PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 11, November 2008, Pages 3839–3850
S 0002-9939(08)09363-5
Article electronically published on June 3, 2008

DIOPHANTINE EQUATIONS AND CONGRUENCES OVER FUNCTION FIELDS

ELENA YUDOVINA

(Communicated by Ken Ono)

Abstract. We generalize the methods of Pierce for counting solutions to the congruence $X^a \equiv Y^b \bmod D$ and the square sieve method for counting squares in the sequence $f(X) + g(Y)$ to the function field setting.

1. Introduction and statement of results

Several recent papers by Pierce [8], [7] and Helfgott and Venkatesh [4] have made advances to the problem of bounding the 3-torsion of class groups of imaginary quadratic fields $\mathbb{Q}(\sqrt{-D})$. Consider the quadratic field $\mathbb{Q}(\sqrt{D})$ with class group $CL(D)$ and class number $h(D)$ for a nonzero integer D. Let $h_3(D)$ represent the size of the 3-torsion in $CL(D)$. It is conjectured that $h_3(D) \ll |D|^{\epsilon}$ for any $\epsilon > 0$. Until recently, the only known bound on $h_3(D)$ was $h_3(D) \leq h(D) \ll |D|^{1/2+\epsilon}$. Pierce uses the methods of counting solutions to certain congruences and Diophantine equations to get a bound of $h_d(D) \ll |D|^{\frac{1}{2}-\theta}$ for certain values of $\theta > 0$. The problem of p-torsion in class groups is discussed further in the more recent related work by Ellenberg and Venkatesh [1].

These methods can be considered over function fields. Let $p > 3$ be a fixed prime, $q = p^n$ a prime power, and set $K = \mathbb{F}_q(t)$ and $A = \mathbb{F}_q[t]$. For $D \in A$ we let $|D| = \#A/(D) = q^{\deg D}$. Write $CL(D)$ for the class group of $K[\sqrt{D}]$, and $h(D)$, $h_3(D)$ as in the number ring case. The bound for $h(D)$ is known [9, Proposition 5.11] to be

$$(\sqrt{q}-1)^{2g} \leq h(D) \leq (\sqrt{q}+1)^{2g},$$

where g is the genus of $K[\sqrt{D}]$, approximately $\frac{1}{2}\deg D$. However, due to the truth of the generalized Riemann hypothesis over function fields, one can show

$$h_3(D) \ll |D|^{1/3+\epsilon}$$

for any $\epsilon > 0$ (the proof due to Soundararajan is outlined in [4]). This is the best known result on this subject; the conjectured result is $h_3(D) \ll |D|^{\epsilon}$ for all ϵ.

Although the methods developed by Pierce do not give optimal bounds for the 3-torsion over function fields, we can generalize her methods for counting solutions to Diophantine equations, which are of independent interest. The following theorem is an analog of [8, Theorem 3] and bounds the number of solutions to a congruence.

Received by the editors July 25, 2007, and, in revised form, October 2, 2007.
2000 *Mathematics Subject Classification.* Primary 11D45.

Theorem 1.1. *Let D be square-free (i.e., a product of relatively prime irreducibles). Define*

$$N_D(a,b,x,y) := \#\{(X,Y) \in A^2 : X^a \equiv Y^b \bmod D, \deg X \le x, \deg Y \le y\}.$$

If $y < x \le d = \deg D$, and $a, b < p$, then for any $\epsilon > 0$,

$$N_D(a,b,x,y) \ll |D|^{\frac{1}{2}+\epsilon} + q^{x+y}\,|D|^{-1+\epsilon}.$$

The implied constant depends only on a, b, and ϵ.

The next theorem generalizes the square sieve methods of [7].

Theorem 1.2. *Let $f, g \in A[x]$ with $e_1 = \deg f$, $e_2 = \deg g$. Assume that e_1 is odd, $(e_1, e_2) = 1$, $e_2 < e_1 < p$, and $e_2(e_1 - 1) < p$. Let D be the lcm of the leading coefficients of f and g, and set $d = \deg D$. Let*

$$N(f,g,x,y) := \#\{(X,Y,Z) \in A^3 : Z^2 = f(X) + g(Y), \deg X \le x, \deg Y \le y\}.$$

If $y = ad$, $x = bd$ with $\frac{b}{3} < a < b$, $a < 1$, $b < 2$, then for any $\epsilon > 0$,

$$N(f,g,x,y) \ll q^{\frac{4}{7}x + \frac{11}{14}y + \epsilon x}.$$

Removing the restriction $\frac{b}{3} < a < b$, we have

$$N(f,g,x,y) \ll q^{\frac{2}{3}x + \frac{1}{2}y + \epsilon x}.$$

In both cases the implied constant depends only on a, b, e_1, e_2, and ϵ.

In Section 2 we prove Theorem 1.1, and in Section 3 we prove Theorem 1.2. In the last section we briefly derive the 3-torsion bounds which follow from these results.

2. Proof of Theorem 1.1

In this section we will bound

$$N_D(a,b,x,y) := \#\{X^a \equiv Y^b \bmod D, \deg X \le x, \deg Y \le y\} \tag{1}$$

when $y < x \le d = \deg D$.

We now set up some notation for additive characters on $A/(D)$ for some $D \in A$. As additive groups, $A/(D) \cong (\mathbb{F}_q)^d$, corresponding to each coefficient of the minimal representative for each polynomial. For $\psi_0, \dots, \psi_{d-1}$ characters on $\mathbb{F}_q$, write

$$\psi = \psi_{d-1} \cdot \psi_{d-2} \cdot \ldots \cdot \psi_0$$

to mean

$$\psi\left(a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \ldots + a_0\right) = \psi_{d-1}(a_{d-1}) \cdot \psi_{d-2}(a_{d-2}) \cdot \ldots \cdot \psi_0(a_0).$$

The trivial character on $\mathbb{F}_q$ will be denoted χ_0; by abuse of notation it may also stand for the trivial character on $A/(D)$. Finally, we write $\psi = \psi(k)$ to mean that $\psi = \psi_{d-1} \cdot \psi_{d-2} \cdot \ldots \cdot \psi_k \cdot \chi_0^k$ (that is, ψ acts trivially on the last k terms of the decomposition).

For $k < d$ let

$$\delta_k(F) := \begin{cases} 1, & F \text{ is the reduction } \bmod D \text{ of a polynomial of degree} \le k; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\delta_k = q^{-(d-k)} \sum_{\psi = \psi(k)} \psi$, where the sum is over all characters $\psi(k)$.

Using the above,

$$\begin{aligned} N_D(a,b,x,y) &= \sum_{X^a \equiv Y^b \bmod D} \delta_x(X)\delta_y(Y) \\ &= q^{x+y-2d} \sum_{\substack{\chi=\chi(x) \\ \psi=\psi(y)}} \sum_{X^a \equiv Y^b \bmod D} \chi(X)\psi(Y). \end{aligned} \tag{2}$$

Let

$$S_D(a,b,\chi,\psi) := \sum_{X^a \equiv Y^b \bmod D} \chi(X)\psi(Y). \tag{3}$$

Lemma 2.1. *For D_1, D_2 relatively prime,*

$$S_{D_1 D_2}(a,b,\chi,\psi) = S_{D_1}(a,b,\chi_1,\psi_1) S_{D_2}(a,b,\chi_2,\psi_2)$$

for some additive characters χ_i, ψ_i modulo D_i.

Proof. By the canonical ring isomorphism $A/(D_1D_2) \cong A/(D_1) \times A/(D_2)$, the congruence $(X_1, X_2)^a \equiv (Y_1, Y_2)^b \bmod D_1D_2$ is equivalent to $X_1^a \equiv Y_1^b \bmod D_1$ and $X_2^a \equiv Y_2^b \bmod D_2$. Simultaneously, the canonical isomorphism $A/(D_1D_2) \cong A/(D_1) \times A/(D_2)$ induces an isomorphism of their dual groups of characters, so we can write $\chi(X_1, X_2) = \chi_1(X_1)\chi_2(X_2)$ and $\psi(Y_1, Y_2) = \psi_1(Y_1)\psi_2(Y_2)$ for some additive characters $\chi_i, \psi_i \bmod D_i$. The result follows. □

We can therefore consider S_P for a prime modulus, in which case $A/(P)$ is a field. Letting $M \equiv X^a \equiv Y^b \bmod P$ we know that $M = Z^{\operatorname{lcm}(a,b)}$ for some Z. Consequently,

$$S_P(a,b,\chi,\psi) = \sum_{Z \bmod P} \chi(Z^{b/\gcd(a,b)})\psi(Z^{a/\gcd(a,b)}).$$

Since χ and ψ are additive characters on a finite field $\mathbb{F} = A/(P)$, we may write them as

$$\chi = \phi \circ \alpha, \quad \psi = \phi \circ \beta,$$

where α and β denote multiplication by $\alpha, \beta \in \mathbb{F}$ respectively, and ϕ is some nontrivial additive character. Therefore,

$$S_P(a,b,\chi,\psi) = \sum_{Z \bmod P} \phi(\alpha Z^{b/\gcd(a,b)} + \beta Z^{a/\gcd(a,b)}).$$

When at least one of α and β is nonzero, the Weil bound [10, Chapter II] gives

$$|S_P(a,b,\chi,\psi)| \le (\max(a,b)-1) q^{\frac{1}{2}\deg P} = (\max(a,b)-1)\,|P|^{\frac{1}{2}}. \tag{4}$$

For nonprincipal characters ($\alpha = \beta = 0$) the Weil bound does not apply, and we have only the trivial bound $|S_D(a,b,\chi,\psi)| \le |D|$.

By (2),

$$N_D(a,b,x,y) \ll q^{x+y-2d} \left(q^{2d-x-y} \eta^{\nu(D)} |D|^{\frac{1}{2}} + \sum_{\substack{\chi,\psi \\ \text{both nonprincipal}}} S_D(a,b,\chi,\psi) \right),$$

where $\eta = \max(a,b)-1$ and $\nu(D)$ is the number of irreducible divisors of D. Letting $d(D)$ be the number of divisors of D, there are $d(D)$ characters modulo D that are

not principal. Using the trivial bound $|S_D(a,b,\chi,\psi)| \leq |D|$ for those character sums, we get

$$N_D(a,b,x,y) \ll \eta^{\nu(D)} |D|^{\frac{1}{2}} + q^{x+y} |D|^{-1} d(D)^2 \ll |D|^{\frac{1}{2}+\epsilon} + q^{x+y} |D|^{-1+\epsilon}, \tag{5}$$

concluding the proof of Theorem 1.1.

3. Proof of Theorem 1.2

Let f and g be polynomials with coefficients in A, $\deg f = e_1$, and $\deg g = e_2$. We are interested in the number of squares of the form $f(X)+g(Y)$ with $\deg X \leq x$, $\deg Y \leq y$. We will be using Lilian Pierce's modification of the square sieve method, originally used by Hooley [5] and Heath-Brown [3]. Some intermediate results will require the following technical conditions on the degrees of f and g:

$$e_1 \text{ odd}; \quad (e_1, e_2) = 1; \quad e_2 < e_1 < p, e_2(e_1 - 1) < p.$$

Furthermore, we will be considering reductions of f and g modulo elements of A and will want their degrees to stay the same. Therefore, let D be the lcm of the leading coefficients of f and g, and let $d = \deg D$. Our results will concern the case where $y < d$ and $x < 2d$.

First, we quote the following lemma from Pierce [7, Lemma 2.1]; the proof in the function field case is identical to the number field case. The lemma is a modification of the square sieve, developed by Heath-Brown [3] to determine the number of squares in a sequence of integers using only information about the distribution of the integers with respect to a set of moduli. Instead of sieving over primes, we sieve over products of pairs of primes of different sizes. The original square sieve method does not give a sufficiently strong bound to improve on the trivial $h_3(D) \ll |D|^{\frac{1}{2}+\epsilon}$; this will be addressed later.

Lemma 3.1 (Modified square sieve)**.** *Let $\mathcal{U}, \mathcal{V}$ be disjoint sets of primes, $U = \#\mathcal{U}$, $V = \#\mathcal{V}$, and let $\mathcal{W} = \mathcal{U}\mathcal{V} = \{uv : u \in \mathcal{U}, v \in \mathcal{V}\}$, with $W = \#\mathcal{W}$. Let w be a weight function $A \to \mathbb{R}$ such that $\sum_{N \in A} w(N) < \infty$. If $w(N) = 0$ for $N = 0$ and for $|N| \gg \exp(\min(U,V))$ (that is, for $\deg N \gg \min(U,V)$), then*

$$\begin{aligned}\sum_N w(N^2) \ll & W^{-1} \sum_N w(N) + W^{-2} \sum_{\substack{F \neq G \in \mathcal{W} \\ (F,G)=1}} \left| \sum_N w(N) \left(\frac{N}{FG}\right) \right| \\ & + VW^{-2} \sum_{u \neq u' \in \mathcal{U}} \left| \sum_N w(N) \left(\frac{N}{uu'}\right) \right| + W^{-2} |E(\mathcal{U})| \\ & + UW^{-2} \sum_{v \neq v' \in \mathcal{V}} \left| \sum_N w(N) \left(\frac{N}{vv'}\right) \right| + W^{-2} |E(\mathcal{V})|.\end{aligned}$$

Here $\left(\frac{N}{M}\right)$ is the Jacobi symbol (defined over function fields as over number rings), and the error terms are defined by

$$E(\mathcal{U}) = \sum_{v \in \mathcal{V}} \sum_{u \neq u' \in \mathcal{U}} \sum_{\substack{N \\ v|N}} w(N) \left(\frac{N}{uu'}\right)$$

and similarly for $\mathcal{V}$.

The summation over $F \neq G \in W$ will be called the main sieve term; the sums over elements of U and of V are the prime sieve terms.

For our application, we will let

$$w(N) := \{X, Y \in A : f(X) + g(Y) = N, \deg X \leq x, \deg Y \leq y\}, \tag{6}$$

so that

$$\begin{aligned} N(f,g,x,y) &:= \#\{(X,Y,Z) : Z^2 = f(X) + g(Y), \deg X \leq x, \deg Y \leq y\} \\ &= \sum_{N \in A} w(N^2). \end{aligned}$$

We write $d = \deg D$. Fix an integer Q to be determined later; for the moment, we require only that $\log d < Q < d$. Let α and β be real numbers with $\alpha + \beta = 1$ such that αQ and βQ are integers. Define

$$\mathcal{U} = \{u \text{ irreducible} : u \nmid D, \deg u = \alpha Q\}, \quad \mathcal{V} = \{v \text{ irreducible} : v \nmid D, \deg v = \beta Q\}, \tag{7}$$

and let $\mathcal{W} = \mathcal{U}\mathcal{V}$, so that elements of W have degree Q. There are $\mathcal{O}(q^{\alpha Q}/\alpha Q)$ primes of degree αQ, of which $\leq d/(\alpha Q)$ divide D. Since $Q \gg \log d$, we have $U \gg q^{\alpha Q}/Q$. Similarly, $V \gg q^{\beta Q}/Q$, and therefore $W \gg q^Q/Q^2$. The condition that $u, v \nmid D$ is equivalent to the requirement that for $a \in \mathcal{W}$ the reductions of f and g modulo a have full degree.

The first term in the bound of the lemma is therefore bounded by

$$W^{-1} \sum_N w(N) \ll Q^2 q^{-Q+x+y}. \tag{8}$$

To evaluate the main and the prime sieve terms, we will be interested in estimating sums of the form

$$C(a,b) = \sum_N w(N) \left(\frac{N}{ab}\right) = \sum_{\substack{\deg X \leq x \\ \deg Y \leq y}} \left(\frac{f(X) + g(Y)}{ab}\right). \tag{9}$$

Our primary estimate for the size of such a sum will be the Weil bound [10, Chapter II], which generally states that the size of a character sum over a full residue set $\bmod M$ is $\mathcal{O}(\sqrt{M})$. Note that the character sum in $C(a,b)$ does not run over a full residue set $\bmod ab$. Expanding to a full character set will only give an improvement on the trivial bound if the number of terms in the sum is $\ll \sqrt{ab}$; this consideration will recur later.

The use of the modified square sieve will allow us to consider character sums over a smaller modulus and therefore to pass beyond the $\sqrt{ab}$ bound. This, ultimately, is what accounts for the improved exponent $27/56 < \frac{1}{2}$ in the last section.

In the main sieve term, we have $\deg ab = \deg FG = 2Q$. If we extend the sum over both X and Y to a complete residue set $\bmod FG$, the square root bound on the character sum will be of the form $|C(a,b)| \ll q^{Q(2+\epsilon)}$ (we have two variables running through a full residue set $\bmod FG$, and therefore the size of the sum is $\sqrt{|FG|}^2$). The main term is $q^{x+y-Q(1-\epsilon)}$, so the sieve term is smaller than the main term only if $3Q < x + y$. However, since our upper bound on Q is only $Q < d$ and we know $x + y < 3d$, we can do better than this.

Set Q so that $2Q \geq x > Q > y$. It makes sense to extend X to the full residue set modulo FG, since $|X| = q^x > q^Q = \sqrt{|FG|}$; it does not, however, make sense

to extend Y yet, since $|Y| < \sqrt{|FG|}$ and the trivial bound would be better than the one coming from the Weil method. Therefore, we rewrite:

$$\begin{aligned} C(F,G) &= \sum_{\substack{\deg X \le x \\ \deg Y \le y}} \left(\frac{f(X)+g(Y)}{FG}\right) \\ &= \sum_{\deg Y \le y} \sum_{L \bmod FG} \left(\frac{f(L)+g(Y)}{FG}\right) \sum_{\deg L \le x} 1 \\ &= \sum_{\deg Y \le y} \sum_{L \bmod FG} \left(\frac{f(L)+g(Y)}{FG}\right) \frac{q^x}{|FG|} \sum_{\psi = \psi(x)} \psi(L). \end{aligned}$$

Let

$$S(R;\psi,Y) = \sum_{L \bmod R} \left(\frac{f(L)+g(Y)}{R}\right) \psi(L)$$

and

$$\mathbf{S}(R;\psi,y) = \sum_{\deg Y \le y} S(R;\psi,Y),$$

so that

$$C(F,G) = \frac{q^x}{|FG|} \sum_{\psi=\psi(x)} \mathbf{S}(FG;\psi,y). \tag{10}$$

We are interested in nontrivial bounds on $|\mathbf{S}|$. Recall that $ab = FG$ for $F, G \in \mathcal{W}$ with $(F,G) = 1$. Write $FG = u_0u_1v_0v_1$ for $u_i \in \mathcal{U}$, $v_i \in \mathcal{V}$. Let $R_0 = u_0u_1$, $R_1 = v_0v_1$, so that $FG = R_0R_1$; in the main sieve, $u_0 \neq u_1$ and $v_0 \neq v_1$.

The sum S is multiplicative in the following sense: if $(R_0, R_1) = 1$, then

$$S(R_0R_1;\psi,Y) = S(R_0;\psi_0,Y)S(R_1;\psi_1,Y) \tag{11}$$

for some additive characters ψ_i modulo R_i. The calculation is similar to the one in Pierce [7, Lemma 3.1] and follows from the isomorphism $A/(R_0R_1) \cong A/(R_0) \times A/(R_1)$.

We now use the q-analogue of Van der Corput's method [2]. Let $h = y - \deg R_1$. For $\deg H \le h$ we have $\deg Y \le y \iff \deg(Y + HR_1) \le y$. Therefore, for $R = R_0R_1$ we have

$$\begin{aligned} q^h \mathbf{S}(R;\psi,y) &= \sum_{\deg Y \le y} \sum_{\deg H \le h} S(R_0;\psi_0,Y+HR_1)S(R_1;\psi_1,Y+HR_1) \\ &= \sum_{\deg Y \le y} S(R_1;\psi_1,Y) \sum_{\deg H \le h} S(R_0;\psi_0,Y+HR_1). \end{aligned}$$

By Cauchy's inequality we have

$$q^{2h} |\mathbf{S}(R;\psi,y)|^2 \le \sum\nolimits_1 \sum\nolimits_2, \tag{12}$$

where

(13)

$$\sum\nolimits_1 := \sum_{\deg Y \le y} |S(R_1;\psi_1,Y)|^2, \qquad \sum\nolimits_2 := \sum_{\deg Y \le y} \left| \sum_{\deg H \le h} S(R_0;\psi_0,Y+HR_1) \right|^2.$$

We rewrite the second sum as follows:

$$\sum\nolimits_2 = q^h \sum_{\deg Y \le y} \left| \sum_{\deg H \le h} S(R_0; \psi_0, Y + HR_1)\overline{S(R_0; \psi_0, Y)} \right| = \sum\nolimits_{2A} + \sum\nolimits_{2B},$$

where

$$\begin{aligned} \sum\nolimits_{2A} &:= q^h \sum_{\deg Y \le y} \left| S(R_0; \psi_0, Y) \right|^2, \\ \sum\nolimits_{2B} &:= q^h \sum_{\substack{\deg H \le h \\ H \ne 0}} \left| \sum_{\deg Y \le y} S(R_0; \psi_0, Y + HR_1)\overline{S(R_0; \psi_0, Y)} \right|. \end{aligned} \tag{14}$$

The sums $\sum_1$ and $\sum_{2A}$ will be easier to bound. In $\sum_{2B}$ we will be able to extend Y to a complete set of residues modulo R_0. This will be advantageous when $y \ge \frac{1}{2}\deg R_0 = \beta Q$, i.e., in the first case of the theorem.

First, we estimate $\sum_1$ and $\sum_{2A}$. By the multiplicativity of S, it suffices to work modulo a prime modulus P (recall that in our case $R_0 = u_0u_1$ for some $u_0 \ne u_1 \in \mathcal{U}$, and similarly for R_1). As a result of the technical restrictions on f, g, and $\mathcal{U}$, the polynomial $f(L)+g(Y)$ has odd degree when reduced modulo u_i, v_i, for any choice of L modulo FG. Therefore, when $\psi \ne \chi_0$ (the trivial character), we have the Weil bound [10, Theorem 2G]

$$|S(P; \psi, Y)| = \left| \sum_{L \bmod P} \left(\frac{f(L) + g(Y)}{P} \right) \psi(L) \right| \le (\deg f) q^{\frac{1}{2}\deg P} = e_1 |P|^{\frac{1}{2}}.$$

In the case of $\psi = \chi_0$ we have an even slightly better bound [10, Theorem 2E],

$$|S(P; \chi_0, Y)| = \left| \sum_{L \bmod P} \left(\frac{f(L) + g(Y)}{P} \right) \right| \le (e_1 - 1) |P|^{\frac{1}{2}},$$

so the bound $e_1 |P|^{1/2}$ is always valid. These bounds immediately give

Lemma 3.2.

$$\left| \sum\nolimits_1 \right| \ll q^y |R_1|, \qquad \left| \sum\nolimits_{2A} \right| \ll q^{h+y} |R_0|,$$

the implicit constants depending only on f and g.

To estimate $\sum_{2B}$, we write

$$\begin{aligned} T(R_0; H, y) &:= \sum_{\deg Y \le y} S(R_0; \psi_0, Y + HR_1)\overline{S(R_0; \psi_0, Y)} \\ &= \sum_{M \bmod R_0} S(R_0; \psi_0, M + HR_1)\overline{S(R_0; \chi_0, M)} \frac{q^y}{|R_0|} \sum_{\phi = \phi(y)} \phi(M). \end{aligned} \tag{15}$$

Expanding Y to the full residue set will be advantageous when $\deg R_0 = 2\beta Q \le 2y$ (i.e., $\beta Q \le y$), i.e., in the first case of Theorem 1.2.

Defining

(16)
$$\mathcal{T}(R_0; H, \psi_0, \phi) := \sum_{M \bmod R_0} S(R_0; \psi_0, M + HR_1)\overline{S(R_0; \psi_0, M)}\phi(M)$$
$$= \sum_{K,L,M \bmod R_0} \left(\frac{f(K) + g(M + HR_1)}{R_0}\right)\left(\frac{f(L) + g(M)}{R_0}\right)\psi_0(K - L)\phi(M),$$

we see that $\mathcal{T}$ is multiplicative in the modulus R_0. In particular, for $R_0 = u_0u_1$ with $(u_0, u_1) = 1$ we have

$$\mathcal{T}(R_0; H, \psi_0, \phi) = \mathcal{T}(u_0; H, \psi_{0u_0}, \phi_{u_0})\mathcal{T}(u_1; H, \psi_{0u_1}, \phi_{u_1})$$

for some additive characters ψ_{0u_i}, ϕ_{u_i} modulo u_i.

To bound a sum of the form $\mathcal{T}(P; H, \psi, \phi)$, where ϕ, ψ are additive characters modulo P, we use the result of Katz [6] on exponential sums in several variables. If $\psi \neq \chi_0$, we can write $\phi = \psi \circ \alpha$ where α is multiplication by some element of $A/(P)$ (since $A/(P)$ is a field). In that case,

$$|\mathcal{T}(P; H, \psi, \phi)| \leq 2e_1e_2(e_1 - 1)\,|P|^{\frac{3}{2}}$$

when either ϕ is nontrivial (i.e., $\alpha \neq 0$) or $HR_1 \neq 0 \bmod P$ (cases (1) and (2) of [6, Theorem 1.3]). Moreover, if ψ is trivial but ϕ is not, expressing ψ in terms of ϕ gives the same estimate (case (3) of [6, Theorem 1.3]), since $e_1 = \deg f$ is odd.

In the exceptional case we have $\psi = \phi = \chi_0$ and $P \mid HR_1$. Since we started out with disjoint set of primes U, V, we will be concerned only with primes $P \nmid R_1$. Therefore, the condition $P \mid HR_1$ is equivalent to $P \mid H$. Then,

$$\mathcal{T}(P; H, \chi_0, \chi_0) = \sum_{M \bmod P} \sum_{K \bmod P} \left(\frac{f(K)+g(M+HR_1)}{P}\right) \sum_{L \bmod P} \left(\frac{f(L)+g(M)}{P}\right).$$

By the Weil bound for the inner sums, the sum is bounded by $e_1^2\,|P|^2$.

Therefore, uniformly

$$|\mathcal{T}(P; H, \psi, \phi)| \leq \max(e_1^2, 2e_1e_2(e_1 - 1))\,|P|^{\frac{3}{2}}\,|(P, H)|^{\frac{1}{2}}.$$

From this, using the multiplicativity of $\mathcal{T}$ and (14), (15), (16), we derive the bound

Lemma 3.3.

$$\left|\sum\nolimits_{2B}\right| \ll q^h\,|R_0|^{\frac{3}{2}} \sum_{\deg H \leq h} |(R_0, H)|^{\frac{1}{2}} \ll q^{2h}\,|R_0|^{\frac{3}{2}}\,d(R_0),$$

where $d(R_0)$ is the number of divisors of R_0 (equal to 4 in our case).

Using (12), Lemma 3.2, Lemma 3.3, and recalling that $h = y - \deg R_1$, we obtain

(17)
$$|\mathbf{S}(R; \psi, y)|^2 \ll q^{-2h}\,(q^y\,|R_1|)\left(q^{h+y}\,|R_0| + q^{2h}\,|R_0|^{\frac{3}{2}}\right) \ll q^{y+2Q}\left(|R_1| + |R_0|^{\frac{1}{2}}\right).$$

Using (10), the main sieve term is bounded by

$$|C(F, G)| \ll q^{y/2+Q}\left(|R_1|^{\frac{1}{2}} + |R_0|^{\frac{1}{4}}\right).$$

Recalling that $\deg R_0 + \deg R_1 = 2Q$, we see that to equalize the contributions of the two error terms we need to set $\deg R_0 = \frac{4}{3}Q$ and $\deg R_1 = \frac{2}{3}Q$, i.e., $\alpha = \frac{2}{3}$ and $\beta = \frac{1}{3}$. The main sieve term then becomes

$$|C(F,G)| \ll q^{\frac{1}{2}y+\frac{4}{3}Q}, \tag{18}$$

which is better than the trivial bound q^{2Q} since we assumed $y < Q$.

We move on to the contributions of the prime sieves. The computations will be identical for $\mathcal{U}$ and $\mathcal{V}$, so for brevity we consider only $\mathcal{U}$. We will be interested in $C(u,u')$ for $u \neq u' \in \mathcal{U}$.

Set $h_{\mathcal{U}} = y - \deg u$ for $u \in \mathcal{U}$; then analogously to (12) we have

$$q^{2h_{\mathcal{U}}} |\mathbf{S}(uu', \psi, y)|^2 \ll \sum\nolimits_1 \left(\sum\nolimits_{2A} + \sum\nolimits_{2B} \right),$$

where

$$\begin{aligned}
\sum\nolimits_1 &= \sum_{\deg Y \leq y} |S(u'; \psi_{u'}, Y)|^2, \\
\sum\nolimits_{2A} &= q^{h_{\mathcal{U}}} \sum_{\deg Y \leq y} |S(u; \psi_u, Y)|^2, \\
\sum\nolimits_{2B} &= q^{h_{\mathcal{U}}} \sum_{\substack{\deg H \leq h_{\mathcal{U}} \\ H \neq 0}} \left| \sum_{\deg Y \leq y} S(u; \psi_u, Y + Hu) \overline{S(u; \psi_u, Y)} \right|.
\end{aligned}$$

Analogous to the case of the main sieve,

$$\begin{aligned}
&\sum\nolimits_1 \ll q^y |u'|, \qquad \sum\nolimits_{2A} \ll q^{h_{\mathcal{U}}+y} |u|, \\
&\sum\nolimits_{2B} \ll q^{h_{\mathcal{U}}} |u|^{\frac{3}{2}} \sum_{\deg H \leq h_{\mathcal{U}}} |(u,H)|^{\frac{1}{2}} \ll q^{2h_{\mathcal{U}}} |u|^{\frac{3}{2}}.
\end{aligned} \tag{19}$$

Recalling that $|u| = |u'|$, the prime sieves satisfy

$$|C(u,u')| \ll q^{y/2} |u|^{\frac{3}{2}}, \qquad |C(v,v')| \ll q^{y/2} |v|^{\frac{3}{2}}. \tag{20}$$

Since $|u| = q^{\alpha Q} = q^{\frac{2}{3}Q}$ and $|v| = q^{\beta Q} = q^{\frac{1}{3}Q}$, the prime sieve terms are smaller than the main sieve term.

Finally, we estimate $|E(\mathcal{U})|$ and $|E(\mathcal{V})|$. Again, we go through the calculations only for $E(\mathcal{U})$. Rewrite

$$E(\mathcal{U}) = \sum_{u \neq u' \in \mathcal{U}} \sum_{v \in \mathcal{V}} \sum_{\deg Y \leq y} \sum_{\substack{\deg X \leq x \\ f(X) \equiv -g(Y) \bmod v}} \left(\frac{f(X) + g(Y)}{uu'} \right). \tag{21}$$

Since v is prime, given Y there are $\leq e_1$ values of $X \bmod v$ that satisfy the criterion of the inner sum. For these values X_0, write $X = X_0 + vF$ with $\deg F \leq x - \deg v = k$, and write

$$E(\mathcal{U}) = \sum_{u \neq u' \in \mathcal{U}} \sum_{v \in \mathcal{V}} \sum_{\deg Y \leq y} \sum_{X_0 \bmod v} \sum_{\deg F \leq k} \left(\frac{f(X_0 + vF) + g(Y)}{uu'} \right).$$

Let

$$D(uu', v, X_0, Y, k) := \sum_{\deg F \leq k} \left(\frac{f(X_0 + vF) + g(Y)}{uu'} \right), \tag{22}$$

so that $|E(\mathcal{U})| \le U^2 V q^y \max_{u,u',v,X_0,Y,k} |D|$.

There are now two cases to consider: $k < \deg uu'$ and $k \ge \deg uu'$ (the latter is possible, since $k = x - \deg v$ is only bounded from above by $\frac{5}{3}Q$, while $\deg uu' = \frac{4}{3}Q$). We handle the case $k < \deg uu'$ first. Expanding the sum D to a complete sum modulo uu' and using the Weil bound for the resulting sum, we see that $|D| \ll |u|$, from which the error term is bounded by

$$W^{-2}|E(\mathcal{U})| \ll Q^4 q^{y+(3\alpha+\beta-2)Q} = Q^4 q^{y+\frac{1}{3}Q}$$

and

$$W^{-2}|E(\mathcal{V})| \ll Q^4 q^{y+(3\beta+\alpha-2)Q} = Q^4 q^{y-\frac{1}{3}Q}.$$

Since $y < Q$, this is smaller than the main sieve term.

If $k \ge \deg uu'$, then F runs through a full residue set modulo uu', and it does so $q^k/|uu'|$ times. Applying the Weil bound, we obtain

$$|D| \ll \frac{q^k}{|uu'|} q^{1/2 \deg u} q^{1/2 \deg u'} \ll q^{\frac{5}{3}Q - \frac{2}{3}Q} = q^Q,$$

from which the error term is bounded by

$$W^{-2}|E(\mathcal{U})| \ll Q^4 q^{y+(2\alpha+\beta-1)Q} = Q^4 q^{y+\frac{2}{3}Q},$$

which is also smaller than the main sieve term. In the corresponding estimates for $\mathcal{V}$, recall $\deg vv' \le \frac{2}{3}Q$. Then $k = x - \deg u \le \frac{4}{3}Q$,

$$|D| \ll \frac{q^k}{|vv'|} q^{\frac{1}{2}\deg v} q^{\frac{1}{2}\deg v'} \ll q^{\frac{4}{3}Q - \frac{1}{3}Q} = q^Q$$

and

$$W^{-2}|E(\mathcal{V})| \ll Q^4 q^{y+(2\beta+\alpha-1)Q} = Q^4 q^{y+\frac{1}{3}Q},$$

which is again smaller than the main sieve term.

We are ready to put the bounds together. As we showed, the prime sieve terms as well as the error terms are dominated by the main sieve term. Therefore, as a result of (8) and (18) we have

$$N(f,g,x,y) \ll Q^2 q^{-Q+x+y} + q^{\frac{1}{2}y+\frac{4}{3}Q}. \tag{23}$$

Equating the contributions of the two terms, we see that for the optimal bound we must set

$$Q = \frac{3}{7}\left(x + \frac{1}{2}y\right).$$

However, in order for us to attain $2Q > x$, we need to bound y from below: $y \ge \frac{1}{3}x$. (This is also the condition at which we arrive simply by requiring the error terms above to be smaller than the main sieve term, with Q optimal and no prior assumptions about y except $y \ge 0$.)

If the condition $y \ge \frac{1}{3}x$ is satisfied, we derive

$$N(f,g,x,y) \ll q^{\frac{4}{7}x+\frac{11}{14}y+\epsilon x}.$$

Otherwise, we set $Q = \frac{1}{2}x$, in which case the second term in (23) dominates and we derive only

$$N(f,g,x,y) \ll q^{\frac{1}{2}y+\frac{2}{3}x+\epsilon x}.$$

This concludes the proof of Theorem 1.2.

4. Corollaries on the 3-torsion

Here we derive bounds on the 3-torsion of the ideal class groups of imaginary quadratic extensions of function fields as corollaries of the above theorems. A field extension L/K will be called (purely) imaginary if the infinite valuation $v(f) = -\deg f$ is totally ramified in the extension. For a polynomial D, $L = K(\sqrt{D})$ is an imaginary quadratic extension when $\deg D = 2n+1$ is odd. We will concern ourselves only with D square-free. Given an ideal $\mathfrak{a}$ we will let the norm $N(\mathfrak{a})$ be the unique monic generator of the ideal $\{N(F)|F \in \mathfrak{a}\}$ (as an ideal of A, this is principal). It is easily verified that this norm is multiplicative and, moreover, the degree valuation on L coincides with taking the K-degree of the norm.

Let D be square-free of degree $2n+1$. The analog of the Minkowski bound for function fields asserts that every ideal class in $Cl(D)$ has a representative whose norm has degree $\leq n$. Let $\mathfrak{b}$ be the minimal representative for an ideal class of order 3; then equating the norms we obtain $N(\mathfrak{b})^3 = N((a))^2$ for some fractional ideal $(a) = (A + B\sqrt{D})$. Now, the norm of (a) is $A^2 - DB^2$. Note that here $\deg A^2$ is even and $\deg DB^2$ is odd, so no cancellation can occur, and we can bound the degrees of A and B as follows:

$$N(\mathfrak{b})^3 = A^2 - DB^2, \quad \deg N \leq n,\ \deg A \leq \frac{3n}{2},\ \deg B \leq \frac{n}{2}. \tag{24}$$

To every solution of this equation there correspond $\ll D^\epsilon$ ideal classes $[\mathfrak{b}]$, so it suffices to bound the number of solutions to this equation.

Theorem 4.1. *Let $p > 3$, and let D be a square-free discriminant of an imaginary field extension of function fields,* $\deg D = 2n+1$. *Let D_0 be a divisor of D of degree d_0. The following are true:*

$$h_3(D) \ll q^{\frac{d_0}{2}+d_0\epsilon} + q^{\frac{5n}{2}-d_0+d_0\epsilon}. \tag{25}$$

In particular, if $d_0 = \frac{5n}{3}$, then we obtain $h_3(D) \ll |D|^{\frac{5}{6}+\epsilon}$. Unconditionally,

$$h_3(D) \ll q^{27/28n+\epsilon n} = |D|^{27/56+\epsilon}. \tag{26}$$

Proof. The first result is a corollary of Theorem 1.1. We have $\deg D = 2n+1$, $x = n$, $y = \frac{3n}{2}$. For every divisor D_0 of D we have the congruence $N^3 \equiv A^2 \bmod D_0$, and for $\deg D_0 = d_0 > \frac{3n}{2}$ we can apply Theorem 1.1 to obtain

$$h_3(D) \ll q^{\frac{d_0}{2}+d_0\epsilon} + q^{\frac{5n}{2}-d_0+d_0\epsilon}.$$

This is an improvement on the trivial bound for $d_0 > \frac{3n}{2}$. The improvement is maximal when $d_0 = \frac{5n}{3}$, in which case we derive the bound $h_3(D) \ll |D|^{5/6+\epsilon}$.

If we instead apply the results of Theorem 1.2 with $f(X) = X^3$, $g(Y) = DY^2$, $D = D$, $d = 2n+1$, and $x = n, y = \frac{1}{2}n$, we derive the unconditional bound

$$h_3(D) \ll q^{(27/28)n+\epsilon n} = |D|^{27/56+\epsilon}.$$

□

Over function fields these results fall short of the known bound $h_3(D) \ll |D|^{\frac{1}{3}+\epsilon}$ ([1], [4]).

References

[1] J. Ellenberg and A. Venkatesh, Reflection principles and bounds for class group torsion. *Int. Math. Res. Not. IMRN* 2007, no. 1, Art. ID #rnm002. MR2331900

[2] D. R. Heath-Brown, Hybrid bounds for L-functions: a q-analogue of Van der Corput's method and a t-analogue of Burgess's method. *Recent Progress in Analytic Number Theory*, eds. Halberstam and Hooley. Academic Press, London (1981), pp. 121-126.

[3] D. R. Heath-Brown, The least square-free number in an arithmetic progression. *J. Reine Angew. Math.* 332 (1982) 204-220. MR656864 (83i:10057)

[4] H. Helfgott and A. Venkatesh, Integral points on elliptic curves and 3-torsion in class groups. *J. Amer. Math. Soc.* 19, no. 3 (2005) 527-550. MR2220098 (2007b:11081)

[5] C. Hooley, A note on square-free numbers in arithmetic progressions. *Bull. London Math. Soc. 7* (1975) 133-138. MR0371799 (51:8016)

[6] N. M. Katz, On a question of Lillian Pierce. *Forum Math.* 18 (2006) 699-710. MR2254391

[7] L. B. Pierce, A bound for the 3-part of class numbers of quadratic fields by means of the square sieve. *Forum Math.* 18 (2006) 677-698. MR2254390

[8] L. B. Pierce, The 3-part of class numbers of quadratic fields. *J. London Math. Soc.* (2) 71 (2005) 579-598. MR2132372 (2006e:11167)

[9] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics, 210, Springer, Berlin (2000). MR1876657 (2003d:11171)

[10] W. Schmidt, *Equations over finite fields: an elementary approach*, Lecture Notes in Mathematics, 536, Springer, Berlin (1976). MR0429733 (55:2744)

Department of Mathematics, FAS, Harvard University, One Oxford Street, Cambridge, Massachusetts 02138