5. *Cohen H.* A Course in Computational Algebraic Number Theory. Springer Science & Business Media, 2013.
6. *Lemmermeyer F.* The Ambiguous Class Number Formula Revisited. arXiv preprint arXiv:1309.1071,2013.
7. *Kirchner P.* Algorithms on Ideal over Complex Multiplication Order. arXiv preprint arXiv:1602.09037, 2016.
8. *Schoof R.* Computing Arakelov class groups. arXiv preprint arXiv:0801.3835, 2008.
9. *Adleman L. M.* Factoring numbers using singular integers. Proc. 23th Ann. ACM Symp. Theory of Computing, ACM, 1991, pp. 64–71.
10. *Pollard J. M.* Theorems on factorization and primality testing. Math. Proc. of the Cambridge Philosophical Soc., Cambridge Univ. Press, 1974, vol. 76, no. 3, pp. 521–528.
11. *Williams H. C.* A $p + 1$ method of factoring. Math. Computation, 1982, vol. 39, no. 159, pp. 225–234.
12. *Bach E. and Shallit J.* Factoring with cyclotomic polynomials. Math. Computation, 1989, vol. 52, no. 185, pp. 201–219.
13. *Cox D. A.* Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. John Wiley & Sons, 2011, vol. 34.
14. *Klüners J. and Pauli S.* Computing residue class rings and Picard groups of orders. J. Algebra, 2005, vol. 292, no. 1, pp. 47–64.
15. *Buchmann J. A. and Lenstra H. W.* Approximating rings of integers in number fields. J. de théorie des nombres de Bordeaux, 1994, vol. 6, no. 2, pp. 221–260.

UDC 512.772.7 DOI 10.17223/2226308X/11/9

COUNTING POINTS ON HYPERELLIPTIC CURVES OF TYPE $y^2 = x^{2g+1} + ax^{g+1} + bx^1$

S. A. Novoselov

In this work, we investigate hyperelliptic curves of type $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ over the finite field $\mathbb{F}_q$, $q = p^n$, $p > 2$. For the case of $g = 3$ or 4, $p \nmid 4g$ and b is a $4g$-root, we provide efficient methods to compute the number of points in the Jacobian of the curve.

Keywords: *hyperelliptic curves, Cartier — Manin matrix, Legendre polynomials, point counting.*

Let $\mathbb{F}_q$ be a finite field, $q = p^n, p > 2$. Hyperelliptic curves with equation

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

were investigated in [1 – 3]. For genus 2 case it is known [4] that Jacobian of such curves splits into product of certain elliptic curves over some extension of the base field. There are explicit formulae [5] expressing number of points in the Jacobian of curve in terms of traces of Frobenius of elliptic curves.

In this work, we generalize this approach to genus 3, 4 case combining it with computing Cartier — Manin matrices where it's possible. Using the method of Paulhus [6, 7] we can obtain decompositions of the Jacobian over the extensions of the ground field. The Cartier — Manin matrix of the curve allows us to find the number of points on the curve modulo p.

[1] The reported study was funded by RFBR according to the research project no. 18-31-00244.

But in general it's only computable for finite fields of small characteristic. In the work [2] the curve C is transformed to the curve

$$C' : y^2 = x^{2g+1} - 2\rho x^{g+1} + x$$

defined over $\mathbb{F}[\sqrt{b}]$ via isomorphism defined over $\mathbb{F}_q[\sqrt[4g]{b}]$, and it is proved that the elements of the Cartier — Manin matrix of this curve can be expressed in terms of Legendre polynomials. But an efficient method to compute Legendre polynomials was not provided. In this work, we show how to compute these polynomials for the case $g = 3$ and big characteristic. Partial results for the case $g > 3$ are also provided.

1. Computing Cartier — Manin matrix of the curve C'

It is known that the number of points on certain elliptic curves can be expressed through Legendre polynomials. Thus some instances of the polynomials from [2, Table 1, 2] can be computed for finite fields of big characteristic using the Schoof — Elkies — Atkin [8, § 17.2.2] algorithm. We collect such cases in the following theorem.

Theorem 1 [9–11]. Let $c \in \mathbb{F}_p$, $p > 3$. Then

1) $P_{\frac{p-1}{2}}(c) \equiv \left(\dfrac{-6}{p}\right) t_2 \pmod{p}$, where t_2 is a trace of Frobenius of the elliptic curve $E_2 : y^2 = x^3 - 3(c^2 + 3)x + 2c(c^2 - 9)$;
2) $P_{\lfloor 3/p \rfloor}(c) \equiv \left(\dfrac{p}{3}\right) t_3 \pmod{p}$, where t_3 is a trace of Frobenius of the elliptic curve $E_3 : y^2 = x^3 + 3(4c - 5)x + 2(2c^2 - 14c + 11)$;
3) $P_{\lfloor p/4 \rfloor}(c) \equiv \left(\dfrac{6}{p}\right) t_4 \pmod{p}$, where t_4 is a trace of Frobenius of the elliptic curve $E_4 : y^2 = x^3 - \frac{3}{2}(3c + 5)x + 9c + 7$;
4) $P_{\lfloor p/6 \rfloor}(c) \equiv \left(\dfrac{3}{p}\right) t_6 \pmod{p}$, where $p > 5$ and t_6 is a trace of Frobenius of the elliptic curve $E_6 : y^2 = x^3 - 3x + 2c$.

Using this theorem we can compute Cartier — Manin matrix of curve C' of genus 3 completely. For the case of $g > 3$ we get partial information. For example, the polynomial $P_{\frac{p-1}{2}}$ appears in the formulae for $g = 5, 7$ in [2, Table 1, 2].

2. Decomposition of the Jacobian of the curve C' over finite field

In the work [6] there are decompositions for the curve C' over algebraically closed field. But the method works over any field as long as we know the group of automorphisms or its subgroups. So we need to obtain information about subgroups of this group over finite field. Denote by $\mathrm{Aut}_C(\mathbb{F}_q)$ an automorphism group of curve over the finite field $\mathbb{F}_q$, C_m a cyclic group of order m and by D_m a dihedral group of order m. Let also ζ_m be a primitive m-root of unity. Every hyperelliptic curve has hyperelliptic involution ω. Some other automorphisms of the curve C' are collected in the following theorem.

Theorem 2. Let $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ be a genus g hyperelliptic curve defined over the finite field $\mathbb{F}_q$, $q = p^n$.

1) $\mathrm{Aut}_{C'}(\mathbb{F}_q)$ contains a non-hyperelliptic involution $s : (x, y) \mapsto \left(\dfrac{1}{x}, \dfrac{y}{x^{g+1}}\right)$ and subgroup $C_2 \times C_2$.
2) If $p \nmid 2g$ and $2g|(q - 1)$ then $\mathrm{Aut}_{C'}(\mathbb{F}_q)$ contains an automorphism $r : (x, y) \mapsto$ $\mapsto (\zeta_g x, \zeta_{2g} y)$ of order $2g$ and subgroup D_{4g}.

Decompositions for the Jacobian of the curve C' follows from Theorem 2 and [7, Th. 4]:

— (genus 3) $J_{C'} \sim E \times J_D$ if $C_2 \times C_2 \subseteq \mathrm{Aut}_{\mathbb{F}_q}(C')$ and $J_{C'} \sim E_1^2 \times E_2$ if $D_{12} \subseteq \mathrm{Aut}_{\mathbb{F}_q}(C')$;

— (genus 4) $J_{C'} \sim J_{D_1} \times J_{D_2}$ if $C_2 \times C_2 \subseteq \mathrm{Aut}_{\mathbb{F}_q}(C')$ and $J_{C'} \sim J_D^2$ if $D_{16} \subseteq \mathrm{Aut}_{\mathbb{F}_q}(C')$

Note that $C_2 \times C_2 \subseteq \mathrm{Aut}_{\mathbb{F}_q}(C')$ holds in any field, thus we always have corresponding decomposition. But $D_{4g} \subseteq \mathrm{Aut}_{C'}$ holds in the field $\mathbb{F}_q[\zeta_{2g}]$, so we should work in an extension of $\mathbb{F}_q$ of degree up to $2g$ to get decomposition. The degree of this extension is the smallest integer k such that $2g|(q^k - 1)$.

3. Genus 3

If we apply Theorem 2 to the genus 3 case, we obtain following result.

Theorem 3. Let $C' : y^2 = x^7 + cx^4 + x$ be a genus 3 hyperelliptic curve defined over the finite field $\mathbb{F}_q, q = p^n, p > 3$. Then

1) $J_{C'} \sim E \times J_D$ over $\mathbb{F}_q$ for some genus 2 curve D and elliptic curve E;
2) $J_{C'} \sim E_1^2 \times E_2$ over $\mathbb{F}_q$ if $q \equiv 1 \pmod 6$ and over $\mathbb{F}_{q^2}$ if $q \equiv -1 \pmod 6$. E_1, E_2 are elliptic curves $E_1 : y^2 = x^3 - 3x + c$ and $E_2 : y^2 = x^3 + cx^2 + x$;
3) if $q \equiv 1 \pmod 6$, then $\#J_{C'}(\mathbb{F}_q) = (1 - t_1 + q)^2(1 - t_2 + q)$, where t_1, t_2 are traces of Frobenius of E_1, E_2 over $\mathbb{F}_q$;
4) if $q \equiv -1 \pmod 6$, then $\#J_{C'}(\mathbb{F}_{q^2}) = (1 - t_{1,2} + q^2)^2(1 - t_{2,2} + q^2)$, where $t_{1,2}, t_{2,2}$ are traces of Frobenius of the curves E_1, E_2 over $\mathbb{F}_{q^2}$. The Frobenius polynomial of the curve C' over $\mathbb{F}_q$ has a form

$$\chi_{C',q}(T) = (T^2 - tT + q)(T^4 - b_1T^3 + (a_{1,2} + t^2 + b_1t + b_1^2 - q)T^2 - qb_1T + q^2),$$

where $a_{1,2} = -(2t_{1,2} + t_{2,2})$, $t \in \mathbb{Z}$, $|t| \leqslant 2\sqrt{q}$, $b_1 \in \mathbb{Z}$, $|b_1| \leqslant 4\sqrt{q}$.

The traces $t_1, t_2, t_{1,2}, t_{2,2}$ can be efficiently computed using SEA-algorithm. By using results from Section 1 to compute polynomials from [2, Table 1, 2] we can efficiently compute $\chi_{C'}(T) \pmod p$ and therefore determine b_1, t. So, theorem 3 provides an efficient method to compute the number of points in the Jacobian of the curve C'.

Since the curve C is isomorphic to C' over $\mathbb{F}_q[\sqrt[12]{b}]$, theorem 3 also allows us to compute the number of points on C in the case $\sqrt[12]{b} \in \mathbb{F}_q$.

4. Genus 4

Applying Theorem 2 and [7, Th.4] to the curve C' of genus 4 we obtain following result.

Theorem 4. Let $C' : y^2 = x^9 + cx^5 + x$ be a genus 4 hyperelliptic curve defined over the finite field $\mathbb{F}_q$, $q = p^n$, $p > 2$ and $8|(q - 1)$. Then $J_{C'} \sim J_D^2$, where D is a genus 2 curve with equation $y^2 = (x^4 - 4x^2 + 2 + c)(x + 2)$.

Since the model of the curve D is known, we can use algorithm [12] to compute number of points in the Jacobian of the curve D and therefore in $J_{C'}$. This also allows us to compute the number of points on genus 4 hyperelliptic curve C in the case $\sqrt[16]{b} \in \mathbb{F}_q$.

Note that this algorithm has complexity $\mathrm{O}(\log^7 p)$ and less efficient than SEA algorithm with complexity $\tilde{\mathrm{O}}(\log^4 p)$, but still more efficient then general algorithms for genus 3 curves. Also, in this case we can't use results from Section 1, because we don't know how to efficiently compute Legendre polynomial $P_{\lfloor p/8 \rfloor}$.

REFERENCES

1. *Miller L.* Curves with invertible Hasse — Witt-matrix. Mathematische Annalen, 1972, vol. 197, no. 2, pp. 123–127.

2. *Novoselov S.A.* Hyperelliptic curves, Cartier — Manin matrices and Legendre polynomials. Prikladnaya Diskretnaya Matematika, 2017, no. 37, pp. 20–31.
3. *Leprevost F. and Morain F.* Revetements de courbes elliptiques a multiplication complexe par des courbes hyperelliptiques et sommes de caracteres. J. Number Theory, 1997, vol. 64, no. 2, pp. 165–182.
4. *Satoh T.* Generating genus two hyperelliptic curves over large characteristic finite fields. LNCS, 2009, vol. 5479, pp. 536–553.
5. *Guillevic A. and Vergnaud D.* Genus 2 hyperelliptic curve families with explicit jacobian order evaluation and pairing-friendly constructions. LNCS, 2012, vol. 7708, pp. 234–253.
6. *Paulhus J. R.* Elliptic factors in Jacobians of low genus curves. Phd Thesis, 2007.
7. *Paulhus J. R.* Decomposing Jacobians of curves with extra automorphisms. Acta Arith., 2008, vol. 132, no. 3, pp. 231–244.
8. *Cohen H., Frey G, et al.* Handbook of Elliptic and Hyperelliptic Curve Cryptography. CRC Press, 2005.
9. *Sun Z. H.* Congruences concerning Legendre polynomials II. J. Number Theory, 2013, vol. 133, no. 6, pp. 1950–1976.
10. *Sun Z. H.* Congruences involving $\binom{2k}{k}^2\binom{3k}{k}$. J. Number Theory, 2013, vol. 133, no. 5, pp. 1572–1595.
11. *Sun Z. H.* Legendre polynomials and supercongruences. Acta Arith., 2013, vol. 159, no. 2, pp. 169–200.
12. *Gaudry P. and Schost E.* Genus 2 point counting over prime fields. J. Symbolic Comput., 2012, vol. 47, no. 4, pp. 368–400.