On Two Moduli Problems Concerning Number of Points and Equidistribution over Prime Finite Fields

Nikolaj M. Glazunov

Glushkov Institute of Cybernetics NAS
03680 Ukraine Kiev-680 Glushkov prospect 40
Email: glanm@d105.icyb.kiev.ua

Introduction

The subject matter of this communication lies in the area between moduli theory and arithmetic geometry over finite fields. Let \( B \) be a class of objects. In our case these are classes of hyperelliptic curves of genus \( g \) over prime finite field \( F_p \) and Kloosterman sums \( T_p(c, d), c, d \in F_p^* \). Let \( S \) be a scheme. A family of objects parametrized by the \( S \) is the set of objects

\[ X_s : s \in S, X_s \in B \]

equipped with an additional structure compatible with the structure of the base \( S \).

We shall consider two problems:

(i) existence of precise (exact) bound for families of hyperelliptic curves over \( F_p \); and

(ii) equidistribution of angles of Kloosterman sums.

Moduli and estimates for hyperelliptic curves of genus \( g \geq 2 \) over \( F_p \)

Let

\[ C : y^2 = f(x) \]

be an algebraic curve and let \( \text{Disk}(C) \) be the discriminant of \( f(x) \). Let \( p \geq 3 \) be a prime. Consider hyperelliptic curve of genus \( g \geq 2 \) over prime finite field \( F_p \)

\[ C_g : y^2 = f(x), \ D(f) \neq 0. \]

For projective closure of \( C_g \) the quasiprojective variety

\[ S_{g,p} = \{ \mathbb{P}^{2g+2}(F_p) \setminus (\text{Disk}(C_g) = 0) \} \]
parametrizes all hyperelliptic curves of genus $g$ over $\mathbb{F}_p$. By well known Weil bound (affine case)
\[ |\#C_g(\mathbb{F}_p) - p| \leq 2g\sqrt{p}. \]
where $\#C$ is the number of points on the curve $C$ over ground field. As we can see from Weil (and some more strong) bounds, for $p \geq 17$ any hyperelliptic curve of genus $g = 2$ has points in $\mathbb{F}_p$ for these prime $p$. Also for $g = 3$ every hyperelliptic (h) curve of genus 3 has points in $\mathbb{F}_p$ for $p \geq 37$. For $p = 3, 5, 7, 11$ there are examples of h-curves of genus 2 that have not points in $\mathbb{F}_p$. By author’s computations [2], any h-curve of genus 2 over $\mathbb{F}_{13}$ has points in the field. Similarly, for $p = 3, 5, 7, 11, 13, 17, 19, 23$ there are examples of h-curves of genus 3 that have not points in $\mathbb{F}_p$.

**Problem of precise bound**

Let $\{F_{g,p}\}$ be a family of moduli spaces which is parametrized by parameters $g$ and $p$. Let $c \in F_{g,p}$ be an element and let $\#c$ be a numeric characteristic of $c$. Let $b(g,p,\#c)$ be a bound that is satisfied for all $c \in F_{g,p}$. Let $P(c,b(g,p,\#c))$ be a predicate on elements of $F_{g,p}$. We shall say that the bound $b(g,p,\#c)$ precisely (exactly) divides family $F_{g,p}$ if for any given $g$ there exists $p_0(g)$ such that for any $p \geq p_0(g)$ and for all $c \in F_{g,p}$ the predicate $P(c,b) = TRUE$, and for $p \leq p_0(g)$ exists $c \in F_{g,p}$ with $P(c,b) = FALSE$.

Let $F = S_{g,p}$ be the quasiprojective variety of hyperelliptic curves of genus $g$, $C_g \in S_{g,p}$, $\#C_g$ be the number of points of $C_g$ in $\mathbb{F}_p$.

**Problem** Does the precise bound for family $S_{g,p}$ exists? If the precise bound exists what is its representation?

More elaborately we have the following situation: let
\[ f(x) = x^{2n+1} + a_1x^{2n} + \cdots + a_{2n}x + a_{2n+1}. \]
Let $degf = 2n + 1 (n = 1, 2, 3, ...)$ or genus(C) = $g(g = 1, 2, 3, ...)$.
Examples
- If $degf = 3$ or $g = 1$ then $p_0 = 3$ (by M-bound every this curve has points in $\mathbb{F}_p$ for $p \geq 5$).
- If $degf = 5$ or $g = 2$ then $p_0 = 13$ (by M-bound every this curve has points in $\mathbb{F}_p$ for $p \geq 17$).
- If $degf = 7$ or $g = 3$ then $p_0 = 29$ (conjecture) (by M-bound every this curve has points in $\mathbb{F}_p$ for $p \geq 31$).
- If $degf = 9$ or $g = 4$ then $p_0 = ?$ (by M-bound every this curve has points in $\mathbb{F}_p$ for $p \geq 61$).
for \( p \geq 53 \).

Let \( \#c \) be the number of points of an algebraic curve \( c \) over prime finite field. Then the predicate is \(((\text{For all } c \in S_{g,p}) \& b(g, p, \#c) \Rightarrow (\#c > 0))\).

**Problem of distribution of Kloosterman sums**

Let

\[
T_p(c, d) = \sum_{x=1}^{p-1} e^{2\pi i \frac{cx+d}{p}}
\]

\[1 \leq c, d \leq p-1; \quad x, c, d \in F_p^*
\]

be a Kloosterman sum.

By A. Weil estimate

\[
T_p(c, d) = 2 \sqrt{p} \cos \theta_p(c, d)
\]

There are possible two distributions of angles \( \theta_p(c, d) \) on semiinterval \([0, \pi)\):

a) \( p \) is fixed and \( c \) and \( d \) varies over \( F_p^* \); what is the distribution of angles \( \theta_p(c, d) \) as \( p \to \infty \);

b) \( c \) and \( d \) are fixed and \( p \) varies over all primes not dividing \( c \) and \( d \).

For the case a) N. Katz [3], A. Adolphson [4] and Chai & Winnie Li [5] proved that \( \theta \) are distributed on \([0, \pi)\) with density \( \frac{2}{\pi} \sin^2 t \).

It is interesting to compare results of computer experiments in cases a) and b). Such computations [6] and [7] demonstrated that though in case b) equidistribution is possible but results of computation shows not so good compatibility with equidistribution as in (proved) case a).

**Acknowledgments**

I would like to thank V.M. Sidelnikov, Winnie Li and Mike Zieve for questions, notes and information.

**References**

[1] Harris J., Morrison J. Moduli of curves. *GTM 187, Springer, 1998, 366p.*

[2] Glazunov N.M., Postnikov A.G. *Researches in Number Theory (in Russian), Saratov:SGU, 1988, p.2-8.*
[3] Katz N. Gauss sums, Kloosterman sums, and monodromy groups. NJ: Princeton university press, 1988.246p.

[4] Adolphson A. Journ. rein. angew. Math., 395, (1989), pp.214-220.

[5] C.-L. Chai, W.-C. Winnie Li. Character sums, automorphic forms, equidistribution, and Ramanujan graphs. 18p. (submitted).

[6] Letter of Mike Zieve.

[7] Glazunov N.M. On a mathematical machine oriented to the study of Diophantine equations.2.Computations in algebra, combinatorics and number theory. Kiev: Inst. of Cyb. Ac.Ukr.SSR.1980. (in Russian)

[8] Glazunov N.M. Dokladi Ukr. Acad. of Sci. Kiev, ser.A, 3, (1983), pp.9-12 (in Russian).

[9] Glazunov N.M. Representation Theory and Computer Algebra. Int. Conf. Kiev: Math. Institute, (1997). p.51.