Alternative Models: Infrastructure

Michael J. Jacobson, Jr.

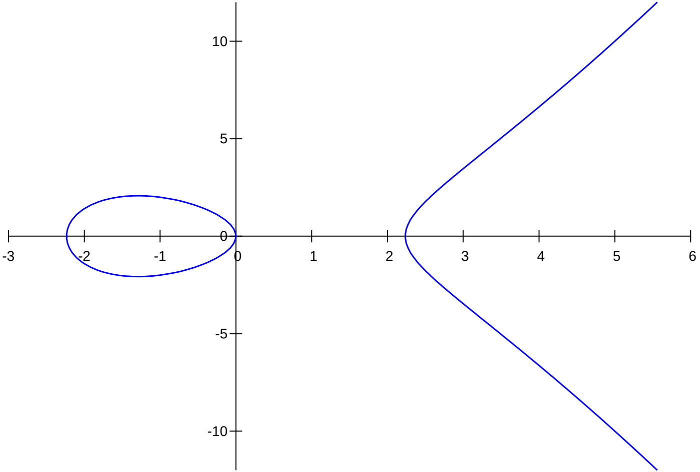
jacobs@cpsc.ucalgary.ca

UNIVERSITY OF CALGARY

UNCG Summer School in Computational Number Theory 2016: Function Fields

Elliptic Curves in Weierstrass Model

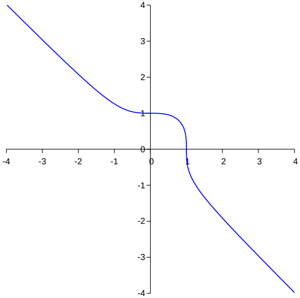
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$



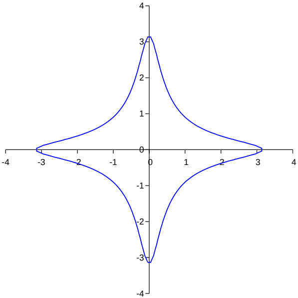
Some Other Elliptic Curve Models

Other elliptic curve models with faster arithmetic:

- **Hessians**: $x^3 + y^3 - 3dxy = 1$
- **Edwards models**: $x^2 + y^2 = c^2(1 + dx^2y^2)$ (q odd) and variations



$$x^3 + y^3 = 1$$



$$x^2 + y^2 = 10(1 - x^2y^2)$$

Split Representations of Hyperelliptic Function Fields

Two infinite places ∞_+ and ∞_-, both of degree 1.

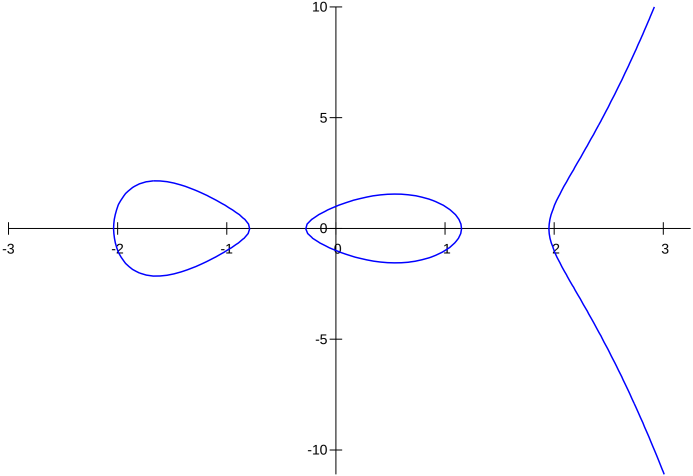
Divisor class epresentation: $\displaystyle\sum_{i=1}^{r} P_i - r\infty_- + n(\infty_+ - \infty_-), \;\; r \le g$

- No restrictions on n: many reduced divisors in each class ($\approx q^g$)
- $n = 0$: infrastructures (misses a few divisor classes)
- $n \approx g$: unique representatives, multiply/reduce plus *adjustment steps* (Paulus/Rück 1999)
- $n \approx \lceil g/2 \rceil$: balanced representation, unique and generally **no adjustment steps** (Galbraith/Harrison/Mireles Morales 2008)

Computations (discrete logarithms, invariants) are polynomially equivalent.

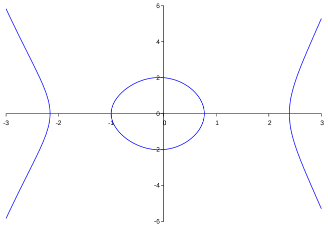
Example: Odd Degree (Ramified) Hyperelliptic Curve

$H : y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$, genus $g = 2$



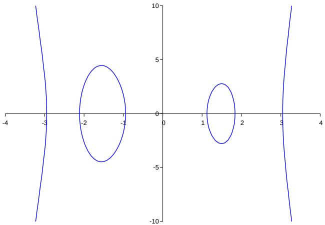
Example: Even Degree (Split) Models

$y^2 + h(x)y = f(x)$, $\deg(f) = 2g+2$, $\deg(h) = g+1$ if $\operatorname{char}(K) = 2$.



$$y^2 = x^4 - 6x^2 + x + 6$$

$$(g = 1)$$



$$y^2 = x^6 - 13x^4 + 44x^2 - 4x - 1$$

$$(g = 2)$$

Why Consider Split Representations?

Main advantage: more general than ramified representations

- split representation always exists, whereas a ramified or inert one may only exist over a larger base field
- Can always transform a ramified to split model over K, but the reverse direction may require an extension of K.
- Some constructions (eg. pairing-friendly curves in cryptography) frequently generate split models which are traditionally just discarded.

Disadvantages:

- Split representations are more complicated than ramified ones.
- Research into efficient arithmetic on real models is far less advanced (i.e. slower, but catching up!)

Almost-Reduction

Let $\mathfrak{a} = [u, v + y]$ be a primitive non-reduced ideal. Set

$$v' \equiv -v \bmod u \ , \quad u' = \frac{f - (v')^2}{u} \ .$$

Properties:

- $\mathfrak{a}' = [u', v' + y]$ is a primitive ideal.
- $\mathfrak{a}' = (z)\mathfrak{a}$ with $z = (v' + y)/u \in F^*$, so $\mathfrak{a}'$ is equivalent to $\mathfrak{a}$.
- $\deg(u') \leq \deg(u) - 2$.
- $\lfloor (\deg(u) - g)/2 \rfloor$ applications of the operation $\mathfrak{a} \to \mathfrak{a}'$ produces a reduced or almost reduced ideal equivalent to $\mathfrak{a}$.

  In particular, if $\mathfrak{a}$ was obtained as the primitive product of two reduced ideals, then this number is $\lfloor g/2 \rfloor$.

Reduction

Suppose $K = \mathbb{F}_q$ is a finite field and $\mathfrak{a} = [u, v + y]$ is almost reduced.

- If P_∞ is ramified in F, then one more iteration $\mathfrak{a} \to \mathfrak{a}'$ produces the unique reduced ideal equivalent to $\mathfrak{a}$.
- If P_∞ is inert in F, then Artin provided a simple iterative procedure for finding the other q almost reduced ideals equivalent to $\mathfrak{a}$.
- If P_∞ splits in F, then "perturbing" the reduction operation on v from

$$v' = \left\lfloor \frac{v}{u} \right\rfloor u - v$$

to

$$v' = \left\lfloor \frac{v + \lfloor y \rfloor}{u} \right\rfloor u - v$$

yields the entire infrastructure of $\mathfrak{a}$. (Note that $y \in \mathbb{F}_q((x^{-1}))$.)

Infrastructures as Ordered Sets

Suppose P_∞ splits in F and let $\mathfrak{a}_1$ be a fixed reduced $\mathbb{F}_q[x, y]$-ideal.

The perturbed reduction operation repeatedly applied to $\mathfrak{a}_1$ cyclically generates the entire infrastructure $\{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \ldots \mathfrak{a}_p\}$:

$$\mathfrak{a}_i = [u_i, v_i + y] \quad \text{and} \quad \mathfrak{a}_{i+1} = (z_i)\mathfrak{a}_i \quad \text{with} \quad z_i = \frac{v_{i+1} + y}{u_i}.$$

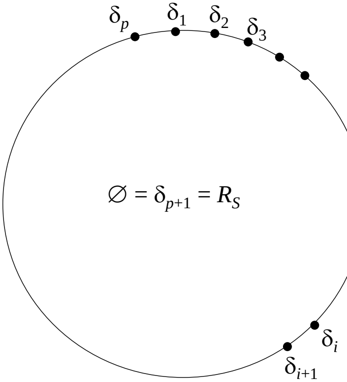
Fix a place P'_∞ of F lying above P_∞ and define the relative distances

$$\delta(\mathfrak{a}_{i+1}, \mathfrak{a}_i) = -v_{P'_\infty}(z_i) = g + 1 - \deg(a_i) \geq 1 \ .$$

$$\delta_{i+1} = \delta(\mathfrak{a}_{i+1}, \mathfrak{a}_1) = \sum_{j=1}^{i} \delta(\mathfrak{a}_{j+1}, \mathfrak{a}_j) = i(g+1) - \sum_{j=1}^{i} \deg(a_i) \ .$$

This imposes an order on the infrastructure according to distance from $\mathfrak{a}_1$.

Properties of Infrastructures



Properties:

- $\delta(\mathfrak{a}_{i+1}, \mathfrak{a}_i) \geq 1$;
- $\delta(\mathfrak{a}_{i+1}, \mathfrak{a}_i) \leq g$ unless $\mathfrak{a}_i = K[x, y]$, in which case $\delta(\mathfrak{a}_{i+1}, \mathfrak{a}_i) = g + 1$;
- $\delta_{p+1} = R_F$, the regulator of $\mathcal{O}_F$ (degree of fundamental unit);
- $\deg(a_i) = g$ almost always and hence $\delta(\mathfrak{a}_{i+1}, \mathfrak{a}_1) \approx i$.

Infrastructures as Structured Sets

Let $\mathfrak{a}$, $\mathfrak{b}$ be reduced ideals with $\mathfrak{b}$ principal, and let $\mathfrak{a} * \mathfrak{b}$ denote the first reduced ideal obtained by applying reduction to the primitive part of $\mathfrak{a}\mathfrak{b}$.

Note that $\mathfrak{a} * \mathfrak{b}$ is equivalent to $\mathfrak{a}$.

Theorem

$0 \leq \delta(\mathfrak{a} * \mathfrak{b}, \mathfrak{a}) - \delta(\mathfrak{b}, O_F) \leq 2g.$

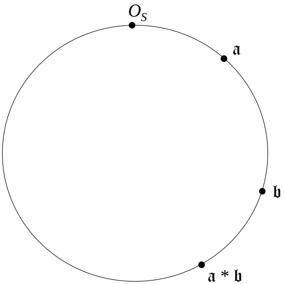
For any reduced principal ideal $\mathfrak{r}$, write $\delta(\mathfrak{r}) = \delta(\mathfrak{r}, O_F)$ for brevity.

Special case: $\mathfrak{a}$ is also principal. Then $\delta(\mathfrak{a} * \mathfrak{b}, \mathfrak{a}) = \delta(\mathfrak{a} * \mathfrak{b}) - \delta(\mathfrak{a})$, so:

Corollary ($\mathfrak{a}$, $\mathfrak{b}$ principal)

$\delta(\mathfrak{a} * \mathfrak{b}) = \delta(\mathfrak{a}) + \delta(\mathfrak{b}) - d \quad \textit{with} \quad 0 \leq d \leq 2g.$

Principal Infrastructure



Distances are “almost” additive on the principal infrastructure.

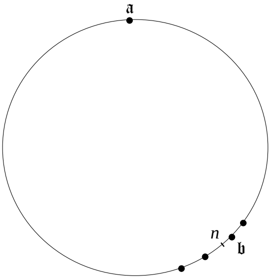
So the principal infrastructure is “almost” an abelian group under “$*$”:

- identity is O_F;
- inverse of $[u, v + y]$ is $[u, -v + y]$;
- associativity “almost” holds.

Principal Infrastructure as a Near-Group

Definition

Let $\mathfrak{a}$ be a reduced ideal and $n \in [0, R_S)$. Then the ideal closest to n with respect to $\mathfrak{a}$ is the unique reduced ideal $\mathfrak{b} \in [\mathfrak{a}]$ with $|\delta(\mathfrak{b}, \mathfrak{a}) - n|$ minimal.



For a pair $\mathfrak{a}, \mathfrak{b}$ of reduced principal ideals, define the ideal $\mathfrak{a} \otimes \mathfrak{b}$ to be the reduced principal ideal closest to $\delta(\mathfrak{a}) + \delta(\mathfrak{b})$ with respect to O_F.

- $\mathfrak{a} \otimes \mathfrak{b}$ can computed efficiently by $\mathfrak{a} * \mathfrak{b}$ (multiplication and reduction) followed by at most $2g$ perturbed reduction steps.

Principal infrastructure is almost an abelian group under the operation $\otimes$ (small number of elements that for which associativity still fails).

Analogy: Cyclic Group

Cyclic group G (order n, generated by g)

- g^i is at *distance* i from 1
- baby step (multiplication by g) advances distance by exactly 1
- given g^i and g^j, $g^i g^j = g^{i+j}$ (distances are exactly additive)
- for $u, v \in \mathbb{Z}$, we have $g^u = g^v$ iff $u \equiv v \pmod{n}$

Principal infrastructure ("order" R_F)

- $\delta(\mathfrak{a}_i)$ is the *distance* from $\mathcal{O}_F$
- perturbed reduction step advances distance by 1 in "most" cases
- given $\mathfrak{a}_i$ and $\mathfrak{a}_j$, $\mathfrak{a}_i \otimes \mathfrak{a}_j$ yields $\mathfrak{a}_k$ with $\delta(\mathfrak{a}_k) \approx \delta(\mathfrak{a}_i) + \delta(\mathfrak{a}_j)$ (not a group)
- we have $(\alpha) = (\beta)$ iff $\deg(\alpha) \equiv \deg(\beta) \pmod{R_F}$

Applications

Invariant computation:

- ideal class number
- regulator and fundamental unit

Public-key cryptography:

- behaves sufficiently like a group that most protocols work as in a cyclic group — problems only with probability $1/q$ (assuming $K = \mathbb{F}_q$)
- security related to *principal ideal problem* — given $\mathfrak{a}$, compute $\delta(\mathfrak{a})$
- various techniques have been developed to avoid problems
- improvements to eliminate almost all of the reduction steps

Comparison to Jacobian

Mirales Morales (2007): map between class of $\infty_+ - \infty_-$ and infrastructure

- balanced representations of divisor classes (with $n = 0$) map to infrastructure elements
- classes with balanced reps with $n \neq 0$ correspond to problems with the $\otimes$ operation ("holes")

Consequences:

- principal infrastructure and class of $\infty_+ - \infty_-$ are computationally equivalent — can compute invariants or do cryptography in either structure
- Rezai Rad (2016): with the right definition of distance, computations in both are identical

Efficient Ideal Arithmetic in Split Models

Arbitrary Genus

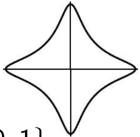
- Regular multiplication, Harley optimizations work
- J./van der Poorten (2003), J./Scheidler/Stein (2007): NUCOMP works, too.

Explicit formulas:

- Erickson/J./Stein (2011): genus 2 (slightly slower than ramified models)
- Rezai Rad/J./Scheidler: genus 3 (work in progress)

Explicit formulas using the geometric method have not been developed for split models of any genus.

Other Models of Elliptic and Hyperelliptic Curves



Most efficient elliptic curve arithmetic (odd characteristic):

- **Edwards models** $x^2 + y^2 = 1 + dx^2y^2$ with $d \in K \setminus \{0, 1\}$.

Most effient genus 2 hyperelliptic curves arithmetic:

- Gaudry (2007): theta functions on Kummer surfaces (not for all curves)
- No Edwards analogues known for $g \geq 2$

Non-Hyperelliptic Function Fields

Smooth plane quartics (genus 3, non-hyperelliptic)

Cubic Extensions of $\mathbb{F}_q(x)$

- Picard curves: $y^3 = f(x) \in \mathbb{F}_q[x]$ square-free with $\deg(f) = 4$
- general radical extension $K = \mathbb{F}_q(x, y)$ with $y^3 = f(x)$ with $f(x) \in \mathbb{F}_q[x]$ cube-free and characteristic $\neq 3$
- Bauer/Webster (2013): certain cubics in characteristic 3

Superelliptic curves: $y^n = f(x)$, ramified (Galbraith/Paulus/Smart 2000)

Arbitrary extensions of unit rank 2 (Tang 2011)

Some **general** arithmetic for arbitrary function fields by Hess and others

- Divisor addition is easy (ideal multiplication)
- Reduction is generally hard

Applications of Geometric Method

$C_{a,b}$ **curves:**

- $y^a + c_{b,0}x^b + \sum_{ia+jb<ab} c_{ij}x^iy^j = 0 \quad (c_{ij} \in K)$
- Explicit formulas, using geometric method / linear algebra for $C_{3,4}$ (Salem/Khuri-Makdisi 2006) and $C_{3,5}$ (Oyono/Thériault 2013)

Jacobian of an arbitrary curve: (Khuri-Makdisi 2004)

Generalization to **abelian varieties:** (Murty/Sastry ongoing)