Isolated Curves for Hyperelliptic Curve Cryptography

Wenhan Wang
Department of Mathematics
University of Washington

October 29, 2012

Conductor Gap and Isogeny

- Let C and C' be genus two curves with isogenous simple ordinary Jacobians. It follows that $\mathrm{End}(J_C)$ and $\mathrm{End}(J_{C'})$ are both orders in a quartic totally imaginary field K.
- The largest prime number dividing the conductor of one of $\mathrm{End}(J_C)$ and $\mathrm{End}(J_{C'})$ but not the other is called the conductor gap of C and C'.
- The conductor gap between C and C' divides the degree of any isogeny from C to C'.
- Such isogenies are difficult to construct if the conductor gap is larger than 80 bits.

Isolated Curves

- Let C be a genus two curve with simple Jacobian such that $\mathrm{End}(J_C) = \mathcal{O}_K$.
- C is called an isolated curve, if C has large conductor gap (≥ 80 bits) with curves in any other endomorphism classes.
- If C is isolated and the endomorphism class of C is small, then it is difficult to construct isogenies from C to almost all other non-isomorphic curves (except for those in the same endomorphism class).

The Curve $Y^2 = X^5 + a$

- Let $p \equiv 1 \mod 5$ be a prime number, so that $Y^2 = X^5 + a$ is non-supersingular over $\mathbf{F}_p$.
- Let ζ be a primitive fifth root of unity in $\mathbf{F}_p$
- $(X, Y) \mapsto (\zeta X, Y)$ induces an automorphism of order 5 on J_C.
- $Y^2 = X^5 + a$ has CM by the maximal order $\mathcal{O}_K = \mathbf{Z}[\zeta]$, where $K = \mathbf{Q}(\zeta)$, $\zeta = e^{2\pi i/5}$.

Representation of Weil p-numbers in $\mathbf{Q}(\zeta_5)$

- The Weil p-number π can be written as

$$\pi = \frac{1}{4}\left(A + B\sqrt{5} + C\sqrt{-5-2\sqrt{5}} + D\sqrt{-5+2\sqrt{5}}\right).$$

- A, B, C, D have the same parity.
-

$$\begin{aligned} p = \pi\bar{\pi} &= \frac{1}{16}(A^2 + 5B^2 + 5C^2 + 5D^2) \\ &\quad + \frac{1}{16}(2AB + 2C^2 + 2CD - 2D^2)\sqrt{5} \end{aligned}$$

- The index of $\mathbf{Z}[\pi, \bar{\pi}]$ in $\mathcal{O}_K$ is $B^2\left|C^2 - 4CD - D^2\right|$.
- In order that this curve is isolated, we need $B = \pm 1$ and $\left|C^2 - 4CD - D^2\right|$ to be a prime number.

Determine Isolated Curves

In order that $C : Y^2 = X^5 + a$ is isolated:

- $A^2 + 5 + 5C^2 + 5D^2 = 16p$ is 16 times an odd prime.
- $A = \pm(D^2 - CD - C^2)$.
- The index $\frac{1}{4}\left|C^2 - 4CD - D^2\right|$ is a prime number.

How often is a curve isolated?

- Consider $K = \mathbf{Q}(\zeta_5)$ (results can be generalized to similar cyclic extensions).
- How often is an ordinary genus two curve with CM by $\mathcal{O}_K$ isolated?
- Let C and D be random odd integers.
- How often are both
  - $p = \frac{1}{16}\left(C^2 + CD - D^2\right)^2 + 5 + 5C^2 + 5D^2)$
  - Index $I = \frac{1}{4}\left|C^2 - 4CD - D^2\right|$

  prime numbers?

Asymptotic Distribution of Isolated Curves

- The probability of both p and l being prime numbers is

$$\lim_{B\to\infty}\prod_{l\leq B} c(l)\cdot\frac{1}{\log p\log l}.$$

- Here l ranges among all prime numbers no larger than B, and $c(l)$ is the local correction factor.
- The above infinite product converges conditionally if $c(3)\neq 0$.
- Proof. Transform and Chebotarev density theorem.

Summary of Local Correction Factors

$$c(l) := \frac{\text{Prob}(l \nmid p \text{ and } l \nmid l)}{(1-1/l)^2}.$$

	prime number l	correction factor $c(l)$
$l \neq 2$	$l \equiv 1 \mod 5$	$(1-2/(l-1))^2$
	$l \equiv 4 \mod 5$	1
	$l \equiv 2,3 \mod 5$	$(1+2/(l-1))$
	$l = 5$	$(1+1/(l-1))$
$l = 2$		4

Computation Evidence

Bound	Actual Number	Predicted Number	Discrepancy
200	896	918	0.02455
400	2575	2638	0.02447
600	4833	5002	0.03497
800	7759	7940	0.02332
1000	11316	11413	0.00857
1200	15308	15390	0.00536

Thank you!