On Arithmetic Of Hyperelliptic Curves

Jing Yu

Abstract

In this exposé, Pell's equation is put in a geometric perspective, and a version of Artin's primitive roots conjecture is formulated for hyperelliptic jacobians. Also explained are some recent results which throw new lights, having to do with Ankeny-Artin-Chowla's conjecture, class number relations, and Cohen-Lenstra heuristics.

Introduction

It is well known that there are close connections between the arithmetic behavior of algebraic number fields and that of the algebraic function fields in one variable over finite fields. This connection has been a constant source for exciting developments of number theory in 20th century. In this article we shall further explore the subject by examining some arithmetic questions about hyperelliptic function fields viewed as analogues of quadratic number fields.

Let $\mathcal{C}$ be a hyperelliptic curve over an arbitrary base field k, i.e. a double cover of the projective line $\mathbb{P}_{/k}$. Its function field K is a separable quadratic extension of the rational function field $k(t)$. In analogy with the classical situation, K is called an imaginary quadratic function field if the point at infinity ∞ on $\mathbb{P}_{/k}$ does not split into two points on $\mathcal{C}$. Otherwise K is said to be a real quadratic function field. If the characteristic of k is not 2, we may always write $K = k(t, \sqrt{D})$, with $D \in k[t]$ a square free polynomial. In that case K is real if and only if $\deg D$ is even, positive and the leading coefficient of D is a square in $k^\times$.

Contents

1.Fundamental units of real quadratic function fields

Given a real quadratic function field K/k. Abel [1] asked the following question: whether there exist functions in K whose divisors supported only at infinity? In other words, if ∞_+ and ∞_- are the two points on $\mathcal{C}$ above ∞, he is looking for functions with divisors of the form $n(\infty_+ - \infty_-)$, $n \in \mathbb{Z}$. A function in K has this property if and only if it is a non-constant unit inside the the integral closure B of $k[t]$ in K. If such functions do exist, then it follows that $B^\times \cong k^\times \times \mathbb{Z}$. If such function does not exist, then $B^\times = k^\times$. A non-constant function u such that $uk^\times$ generates $B^\times/k^\times$ is called a fundamental unit of K. If u is a fundamental unit with $\operatorname{div} u = n(\infty_+ - \infty_-)$, then $|n|$ is the least positive integer such that the $n(\infty_+ - \infty_-) \sim 0$. We call $|n|$ the regulator of K (or $\mathcal{C}$). In the case of characteristic $\neq 2$ and $K = k(t, \sqrt{D})$, one may write $u = r + s\sqrt{D}$, with $r, s \in k[t]$. Then $r^2 - s^2 D = \xi \in k^\times$. Thus finding units amounts to solving Pell's equations over polynomial rings.

Geometrically one considers the Jacobian variety of the curve $\mathcal{C}$. Then non-constant units exist in B if and only if the divisor class of $\infty_+ - \infty_-$ is a torsion point inside the Jacobian $\operatorname{Jac}\mathcal{C}$. The regulator of K is precisely the torsion in question. To find out whether such units exists for a given real quadratic function field, Abel makes an appeal to the well-known continued fractions method for solving Pell's equation.

Suppose the characteristic of k is $\neq 2$. Expand $\sqrt{D(t)}$ binomially in the formal series field $k((1/t))$ as $\sqrt{D(t)} = a_0 + \frac{1}{\alpha_1}$, where $a_0 \in k[t]$ and $1/\alpha_1 \in k[[1/t]]/t$. Then write α_1 as $a_1 + \frac{1}{\alpha_2}$ with $a_1 \in k[t]$ and $1/\alpha_2 \in$

$k[[1/t]]/t$, ... Proceed in this way one arrives at the continued fraction expansion :

$$\sqrt{D(t)} = [a_0, a_1, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

As Abel observed, non-constant unit exists in $k[t, \sqrt{D}]$ if and only if this continued fraction expansion is quasi-periodic, in the sense that there are positive integers n_0 and l such that $\alpha_{n_0+l} = \xi\alpha_{n_0}$ for some $\xi \in k^\times$. If indeed quasi-periodicity happens, one can solve the Pell's equation non-trivially just as in the classical story of real quadratic number fields.

In the even characteristic case, hyperelliptic curves are given by Artin-Schreier curves: $y^2 + y = R(t)$, with $R(t) \in k(t)$. Abel's observation is still correct. One just has to write down the continued fraction expansion of the Artin-Schreier root instead of the square root, and Pell's equation replaced by a norm equation.

In general, one expects that non-constant units do not always exist in real quadratic function fields. The above procedure provides us only with a pseudo-algorithm to answer the question of existence of non-trivial units for real quadratic function fields. However if k is finite, the continued fractions in question are always periodic so that non-constant units can be found all the time.

The most interesting case is certainly the case $k = \mathbb{Q}$ and $D \in \mathbb{Z}[t]$.

To decide whether there are non-constant units in $\mathbb{Q}[t, \sqrt{D}]$, one reduces the equation $y^2 = D(t)$ modulo various odd primes p. For all but finitely many p (namely those dividing the discriminant of the polynomial $D(t)$), one obtains curve $\mathcal{C}_p$ over the finite field $\mathbb{F}_p$. Given such a prime p of "good" reduction. If the divisor class of $\infty_+ - \infty_-$ is of order n in $\operatorname{Jac}\mathcal{C}$, then unless $p \mid n$, the divisor class of $\infty_+ - \infty_-$ is also of order n in $\operatorname{Jac}\mathcal{C}_p$. This fact follows from the theory of reduction of abelian varieties. The assertion that $\infty_+ - \infty_-$ is of order n in $\operatorname{Jac}\mathcal{C}_p$ can be checked easily via continued fraction expansion of $\sqrt{D}$ modulo p. Therefore in this case, one also has at hand an effective algorithm to decide whether there are non-constant units.

Algorithm. *Given $D \in \mathbb{Q}[t]$ and consider the curve $\mathcal{C} : y^2 = D(t)$. Compute first the regulator m of $\mathbb{F}_p(t, \sqrt{D})$ for the least prime p of good reduction. Then choose another prime p_1 where the curve has good reduction and $p_1 \nmid m$. If the regulator m_1 of $\mathbb{F}_{p_1}(t, \sqrt{D})$ does not coincide with mp^i for some $i \geq 0$, then the divisor class of $\infty_+ - \infty_-$ must be of infinite order. Otherwise, one writes down a few terms of the continued fraction expansion of $\sqrt{D} = \alpha_0$. Let n_0 be the least integer such that $\deg_t \alpha_{n_0} > 0$ and $\deg_t \alpha'_{n_0} < 0$, where α'_{n_0} is the conjugate of α_{n_0} over $\mathbb{Q}(t)$. If $\sqrt{D}$ is quasi-periodic with period length l, then m_1 should also be the regulator of*

$\mathbb{Q}(t, \sqrt{D})$ and the following holds

$$\sum_{i=n_0}^{n_0+l-1} \deg_t \alpha_i = m_1.$$

This last identity can now be checked easily.

Remark. The above algorithm can be generalized inductively to decide the existence of non-constant units for real quadratic function field with constant field k finitely generated over its prime field. As a consequence, fundamental units even in the most general case, if exist, can always be found effectively through the continued fraction expansion.

Example 1.1. Curve is $\mathcal{C} : y^2 = t^{10} + t$. Checking continued fraction expansion of $\sqrt{t^{10}+t}$ in $\mathbb{F}_p((1/t))$, for $p = 5, 7, 11, 13$, one sees that the regulator of $\mathcal{C}_p$ is always 9. A fundamental unit of $\mathbb{Q}(t, \sqrt{t^{10}+t})$ is just $1 + 2t^9 + 2t^4\sqrt{t^{10}+t}$.

Example 1.2. Curve is $\mathcal{C} : y^2 = t^6 + t + 2$. The regulator of $\mathcal{C}_3$ is 13. The regulator of $\mathcal{C}_5$ is 21. Hence non-constant unit does not exist in $\mathbb{Q}[t, \sqrt{t^6+t^3+1}]$.

2. A horizontal class number one problem: Artin's conjecture for hyperelliptic Jacobians

Let K be the real quadratic function field of a given hyperelliptic curve $\mathcal{C}$ over a finite field $\mathbb{F}_q$. The ideal class group of of the integral closure of

$\mathbb{F}_q[t]$ in K is denoted by Cl_K. It is related to the Jacobian $\mathrm{Jac}\,\mathcal{C}$ through the following exact sequence of finite abelian groups

$$0 \to \mathrm{Jac}\,\mathcal{C}_\infty(\mathbb{F}_q) \to \mathrm{Jac}\,\mathcal{C}(\mathbb{F}_q) \to \mathrm{Cl}_K \to 0,$$

where $\mathrm{Jac}\,\mathcal{C}(\mathbb{F}_q)$ denote the group of $\mathbb{F}_q$-rational points on $\mathrm{Jac}\,\mathcal{C}$ identified as the divisor class group of degree 0 on $\mathcal{C}$, and $\mathrm{Jac}\,\mathcal{C}_\infty(\mathbb{F}_q)$ corresponds to the part of the divisor class group of $\mathcal{C}$ whose divisor classes are represented by divisors supported only at points of $\mathcal{C}$ lying above ∞. It follows that the class number h_K of K, i.e. the order of the ideal class group Cl_K, is precisely the order of $\mathrm{Jac}\,\mathcal{C}(\mathbb{F}_q)$ divided by the regulator of K. In particular the real quadratic function field K is of class number one if and only if $\mathrm{Jac}\,\mathcal{C}(\mathbb{F}_q)$ is a cyclic group and the divisor class $[\infty_+ - \infty_-]$ generates $\mathrm{Jac}\,\mathcal{C}(\mathbb{F}_q)$.

Back to the case $k = \mathbb{Q}$ and $D \in \mathbb{Z}[t]$. Let $\mathcal{C}$ be the hyperelliptic curve over $\mathbb{Q}$ given by $y^2 = D(t)$. Suppose that non-constant unit does not exist and the divisor class $[\infty_+ - \infty_-]$ corresponds to a point of infinite order inside the Mordell-Weil group $\mathrm{Jac}\,\mathcal{C}(\mathbb{Q})$. We are interested in the set $S_\mathcal{C}$ consisting of odd primes p where the curve $\mathcal{C}_{/\mathbb{Q}}$ has good reduction modulo p and satisfies

$$< [\infty_+ - \infty_-] >= \mathrm{Jac}\,\mathcal{C}_p(\mathbb{F}_p).$$

In other words, we are looking for the primes p for which $[\infty_+ - \infty_-]$ is a "primitive" point on the Jacobian of $\mathcal{C}$ modulo p.

Let $\mathcal{P}$ be the set of all prime numbers. As a higher dimensional generalization of Artin's conjecture, we ask for positivity of the density of $S_{\mathcal{C}}$:

Conjecture. *Suppose* $\operatorname{Jac}\mathcal{C}(\mathbb{Q})_{\mathrm{tor}}$ *is cyclic and* $\operatorname{Jac}_{\mathcal{C}}$ *is simple as an abelian variety over* $\mathbb{Q}$*. The following limit (called the density of* $S_{\mathcal{C}}$*):*

$$\lim_{s->1} \frac{\sum_{p\in S_{\mathcal{C}}} \frac{1}{p^s}}{\sum_{p\in\mathcal{P}} \frac{1}{p^s}},$$

exists and is positive provided $[\infty_+ - \infty_-]$ *is of infinite order inside* $\operatorname{Jac}_{\mathcal{C}}$*.*

Here $\operatorname{Jac}\mathcal{C}(\mathbb{Q})_{\mathrm{tor}}$ denotes the torsion part of the Mordell-Weil group. This cyclicity is clearly a necessary restriction. However even if this condition is not satisfied for the given curve, the set of those primes p for which $[\infty_+ - \infty_-]$ generates $\operatorname{Jac}\mathcal{C}_p(\mathbb{F}_p)$ modulo the part coming from global torsion should still has a positive density.

If this conjecture is true for the hyperelliptic $\mathcal{C}$, then there are infinitely many p for which the divisor class $[\infty_+ - \infty_-]$ is a primitive point on $\operatorname{Jac}\mathcal{C}_p$. This is also equivalent to the assertion that there are infinitely many primes p for which the real quadratic function field $\mathbb{F}_p(t, \sqrt{D})$ has class number one.

Classically, as Gauss observed, there are plenty real quadratic number fields of prime discriminants with class number one. Although it is unknown whether there are infinitely many (the class number one problem). As to the case of quadratic function fields over $\mathbb{F}_q$, class numbers can be computed effectively by either developing a theory of reduction for quadratic forms over $\mathbb{F}_q[t]$, or by an appeal to an analogue of Dirichlet's class number formula, as is done in Artin's Thesis for odd q [4]. Computations also indicate that real quadratic function fields with irreducible D are frequently there with class number one. This leads to empirical evidences in favor of the above generalization of Artin's conjecture to hyperelliptic Jacobians.

When the genus of the hyperelliptic curves is 1, this conjecture is a special case of Lang-Trotter's conjecture ([12] 1977) for elliptic curves. Although this conjecture is not known for any single elliptic curve yet, there are strong evidences to support it. Gupta-Murty (1986 [7]) proved that if the elliptic curve in question has complex multiplications, then the Lang-Trotter conjecture is true under the Generalized Riemann Hypothesis (GRH).

A weaker statement than our Conjecture 2.1 is the cyclicity conjecture. Let $S'_{\mathcal{C}}$ be the set consisting of odd primes p where the curve $\mathcal{C}_{/\mathbb{Q}}$ has good reduction modulo p and $\mathrm{Jac}\,\mathcal{C}_p(\mathbb{F}_p)$ is cyclic. Suppose $\mathrm{Jac}\,\mathcal{C}(\mathbb{Q})_{\mathrm{tor}}$ is also cyclic and $\mathrm{Jac}_{\mathcal{C}}$ is simple over $\mathbb{Q}$. Then the cyclicity conjecture says that the set $S'_{\mathcal{C}}$ should have positive density. Under GRH, this conjecture was proved by Serre (1978) for all elliptic curves over $\mathbb{Q}$ (the genus one case). In 1991 Gupta-Murty [8] succeeded in proving the infinitude of the set $S'_{\mathcal{C}}$ in the case of genus one without assuming GRH.

EXAMPLE 2.1. $\mathcal{C} : y^2 = t^6 + t + 2$.

p	$\#(\mathrm{Jac}\,\mathcal{C}_p(\mathbb{F}_p))$	*Regulator*	*ClassNo.*
3	13	13	1
5	21	21	1
7	76	38	2
11	91	13	7
13	156	13	12
17	451	451	1

3. A geometric analogue of Ankeny-Artin-Chowla's conjecture

In 1953 Ankeny, Artin and Chowla [2] asked the following question. Let $D = p$ be a prime number such that $p \equiv 1 \pmod 4$. Let $u = r + s\sqrt{D}$ be a fundamental unit of the real quadratic number field $\mathbb{Q}(\sqrt{D})$. Is it always true that p does not divide s?

Later on Mordell and Ankeny-Chowla [3] showed that this conjecture is equivalent to the following statement about the Bernoulli numbers: $p \nmid B_{p-1/2}$. Here the Bernoulli B_n are defined by

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} B_n \frac{z^n}{n!}.$$

Although no theoretical evidence has been found, computer search did find no counterexamples to this Ankeny-Artin-Chowla's conjecture in which $p < 10^8$.

A geometric analogue of this conjecture can however be proved without difficulty for hyperelliptic curves [14]. Let k be a field of characteristic $\neq 2$, $D \in k[t]$ monic square free. Let $g = (\deg D - 2)/2$, the genus of the hyperelliptic curve in question. Then we have

Theorem 3.1.. *Let $u = r + s\sqrt{D}$ be a fundamental unit of $k[T, \sqrt{D}]$, with $r, s \in k[T]$. Then* $\deg \gcd(D, s) \leq g$.

Remark 3.1. It follows immediately that $D \nmid s$ in this geometric situation. The corresponding general statement is nevertheless **false** for classical real quadratic number fields.

Remark 3.2. The inequality obtained in this Theorem is sharp, as a computation of fundamental units of $\mathbb{F}_5(t, \sqrt{D})$ with $\deg D = 4$ shows.

Remark 3.3. A corresponding Theorem for real quadratic function fields of characteristic 2 can also be proved. It is more subtle because of the occurrence of wild ramifications.

We now deduce Theorem 3.1 from the so-called *abc* Theorem of Mason. Write $D' = \gcd(D, s)$, $s = D's'$, $\deg D' = g'$, $\deg s' = m$, then $\deg r = m + g + g' + 1$. Let $a = r^2$, $b = -D(D's')^2$, $c \in k^\times$ is the norm of u. Then $a + b = c$ and $\gcd(a, b, c) = 1$. Since u is fundamental not all three of a, b, c are p^{th} powers if k is of characteristic $p \neq 0$. By Mason's Theorem,

$$\max \deg\{a, b, c\} \leq n_0(abc) - 1,$$

where $n_0(abc)$ is the number of distinct zeros of abc, and is $\leq \deg(rDs') = 2m + 3g + g' + 3$ in our case. Clearly, $\max \deg\{a, b, c\} = 2m + 2g + 2g' + 2$. Now Mason's theorem tells us $g' \leq g$, which is what we want to prove.

We recorded here the statement of the very elementary *abc* Theorem of Mason, cf. [11] :

Theorem 3.2.. *Let $a, b, c \in k[t]$ such that $a + b = c$, $a' \neq 0$ or $b' \neq 0$, and* $\gcd(a, b, c) = 1$. *Let $n_0(abc)$ be the number of distinct roots of abc. Then*

$$\max\{\deg a, \deg b, \deg c\} \leq n_0(abc) - 1.$$

4. Class number relations

In this section we consider imaginary quadratic function fields K over a finite field $\mathbb{F}_q$. Thus all hyperelliptic curves here have only one place above ∞. These quadratic function fields behave very much like imaginary quadratic number fields. Their class number, i.e. the order of the ideal class group of the integral closure of $\mathbb{F}_q[t]$ in K, grows with the discriminant, hence is usually large. One has the following exact sequence relating the ideal class group to the Jacobian $\operatorname{Jac} \mathcal{C}$:

$$0 \to \operatorname{Jac} \mathcal{C}(\mathbb{F}_q) \to \mathrm{Cl}_K \to \mathbb{Z}/\delta\mathbb{Z} \to 0,$$

where $\delta = 1$ or 2 according to whether ∞ is ramified in K or not.

Classically, one of the most effective way to compute tables of class numbers for imaginary quadratic number fields is through a beautiful formula of Hurwitz [10]. This formula, derived using informations from the moduli space of elliptic curves, gives relations between class numbers of different imaginary quadratic fields. This story has its counterpart in our setting of imaginary quadratic function fields over $\mathbb{F}_q$. The moduli space of elliptic curves is replaced by the moduli space of rank 2 Drinfeld $\mathbb{F}_q[t]$-modules introduced by Drinfeld [6].

This analogue of Hurwitz class number relation is first established by Jiu-Kang Yu [15] in the case q is odd, then by Julie T.-Y. Wang and Jing Yu [13] in the case q is even. The resulting formula gives interesting relations between the number of $\mathbb{F}_q$-rational points of the Jacobians of different imaginary hyperelliptic curves.

Here we shall write down only the even characteristic case. A separable quadratic function field over $\mathbb{F}_q$ can be normalized to $K = \mathbb{F}_q(t, \alpha)$ with α a root of $\wp(X) = X^2 + X = \frac{D_1}{D_2}$, where $D_1, D_2 \in \mathbb{F}_q[t]$, D_2 is monic and $\gcd(D_1, D_2) = 1$. Denote the leading coefficient of D_1 by $\mathrm{sgn} D_1$. K is imaginary if and only if either $\deg D_1 > \deg D_2$ or $\deg D_1 = \deg D_2$ and the equation $X^2 + X = \mathrm{sgn} D_1$ has no solution in $\mathbb{F}_q$. In both case we may assume that the prime factorization of D_2 in $\mathbb{F}_q[t]$ is $P_1^{e_1} \dots P_r^{e_r}$ and each exponent e_i is odd by adding an element $Q^2 + Q$ in $\mathbb{F}_q(t)$ to $\frac{D_1}{D_2}$. Define $B = B(D_2) = P_1^{\frac{e_1+1}{2}} \dots P_r^{\frac{e_r+1}{2}}$. If $\deg D_1 > \deg D_2$, we may also assume that $\deg D_1 - \deg D_2$ is odd. Given $R \in \mathbb{F}_q(t)$, we will use the following notation: $R \rightsquigarrow \frac{D_1}{D_2}$ means that R is normalized to $\frac{D_1}{D_2}$, in other words $X^2 + X = R$ and $X^2 + X = \frac{D_1}{D_2}$ define the same quadratic field over $\mathbb{F}_q(t)$.

Define Hasse symbol on the set of monic irreducible polynomials in

$\mathbb{F}_q[t]$ as follows:

$$\chi_{\frac{D_1}{D_2}}(P) = \begin{cases} 1 & \text{if } P \text{ splits in } K, \\ 0 & \text{if } P \text{ is ramified in } K. \\ -1 & \quad \text{otherwise.} \end{cases}$$

Given K and monic $f \in \mathbb{F}_q[t]$, the separable Hurwitz class number of conductor f is defined to be

$$H_{\frac{D_1}{D_2}}(Bf) = h_K \sum_{f'|f} (q^{\deg f'} \prod_{P|f'} (1 - \chi_{\frac{D_1}{D_2}}(P) q^{-\deg P})),$$

if $\deg D_1 \neq 0$, and if $D_1/D_2 = \xi \in \mathbb{F}_q$

$$H_\xi(f) = \frac{1}{(q+1)} \sum_{f'|f} (q^{\deg f'} \prod_{P|f'} (1 - \chi_\xi(P) q^{-\deg P})).$$

We also define for monic $m \in \mathbb{F}_q[t]$ that,

$$H_m(0) = \begin{cases} 0, & \text{if } m \text{ is not a square,} \\ -1/(q^2-1) & \text{if } m \text{ is a square,} \end{cases}$$

and

$$G_s(m) = 2H_m(0) + 2 \sum_{\substack{l \,\text{monic} \\ \xi \in \mathbb{F}_q^\times}} H_{\frac{D_1}{D_2}}(l),$$

where the sum is taken over those pairs (l, ξ) such that $\mathbb{F}_q(t)(\wp^{-1}(\xi m/l^2))$ $= \mathbb{F}_q(t)(\wp^{-1}(D_1/D_2))$ is imaginary (D_1/D_2 normalized).

The only inseparable quadratic function field $K = \mathbb{F}_q(\sqrt{t})$ has also to be taken into consideration here. Given monic $f \in \mathbb{F}_q[t]$. The inseparable Hurwitz class number of conductor f is defined to be

$$H_i(tf^2) = \sum_{f'|f} q^{\deg f'}.$$

Also set for monic $m \in \mathbb{F}_q[t]$ is:

$$G_i(m) = 2 \sum_{a \in \mathbb{F}_q[t]} H_i(a^2 + m),$$

where the sum runs over the unique a such that $\frac{a^2+m}{t}$ is a square in $\mathbb{F}_q[t]$.

Finally, our class number relations in characteristic 2 are given by:

Theorem 4.1.. *For any $m \in \mathbb{F}_q[t]$ monic, the sum $G_s(m) + G_i(m)$ is equal to*

$$\sum_{d|m} \max(q^{\deg d}, q^{\deg(m/d)}) - \sum_{\substack{d|m \\ \deg d = \frac{1}{2}\deg m}} \frac{q^{\deg m} - q^{\deg(m-d^2)}}{q-1} q^{-\frac{1}{2}\deg m}.$$

Example 4.1. Let $q = 2$ and $m = t^3+t+1$. Then $G_i(m) = 2H_i(t^3+t) == 2(1+2) = 6$. To calculate $G_s(m)$, we need to find D_1, D_2, l such that $\frac{t^3+t+1}{l^2} \rightsquigarrow \frac{D_1}{D_2}$. If $l = 1$, $t^3+t+1 = \frac{D_1}{D_2}$. Therefore, $D_1 = t^3+t+1$, $D_2 = 1$. If $l = t$, $\frac{t^3+t+1}{t^2} \rightsquigarrow t = \frac{D_1}{D_2}$. Therefore, $D_1 = t$, $D_2 = 1$. If $l = t+1$, $\frac{t^2+t+1}{t^2+1} \rightsquigarrow \frac{t^2+t+1}{t+1} = \frac{D_1}{D_2}$. Therefore, $D_1 = t^2+t+1$, $D_2 = t+1$. Hence,

$$\begin{aligned} G_s(m) &= 2(H_{t^3+t+1}(1) + H_t(t) + H_{\frac{t^2+t+1}{t+1}}(1)) \\ &= 2(1+2+2) = 10. \end{aligned}$$

On the other hand,

$$\sum_{d|m} \max(2^{\deg d}, 2^{\deg(m/d)}) = 16.$$

5. A vertical class number one problem; Cohen-Lenstra heuristics

Given finite field $\mathbb{F}_q$. We ask whether there are infinitely many real quadratic function fields over $\mathbb{F}_q$ which has class number one. In other words, infinitely many real hyperelliptic curves $\mathcal{C}$ such that the divisor class $[\infty_+ - \infty_-]$ generates $\mathrm{Jac}\,\mathcal{C}(\mathbb{F}_q)$. This is a vertical class number one problem, in the sense that the constant field is pinned down and one varies (the genus of) the curve in order to find real quadratic function fields of class number one. Like the old problem asked by Gauss, this one is also out of reach at present.

In order to make more precise conjectures, we follow Cohen-Lenstra [5]. The heuristic principle they introduced should hold well also in the geometric setting of hyperelliptic curves. Fix the constant field $\mathbb{F}_q$. Thus the class groups of imaginary quadratic function fields should behave as random finite abelian groups weighted by the reciprocal of the number of their automorphisms. On the other hand the class groups of real quadratic function fields should behave as the quotient of a random (weighted as before) finite abelian groups by the cyclic subgroup generated by a random point. In other words, the divisor class $[\infty_+ - \infty_-]$ should be a random $\mathbb{F}_q$-rational point on the Jacobians.

Basing on this heuristic ground, one can make various quantitative predictions about class numbers and ideal class groups. For example, fixing

q, the probability that the odd part of the ideal class group of real quadratic function fields over $\mathbb{F}_q$ is trivial, is the value below:

$$(2\prod_{m=2}^{\infty}\zeta(m)\prod_{n=1}^{\infty}(1-2^{-n}))^{-1}\approx 0.75446$$

This fits well with our computations of class numbers of real quadratic function fields when $q=2,3$, or 5.

Unlike the original conjectures by Cohen-Lenstra, the conjectures in this geometric setting are more reachable. It is supported not merely by numerical evidences but also by strong theoretical evidences. Indeed Jiu-Kang Yu (1994 [16]) proved theorems in this direction in which the exact values predicted by Cohen-Lenstra come out.

To state J.-K. Yu's results, let q be odd, p be an odd prime relatively prime to q. Let $\mathbb{Z}_p$ be the ring of p-adic integers. Let G be a finite abelian p-group. For any $n\geq 1$, let $X_n(\mathbb{F}_q)$ be the set consisting of $D\in\mathbb{F}_q[t]$, monic, square free and of degree n. Given $D\in X_n(\mathbb{F}_q)$, the ideal class group of $\mathbb{F}_q[t,\sqrt{D}]$ is denoted by Cl_D, and the corresponding Jacobian variety is denoted by Jac_D. In the following we state two of his theorems. The first concerns the probability that the p-part of an ideal class group of an imaginary quadratic function field is isomorphic to a given p-group :

Theorem 5.1.. *For any $n\geq 3$ odd, as q ranges over odd prime powers* *such that* $\gcd(p,q)=1$ *and* $p\nmid(q-1)$*, the limit*

$$\lim_{q\to\infty}\frac{\#\{D\in X_n(\mathbb{F}_q)\ \mid\ \mathrm{Cl}_D\otimes\mathbb{Z}_p\cong G\}}{\#X_n(\mathbb{F}_q)}=d_n(G)$$

exists. Furthermore

$$\lim_{\substack{n\to\infty\\ n\text{ odd}}}d_n(G)=\frac{c_p}{\#\operatorname{Aut}(G)},$$

where $c_p=\prod_{n=1}^{\infty}(1-p^{-n})$*.*

In the next Theorem, the divisor class $[\infty_+-\infty_-]$ inside the Jacobian of a real quadratic function field is viewed as a pointed group. One is interested in the probability that the p-part of this pointed group is isomorphic to a given pointed p-group:

Theorem 5.2.. *Let* (G,x) *be a pointed finite abelian p-group. For any* $n\geq 4$ *even, as q ranges over odd prime powers such that* $\gcd(p,q)=1$ *and* $p\nmid(q-1)$*, the limit*

$$\lim_{q\to\infty}\frac{\#\{D\in X_n(\mathbb{F}_q)\ \mid\ (\mathrm{Jac}_D(\mathbb{F}_q),[\infty_+-\infty_-])\otimes\mathbb{Z}_p\cong(G,x)\}}{\#X_n(\mathbb{F}_q)}=d_n(G,x)$$

exists. Furthermore

$$\lim_{\substack{n\to\infty\\ n\text{ even}}}d_n(G,x)=\frac{c_p}{\#\operatorname{Aut}(G,x)\#\operatorname{Aut}(G)},$$

where c_p *is as before.*

Yu's Theorems should be compared with the following strong conjectures based on Cohen-Lenstra heuristics, where q is **not allowed to vary**

:

Conjecture 5.1.. *Given q odd and prime p such that* $\gcd(p,q)=1$. *Then*

$$\lim_{\substack{n\to\infty \\ n \text{ odd}}} \frac{\#\{D \in X_n(\mathbb{F}_q) \ | \ \mathrm{Cl}_D \otimes \mathbb{Z}_p \cong G\}}{\# X_n(\mathbb{F}_q)} = \frac{c_p}{\# \operatorname{Aut}(G)}.$$

Conjecture 5.2.. *Given q odd and prime p such that* $\gcd(p,q)=1$. *Let (G,x) be a pointed finite abelian p-group. Then the limiting value*

$$\lim_{\substack{n\to\infty \\ n \text{ even}}} \frac{\#\{D \in X_n(\mathbb{F}_q) | (\mathrm{Jac}_D(\mathbb{F}_q), [\infty_+ - \infty_-]) \otimes \mathbb{Z}_p \cong (G,x)\}}{\# X_n(\mathbb{F}_q)}$$

is precisely

$$\frac{c_p}{\# \operatorname{Aut}(G,x) \# \operatorname{Aut}(G)}.$$

J.-K. Yu considers a projective system of étal coverings $\widetilde{X}_n$ of the scheme X_n. His proof of the above results is based on Weil's Conjecture as proved by Deligne, and the geometric fact that $\widetilde{X}_n$ is a geometrically connected variety over $\mathbb{F}_q$. The later relies on the connectivity of $\widetilde{X}_n(\mathbb{C})$ as an analytic variety, which comes from very deep algebraic geometry and a representation of the braid group B_n. Thus the routes those predicted values are derived are very very interesting.

In conclusion, there are many open problems in the arithmetic of hyperelliptic curves and we are still expecting more exciting developments.

Acknowledgement. This work has benefited from comments and suggestions by Jiu-Kang Yu.

References

[1] N. Abel, *Sur l'intégration de la Formale Différentiell $\rho dx/\sqrt{R}$ et ρ étant des Fonctions Entières*, Oeuvres Complètes, Tome 1, Christiania 1881.

[2] N.C. Ankeny, E. Artin, and S. Chowla, *The class number of real quadratic fields*, Annals of Math.**56** (1953), 479-492.

[3] N.C. Ankeny and S. Chowla, *A further note on the class number of real quadratic fields*, Acta Arith. **7** (1962), 271-272.

[4] E. Artin, *Quadratische Korper im Gebiet der hoheren Kongruenzen* I,II, Math. Zeit. **19** (1924), 153-246.

[5] H. Cohen and H.W. Lenstra, *Heuristics on class groups of number fields*, Lecture Notes in Math. **1068** (1984), 33-62, Springer-Verlag.

[6] V.G. Drinfeld, *Elliptic modules*,Math. Sbornik **94** (1974) transl. **23** (1974), 561-592.

[7] R. Gupta and M. Ram Murty, *Primitive points on elliptic curves*, Compositio Math. **58** (1986), 13-44.

[8] R. Gupta and M. Ram Murty, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. **101** (1990), 225-235.

[9] J. Hoffstein and M. Rosen, Âverage values of L-series in function fields, Jour. Reine Angew. Math. **426** (1992), 117-150.

[10] A. Hurwitz, *Über Relationen zwischen Klassenanzahlen binärer quadratischer Formen von negativer Determinante*, Math. Ann. **25**

(1885), 157-196.

[11] S. Lang, *Algebra*, 3rd ed. Addison-Wesley (1993).

[12] S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bul. Amer. Math. Soc. **83** (1977), 289-292.

[13] Julie T.-Y. Wang and Jing Yu, *On class number relations over function fields*, Jour. Numer Theory **69** (1998), 181-196.

[14] Jing Yu and Jiu-Kang Yu, *A note on a geometri analogue of Ankeny-Artin-Chowla's conjecture*, Contemporary Math.A.M.S. **210** (1998), 101-105.

[15] Jiu-Kang Yu, *A class number relation over function fields*, Jour. Numer Theory **54** (1995), 318-340.

[16] Jiu-Kang Yu, *Toward a proof of the Cohen-Lenstra conjecture in the function field case*, Preprint (1997).

Jing Yu
Institute of Mathematics
Academia Sinica, Taipei, Taiwan