Point-counting on families of curves with geometrically split Jacobian

Semyon Novoselov

Immanuel Kant Baltic Federal University

ECC 2019. Rump Session.
December 2, 2019

My work

Curves with geometrically split Jacobians

- $\mathrm{Jac}_C(\mathbb{F}_{q^k}) \sim \mathrm{Jac}_{X_1} \times \mathrm{Jac}_{X_2}$
- $\mathrm{Jac}_C(\mathbb{F}_q)$ is simple or has factors of cryptographic interest ($g = 2, 3$)

What I've done?

- Implemented general algorithm for computation of $\chi_{C,q}(T)$ from $\chi_{C,q^k}(T)$ (Sage, slow, any g).
- Generalization of Satoh'09 algorithm for curves $y^2 = x^5 + ax^3 + bx$ to $g > 2$.
- Obtained full lists of $\chi_{C,q}(T) \pmod p$ via Legendre polynomials.

Generalized Legendre/Satoh curves

$$C : y^2 = x^{2g+1} + ax^{g+1} + bx$$

$$\mathrm{Jac}_C(k) \sim \mathrm{Jac}_{X_1} \times \mathrm{Jac}_{X_2}$$

Odd g

$k \simeq \mathbb{F}_q[\sqrt[g]{b}]$

$X_1 : y^2 = D_g(x, \sqrt[g]{b}) + a$

$X_2 : y^2 = (x^2 - \sqrt[g]{b})(D_g(x, \sqrt[g]{b}) + a)$

$\mathrm{Jac}_C(\mathbb{F}_q) \sim E \times A$

Even g

$k \simeq \mathbb{F}_q[\sqrt[2g]{b}]$

$X_1 : y^2 = (x + 2\sqrt[2g]{b})(D_g(x, \sqrt[g]{b}) + a)$

$X_2 : y^2 = (x - 2\sqrt[2g]{b})(D_g(x, \sqrt[g]{b}) + a)$

$\mathrm{Jac}_C(\mathbb{F}_q)$ can be simple.

Methods

Kani-Rosen'89, Tautz-Top-Verberkmoes'91 ($b = 1$), Smith'05 (odd g, X_1), Paulhus'07 (over $\overline{k}$).

Genus 3 case

$$y^2 = x^7 + ax^4 + bx$$

- $\mathrm{Jac}_C(\mathbb{F}_q) \sim E_1 \times A$
- $\mathrm{Jac}_C(\mathbb{F}_{q^3}) \sim E_1 \times E_2 \times \widetilde{E}_2$
- $E_1 : y^2 = x^3 + ax^2 + bx$, A is abelian surface
- $E_2 : y^2 = x^3 - 3\sqrt[3]{b}x + a$

Example: 256-bit prime group order

- $p = b8f1c70570a105ab167718f29ac140b5$
- $a = 3a55c031b0e04911dab20f29af712b8e$
- $b = 730b82ddda1819bb43014650f43bb5eb$

$\#A = 859c727024defc8b8ee1533ed8c992b41e559b27aca96a7485a4914927c0373d$

- $A(\mathbb{F}_{p^2})$ is simple

- $A \sim J_D$ for some curve D (the explicit equation is yet to be found).

Application of Cartier-Manin method

- $\#Jac_C(\mathbb{F}_q)$ mod p can be written in terms of Legendre polynomials P_n.

Example: List of characteristic polynomials (mod p) for $b = 1$

g	conditions	$\chi_p(T) \pmod p$
2	$p \equiv 1 \pmod 4$	$T^2(T - P_{(p-1)/4})^2$
2	$p \equiv 3 \pmod 4$	$T^2(T^2 - P^2_{(p-3)/4})$
3	$p \equiv 1 \pmod 3$	$T^3(T - P_{(p-1)/2})(T - P_{(p-1)/6})^2$
3	$p \equiv 2 \pmod 3$	$T^3(T - P_{(p-1)/2})(T^2 - P^2_{(p-5)/6})$
4	$p \equiv 1 \pmod 8$	$T^4(T - P_{(p-1)/8})^2(T - P_{(3p-3)/8})^2$
4	$p \equiv 3 \pmod 8$	$T^4(T^2 - P_{(p-3)/8}P_{(3p-1)/8})^2$
4	$p \equiv 5 \pmod 8$	$T^4(T^2 - P_{(p-5)/8}P_{(3p-7)/8})^2$
4	$p \equiv 7 \pmod 8$	$T^4(T^2 - P^2_{(p-7)/8})(T^2 - P^2_{(3p-5)/8})$
5	$p \equiv 1 \pmod 5$	$T^5(T - P_{(p-1)/2})(T - P_{(p-1)/10})^2(T - P_{(3p-3)/10})^2$
5	$p \equiv 2 \pmod 5$	$T^5(T - P_{(p-1)/2})(T^4 - P^2_{(p-7)/10}P^2_{(3p-1)/10})$
5	$p \equiv 3 \pmod 5$	$T^5(T - P_{(p-1)/2})(T^4 - P^2_{(p-3)/10}P^2_{(3p-9)/10})$
5	$p \equiv 4 \pmod 5$	$T^5(T - P_{(p-1)/2})(T^2 - P^2_{(p-9)/10})(T^2 - P^2_{(3p-7)/10})$

- Further work:
  - generalization to other curves with non-trivial $\mathrm{Aut}_C(\overline{k})$
- Would be happy to cooperate in topics:
  - isogenies (esp. ℓ-adic and function-field theoretic methods)
  - point-counting (esp. ℓ-adic, SEA generalization)
- More details for curves $y^2 = x^{2g+1} + ax^{g+1} + bx$: `https://arxiv.org/abs/1902.05992`
- Email: snovoselov@kantiana.ru

Thank you!