ℓ.

Theorem

Let $f_{\ell,\lambda}$ be an Elkies factor and $r \in \mathbf{F}_q$ a zero of U_ℓ. Then

$$f_{\ell,\lambda}(X) = \gcd\big(h(X) - r, \psi_\ell(X)\big).$$

- Hence the Elkies-factor $f_{\ell,\lambda}$ can be computed by purely algebraic means: resultant and GCD computation.

Complexity

- Resultant computation for $U_\ell^{(\ell-1)/2}$: $\mathcal{O}(\ell^2 M(\ell^2)\log(\ell^2))$.
- Cut down to $\mathcal{O}(\ell M(\ell^2)\log(\ell^2))$ for U_ℓ exploiting the fact that we know the resultant yields a $(\ell-1)/2$th power.
- Can we do better?

C. Peters,
Bestimmung des Elkies-Faktors im
Schoof-Elkies-Atkin-Algorithmus (in German)
Diploma thesis, Universität Paderborn, 2006
Supervision: Peter Bürgisser and Preda Mihăilescu

Contact: c.p.peters@tue.nl

Thank you very much for your attention!