Catrel Workshop, École Polytechnique — October 1-2, 2015

How to get rid of units?

Razvan Barbulescu

Motivation

Context

Ccomputing discrete logs in $\mathbb{F}_{p^n}$ with $n > 1$ and small.

One wants to "turn off the Schirokauer maps"

1. when using Galois action in linear algebra (preprint theorem is correct for polys without Schirokauer maps (SMs));
2. when implementing linear algebra on GPU (currect CADO for GPU is slower in presence of SMs);
3. when adapting the code to MNFS.

Zoom on Galois action

Joux Lercier Smart Vercauteren proposed to reduce the matrix using equations of type:

$$\log \sigma(\mathfrak{q}) = p^{\kappa} \log \mathfrak{q}.$$

One can prove the equation for elements

$$\forall x \in K, \log \sigma(x) = p^{\kappa} \log x.$$

The result on ideals is true only if the logs of units are zero.

Pohlig-Hellman simplification

Logarithms modulo ℓ

1. In order to compute discrete logs in $\mathbb{F}_{p^n}$ it is enough to implement an algorithm which computes discrete logs modulo any prime factor of $p^n - 1$.
2. In pairing-based cryptography, the computations are done in a subgroup of prime order ℓ.

Logs in subfields when ℓ divides $\Phi_n(p)$

Let g be a generator of $(\mathbb{F}_{p^n})^*$ and $y \in (\mathbb{F}_{p^d})^*$ for some divisor d of n.

$$y^{p^d-1} = 1 \Rightarrow y^{\frac{p^n-1}{\Phi_n(p)}} = 1 \Rightarrow y^{\frac{p^n-1}{\ell}} = 1 \Leftrightarrow \log_g y \equiv 0 \pmod{\ell}.$$

Logarithms of subfield elements (1/2)

Lemma

If σ is an automorphism of the number field of $f \in \mathbb{Z}[x]$ such that

- $\sigma\mathfrak{p} = \mathfrak{p}$;
- $\mathrm{Disc}(f) \not\equiv 0 \mod p$.

Then the map

$$\begin{array}{rccc} \overline{\sigma}: & k_{\mathfrak{p}} & \to & k_{\mathfrak{p}} \\ & x \bmod \mathfrak{p} & \mapsto & \sigma(x) \bmod \mathfrak{p}. \end{array}$$

belongs to $\mathrm{Gal}(k_{\mathfrak{p}})$ *and* $\mathrm{ord}(\overline{\sigma}) = \mathrm{ord}(\sigma)$.

Logarithms of subfield elements (1/2)

$$
\begin{array}{ccc}
K & \longrightarrow & \mathbb{F}_{p^k} \\
| & & | \\
K^{\langle\sigma\rangle} & \longrightarrow & \mathbb{F}_{p^{k/\operatorname{ord}(\sigma)}} \\
| & & | \\
\mathbb{Q} & \longrightarrow & \mathbb{F}_p
\end{array}
$$

Logarithms of subfield elements (1/2)

$$
\begin{array}{ccc}
K & \longrightarrow & \mathbb{F}_{p^k} \\
| & & | \\
K^{\langle\sigma\rangle} & \longrightarrow & \mathbb{F}_{p^{k/\operatorname{ord}(\sigma)}} \\
| & & | \\
\mathbb{Q} & \longrightarrow & \mathbb{F}_p
\end{array}
$$

$$\boxed{x \in K^{\langle\sigma\rangle} \Rightarrow \log(x) \equiv 0 \pmod{\ell}.}$$

Degree 4 family without units

Idea

We choose f so that $\mathrm{ord}(\sigma) = 2$ and all the units of its number field K are in $K^{\langle\sigma\rangle}$.

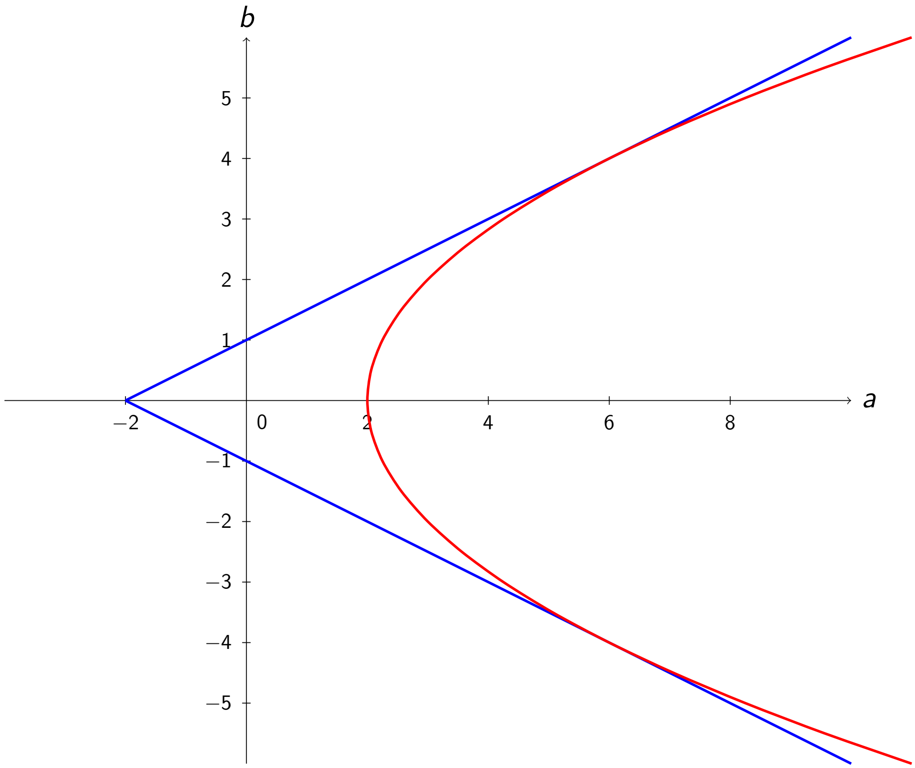
1. signature of K: $(0, r)$;
2. signature of $K^{\langle\sigma\rangle}$: $(r, 0)$;

Proposition

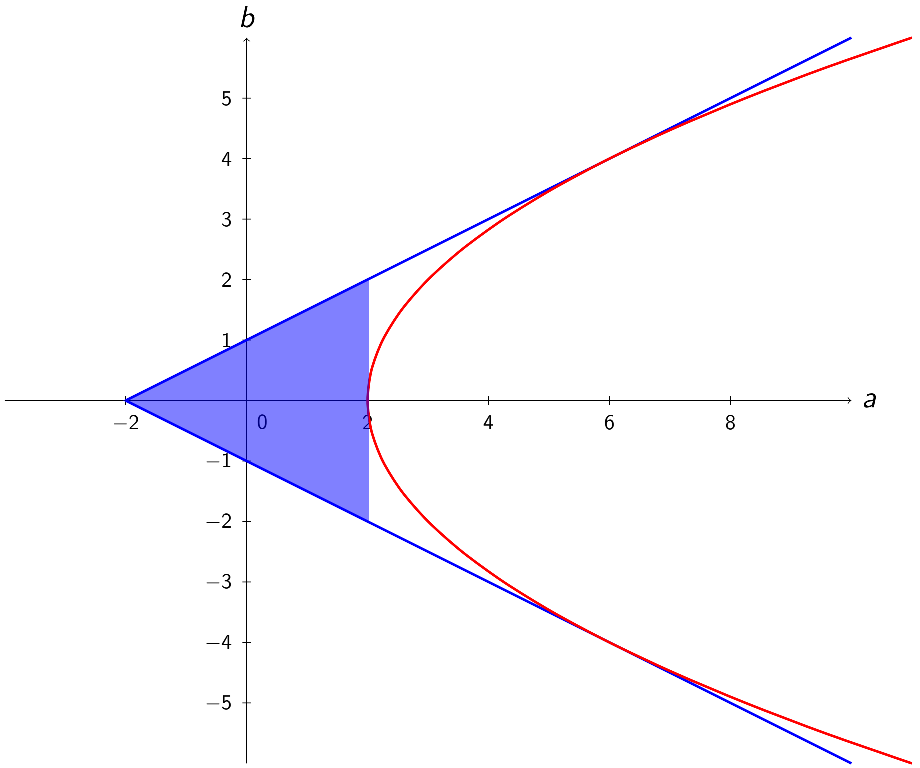
Polynomials $f = x^4 + bx^3 + ax^2 + bx + 1$ are as above if and only if

1. $b^2 - 4(a-2) > 0$;
2. and $|b| < 1 + a/2$.

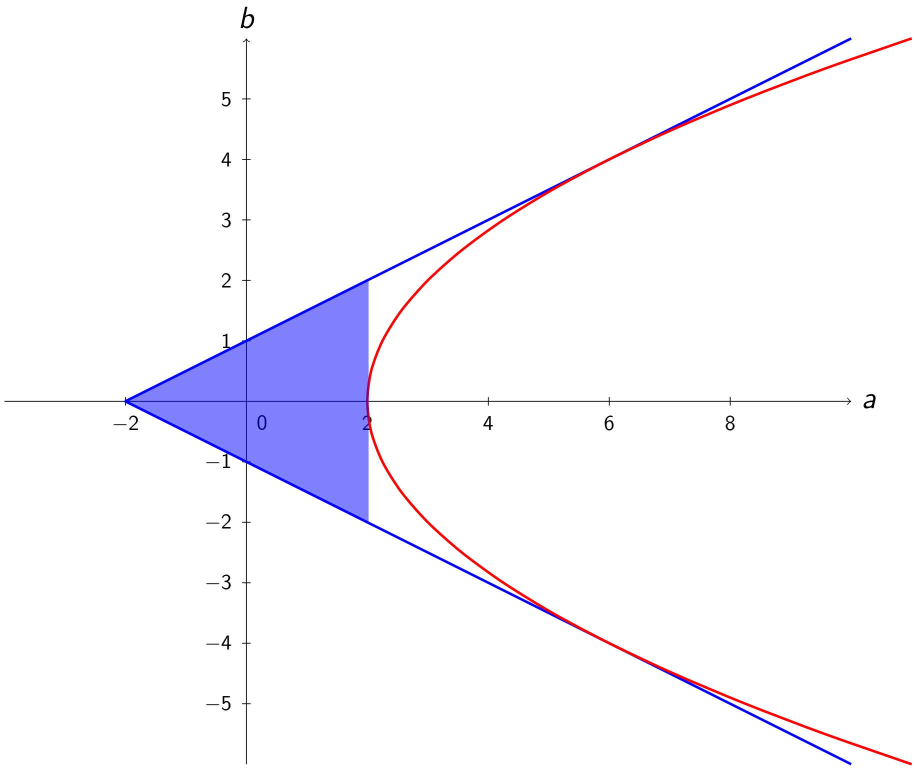
Convex subfamily



Convex subfamily



Convex subfamily



Corollary

When $|a| < 2$ *and* $|b| < a/2 + 1$ *we can combine polys for MNFS.*

Constructing pairs of polynomials without units

Algorithm

$\kappa \leftarrow 100$;

repeat

  $a \leftarrow$ Random($\sqrt{p}$, p);

  $\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \leftarrow \mathrm{LLL} \begin{pmatrix} p & 0 \\ a & 1 \end{pmatrix}$;

until $|u_1/v_1| < \frac{2\kappa}{2+\kappa}$ and $|u_2/v_2| < \frac{2\kappa}{2+\kappa}$.

$a_1 \leftarrow u_1/v_1$;

$a_2 \leftarrow u_2/v_2$;

$b_1 \leftarrow a_1/\kappa$;

$b_2 \leftarrow a_2/\kappa$;

return $x^4 + b_1x^3 + a_1x^2 + b_1x + 1$ and $x^4 + b_2x^3 + a_2x^2 + b_2x + 1$.

Experimental law

The termination condition occurs for $\approx 40\%$ of values for a.

Degree six family of polynomials without units

Theorem

For all positive rationals a, b, c, d the polynomial

$$P(x) = (a + 3b + 3c + d)\,(x^2 + 4)^3 + (-3a - 6b - 3c)\,(x^2 + 4)^2 + (2a - 3b - 6c - d)\,(x^2 + 4) - 6b$$

has signature $(0, 3)$, is even and the subfield fixed by $x \mapsto -x$ has three real roots.

Proof.

$P(x) = Q(x^2 + 4)$ where Q has three real roots less than 4. □

Degree six family of polynomials without units

Theorem

For all positive rationals a, b, c, d the polynomial

$$P(x) = (a+3b+3c+d)\,(x^2+4)^3 + (-3a-6b-3c)\,(x^2+4)^2 + (2a-3b-6c-d)\,(x^2+4) - 6b$$

has signature $(0,3)$, is even and the subfield fixed by $x \mapsto -x$ has three real roots.

Proof.

$P(x) = Q(x^2+4)$ where Q has three real roots less than 4. □

Are there other families without units?

Characterization of polynomials "without units"

Lemma

Let f be fixed polynomial with automorphism σ. For large enough prime ℓ we have

$$\forall \varepsilon \text{ unit}, \sigma(\varepsilon)/\varepsilon \in E^{\ell} \Rightarrow \sigma(\varepsilon) = \varepsilon.$$

Theorem

Let $n \leq 7$ be an integer, $f \in \mathbb{Z}[x]$ irreducible of degree n. Let p be a prime and ℓ a factor of $\Phi_n(p)$. If $\log \rho(\varepsilon) \equiv 0 \pmod{\ell}$ for all unit ε, and ℓ is large enough, then $n = 4$ or 6 and the number field of f is CM or biquadratic real.

Characterization of polynomials "without units"

Lemma

Let f be fixed polynomial with automorphism σ. For large enough prime ℓ we have

$$\forall \varepsilon \text{ unit}, \sigma(\varepsilon)/\varepsilon \in E^{\ell} \Rightarrow \sigma(\varepsilon) = \varepsilon.$$

Theorem

Let $n \leq 7$ be an integer, $f \in \mathbb{Z}[x]$ irreducible of degree n. Let p be a prime and ℓ a factor of $\Phi_n(p)$. If $\log \rho(\varepsilon) \equiv 0 \pmod{\ell}$ for all unit ε, and ℓ is large enough, then $n = 4$ or 6 and the number field of f is CM or biquadratic real.

Proof.

- when n is prime, there are no proper subfield;
- when $n = 4$ and there are subfields f is Galois, and then CM or biquadratic;
- when $n = 6$ and there are subfields then $\#\mathrm{Gal}(f) = 6$ or 12, and then CM.

□

Unit group as $\mathbb{F}_\ell$-vector space

Let E be the unit group of f.

Vector space structure

Let $\varepsilon_1, \ldots, \varepsilon_r$ be a basis of E/E^ℓ.

$$(u_1, \ldots, u_r) \in \mathbb{F}_\ell^r \leftrightarrow \prod_{i=1}^{r} \varepsilon_i^{u_i} \in E/E^\ell.$$

Eigenspaces

For any eigenvalue $c \in \mathbb{F}_\ell$ of σ, we denote by E_c the eigenspace of c:

$$E_c = \left\{\epsilon \in E \mid \exists \eta \in E, \sigma(\epsilon) = \epsilon^c \eta^\ell \right\}.$$

Exemple of partial vanishing

- $f = x^6 + 2x^5 - 10x^4 - 20x^3 - 5x^2 + 4x + 1$;
- $A = u$ root of Φ_3 modulo $\ell = 360187$.
- η_i units depending on ℓ (not on p);
- ℓ fixed and $p \equiv 1039 \pmod{\ell}$.

		E_1	E_u		E_{u^2}	
p	A	$\log(\rho_p(\eta_1))$	$\log(\rho_p(\eta_2))$	$\log(\rho_p(\eta_3))$	$\log(\rho_p(\eta_4))$	$\log(\rho_p(\eta_5))$
1039	u	0	$\star$	$\star$	0	0
30256747	u	0	$\star$	$\star$	0	0
46825349	u	0	$\star$	$\star$	0	0
54029089	u^2	0	0	0	$\star$	$\star$
70597691	u	0	$\star$	$\star$	0	0
73479187	u^2	0	0	0	$\star$	$\star$

Eigenspaces

Lemma

If $A \in \mathbb{F}_\ell$ *is such that* $\log \rho(\sigma(x)) = A \log \rho(x) \pmod{\ell}$, *then*

$$\forall c \neq A, \forall \varepsilon \in E_c, \log \rho(\varepsilon) \equiv 0 \mod \ell.$$

Eigenspaces

Lemma

If $A \in \mathbb{F}_\ell$ *is such that* $\log \rho(\sigma(x)) = A \log \rho(x) \pmod{\ell}$*, then*

$$\forall c \neq A, \forall \varepsilon \in E_c, \log \rho(\varepsilon) \equiv 0 \mod \ell.$$

Theorem

For large enough ℓ*, the dimesion of* E_u *is the same for all* $u \in \mathbb{F}_\ell$ *of the maximal order.*

Proof.

- σ cancels a poly with simple roots so it is diagonal in a basis of $\mathbb{Q}(\zeta)^r$;
- for large enough ℓ, the basis projects into a basis of $\mathbb{F}_\ell^r$, so $\dim E_\gamma = \dim E_{\overline{\gamma}}$;
- $\dim E_\gamma = \dim E_\gamma^i$ when $\gcd(i, n) = 1$ because automorphisms of $\mathbb{Q}(\zeta)$ are semi-linear maps.

□

Results on partial vanishing

Odd prime degree

- totally real;
- dim $E_1 = 0$ because no subfields;
- dim $E_u = 1$ for all u because same dimension.

Degree 4 and 6

Depending on the signatures of K and $K^{\langle\sigma\rangle}$ there are 16 cases.

Degree 4 and 6 (table)

	$\deg(K)$	$\mathrm{ord}(\sigma)$	$\mathrm{rk}(K)$	$\mathrm{rk}(K^{\langle\sigma\rangle})$	$\dim E_u$	example
i	4	2	3	1	2	x^4-5x^2+2
ii			2	1	1	x^4-5x^2-2
iii			1	0	1	x^4-x^2+2
iv			1	1	0	x^4+5x^2+2
v		4	3	0	1	$x^4+x^3-6x^2-x+1$
vi			1	0	0	$x^4+x^3+x^2+x+1$
vii	6	2	5	2	3	$x^6-6x^4+9x^2-3$
viii			4	2	2	x^6-3x^2+1
ix			3	1	2	x^6+3x^2-1
x			3	2	1	x^6-3x^2-1
xi			2	1	1	x^6+3x^2+1
xii			2	2	0	$x^6+6x^4+8x^2+1$
xiii		3	5	1	2	$x^6-8x^4+6x^3+7x^2-6x+1$
xiv			2	0	2	$x^6-5x^4+10x^2-6x+1$
xv		6	5	0	1	$x^6+2x^5-10x^4-20x^3-5x^2+4x+1$
xvi			2	0	0	$x^6+x^5+x^4+x^3+x^2+x+1$