Proceedings of the Edinburgh Mathematical Society (2009) **52**, 719–729 ©
DOI:10.1017/S001309150700123X Printed in the United Kingdom

ON QUADRATIC FIELDS GENERATED BY THE SHANKS SEQUENCE

FLORIAN LUCA[1] AND IGOR E. SHPARLINSKI[2]

[1] *Instituto de Matemáticas, Universidad Nacional Autonoma de México,*
CP 58089, Morelia, Michoacán, Mexico (fluca@matmor.unam.mx)
[2] *Department of Computing, Macquarie University,*
Sydney, NSW 2109, Australia (igor@ics.mq.edu.au)

(Received 12 October 2007)

Abstract Let $u(n) = f(g^n)$, where $g > 1$ is integer and $f(X) \in \mathbb{Z}[X]$ is non-constant and has no multiple roots. We use the theory of $\mathcal{S}$-unit equations as well as bounds for character sums to obtain a lower bound on the number of distinct fields among $\mathbb{Q}(\sqrt{u(n)})$ for $n \in \{M+1,\dots,M+N\}$. Fields of this type include the Shanks fields and their generalizations.

Keywords: quadratic fields; $\mathcal{S}$-unit equations; square sieve; character sums

2000 *Mathematics subject classification:* Primary 11D45; 11L40; 11N36; 11R11

1. Introduction

Given some fixed integer $g > 1$ and a non-constant polynomial $f(X) \in \mathbb{Z}[X]$ without multiple roots, we consider the sequence $u(n) = f(g^n)$, $n = 1, 2, \dots$. It is clear that $u(n)$ has constant sign for large n. Thus, up to replacing $f(X)$ by $-f(X)$ and discarding a few initial terms, we may assume that $u(n) > 0$ for every n.

Given a square-free integer $s \geqslant 1$ and two arbitrary integers $M \geqslant 0$ and $N \geqslant 1$, we denote by $Q_u(s; M, N)$ the number of $n \in \{M+1,\dots,M+N\}$ for which $\mathbb{Q}(\sqrt{u(n)}) = \mathbb{Q}(\sqrt{s})$. If $f(0) = 0$, then by setting $h(X) = f(X)/X$ and $v(n) = h(g^n)$ we see easily that $\mathbb{Q}(\sqrt{u(n)})$ equals $\mathbb{Q}(\sqrt{v(n)})$ or $\mathbb{Q}(\sqrt{gv(n)})$ according to whether n is even or odd. Thus, without loss of generality, we can assume that $f(0) \neq 0$.

We note that the Shanks family of quadratic fields [**14**] corresponds to the sequence

$$u(n) = (2^n + 3)^2 - 8.$$

For various generalizations of this family, which are all of the form $f(g^n)$ with a polynomial $f(X) \in \mathbb{Z}[X]$, see [**13**, **15**, **16**] and references therein. Despite the quite extensive study of these fields, very little seems to be known about their discriminants.

Here, we use the theory of $\mathcal{S}$-unit equations as well as bounds on character sums to obtain non-trivial upper bounds on $Q_u(s; M, N)$. We also write

$$Q_u(s) = \lim_{N\to\infty} Q_u(s; 0, N) = \#\{n \geqslant 1 : \mathbb{Q}(\sqrt{u(n)}) = \mathbb{Q}(\sqrt{s})\}.$$

https://doi.org/10.1017/S001309150700123X Published online by Cambridge University Press

It follows easily from [**4**, Theorem 2] that $Q_u(s)$ is finite for every square-free number s. In this paper, we are interested in finding bounds on $Q_u(s)$ and $Q_u(s; M, N)$ which are independent of s.

In what follows, the implied constants in 'O', '$\ll$' and '$\gg$' may depend on the sequence u as well as on other parameters, such as α. We recall that $A = O(B)$, $A \ll B$ and $A \gg B$ are equivalent to the inequality $|A| \leqslant cB$ with some constant $c > 0$. For a positive number x we write $\log x$ for the maximum between the natural logarithm of x and 1. Thus, we always have $\log x \geqslant 1$.

In the case when $f(X)$ has degree 1 or 2, our result is very satisfying.

Theorem 1.1. *If $f(X) \in \mathbb{Z}[X]$ is a polynomial of degree $\deg f \leqslant 2$ with $f(0) \neq 0$ having only simple roots, then*

$$\limsup_{s\to\infty} Q_u(s) < \infty.$$

The proof of Theorem 1.1 uses results about $\mathcal{S}$-unit equations. We suspect that the conclusion of Theorem 1.1 remains true even for polynomials $f(X)$ of degree 3 or more. When the degree of $f(X)$ is at least 5, then every solution of the equation $u(n) = sy^2$ in integers $n \geqslant 1$ and y leads to an integer solution $(X, Y) = (g^n, y)$ of the equation $f(X) = sY^2$. Since $f(X)$ has no multiple roots, the latter equation represents an irreducible curve of genus $g > 1$. The uniformity conjecture from [**3**] implies that the number of such solutions is bounded by some number depending only on the degree of $f(X)$, so, in particular, it is independent not only of s but even of the polynomial $f(X)$. Then the case when $f(X)$ is of degree 3 or 4 can be reduced to the case of a polynomial of a larger degree by the following procedure. Let $k \geqslant 2$ be an integer. For $i = 0, \dots, k-1$, set $h_i(X) = f(g^i X^k)$. Then $h_i(X)$ is a polynomial of degree $k \deg f > \deg f$ and has only simple roots because $f(0) \neq 0$. Furthermore, $f(g^n) = h_i(g^{\lfloor n/k \rfloor})$, where $i = n - k\lfloor n/k \rfloor$. Now the uniformity conjecture applies again. So, we have the following conjecture.

Conjecture 1.2. *For any polynomial $f(X) \in \mathbb{Z}[X]$ with $f(0) \neq 0$ having only simple roots we have*

$$\limsup_{s\to\infty} Q_u(s) < \infty.$$

Our unconditional result when $\deg f \geqslant 3$ is substantially weaker and depends on our knowledge of the prime divisors of shifted primes. More precisely, let $\alpha > \frac{1}{2}$ be any real number such that the inequality

$$\#\{\ell \leqslant z : \ell \text{ prime and } P(\ell - 1) \geqslant \ell^\alpha\} \gg \frac{z}{\log z}$$

holds, where the implied constant might depend on α and $P(k)$ stands for the largest prime divisor of k.

By the work of Baker and Harman [**1**], it is known that we can take

$$\alpha = 0.677. \tag{1.1}$$

It is conjectured that α can be taken to be $1 - \varepsilon$ for any $\varepsilon > 0$. In particular, this holds under the extended Riemann hypothesis (see [**7, 12**]).

Using the square sieve of Heath-Brown [**9**], we obtain the following estimate.

https://doi.org/10.1017/S001309150700123X Published online by Cambridge University Press

Theorem 1.3. *Let $u(n) = f(g^n)$, where $f(X) \in \mathbb{Z}[X]$ is a fixed polynomial of degree $\deg f \geqslant 3$ with $f(0) \neq 0$ having only simple roots. Then uniformly for square-free integers $s \geqslant 1$ and arbitrary integers $M \geqslant 0$ and $N \geqslant 2$, we have*

$$Q_u(s; M, N) \ll N^{\vartheta}(\log N)^{\rho},$$

where

$$\vartheta = \frac{3}{2(1+\alpha)} \quad \textit{and} \quad \rho = \frac{4+\alpha}{1+\alpha}.$$

Let $R_u(M, N)$ be the number of distinct fields among $\mathbb{Q}(\sqrt{u(n)})$, when $n \in \{M+1, \dots, M+N\}$. Theorems 1.1 and 1.3 immediately give the lower bound

$$R_u(M, N) \gg \begin{cases} N & \text{if } \deg f \leqslant 2, \\ N^{1-\vartheta}(\log N)^{-\rho} & \text{if } \deg f \geqslant 3, \end{cases}$$

which is uniform in M.

Taking α as in (1.1) we get

$$\vartheta \leqslant 0.895,$$

while assuming the extended Riemann hypothesis and taking $\alpha = 1 + o(1)$ gives

$$\vartheta = 0.75 + o(1) \quad \text{as } N \to \infty.$$

We remark that Cutter *et al.* [**5**] have obtained an asymptotic formula for the number of distinct fields among $\mathbb{Q}(\sqrt{f(n)})$, for $n = 1, \dots, N$, with a given polynomial $f(X) \in \mathbb{Z}[X]$ of degree at most 2. They also have an asymptotic formula when the polynomial $f(X)$ is of degree 3 and higher, but their proof in this case is conditional upon the *abc* conjecture.

2. $\mathcal{S}$-unit equations

For the proof of Theorem 1.1, we need the following result on the finiteness of the number of non-degenerate solutions of $\mathcal{S}$-unit equations due to Evertse *et al.* [**8**].

Given non-zero complex numbers $A_1, \dots, A_N$, we consider the equation

$$\sum_{i=1}^{N} A_i x_i = 1 \tag{2.1}$$

in unknowns $\boldsymbol{x} = (x_1, \dots, x_N) \in \Gamma$. We say that a solution is *non-degenerate* if

$$\sum_{i \in I} A_i x_i \neq 0 \quad \text{for all non-empty sets } I \subset \{1, \dots, N\}. \tag{2.2}$$

Lemma 2.1. *Let $N \geqslant 1$ and Γ be a finitely generated subgroup of $(\mathbb{C}^*)^N$ of rank r. Given the non-zero complex numbers $A_1, \dots, A_N$, equation (2.1) has at most $\exp((6N)^{3N}(r+1))$ non-degenerate solutions.*

We note that in the case of $N = 2$ (which appears in the case of linear polynomials in the proof of Theorem 1.1), one can use a stronger bound of Beukers and Schlickewei [**2**], which leads to numerically stronger estimates.

https://doi.org/10.1017/S001309150700123X Published online by Cambridge University Press

3. Proof of Theorem 1.1

We first consider the case when $f(X) = aX + b$ with $b \neq 0$ is linear. Since, as we have remarked, it follows from [**4**, Theorem 2] that $Q_u(s)$ is finite for every square-free integer s, it follows that we may assume that

$$\mathbb{Q}(\sqrt{s}) \neq \mathbb{Q}, \mathbb{Q}(\sqrt{a}), \mathbb{Q}(\sqrt{ag}).$$

We further assume that n is even, since the case of odd n can be dealt with similarly. If $\mathbb{Q}(\sqrt{u(n)}) = \mathbb{Q}(\sqrt{s})$, then $u(n) = sy^2$ holds with some integer y. Thus,

$$(a^{1/2}g^{n/2} - s^{1/2}y)(a^{1/2}g^{n/2} + s^{1/2}) = -b. \tag{3.1}$$

Let $\mathbb{K} = \mathbb{Q}[\sqrt{a}, \sqrt{s}]$ and let $\mathcal{O}_{\mathbb{K}}$ be its ring of integers. Note that for $d = [\mathbb{K} : \mathbb{Q}]$ we have $d = 2$ or $d = 4$ according to whether or not a is a square. The relation (3.1) shows that $(a^{1/2}g^{n/2} - s^{1/2}y)\mathcal{O}_{\mathbb{K}}$ is a principal ideal divisor of b. Since $d \leqslant 4$, each prime divisor of b has at most four prime ideal divisors. Therefore, the number of principal ideal divisors of b does not exceed $\tau(b)^4$, where $\tau(b)$ is the number of integer positive divisors of b. Let t be the number of such ideals and let $\beta_1, \dots, \beta_t \in \mathcal{O}_{\mathbb{K}}$ be generators of these ideals. Thus,

$$a^{1/2}g^{n/2} - s^{1/2}y = \beta_i\zeta$$

holds for some $i = 1, \dots, t$ and some unit ζ in $\mathcal{O}_{\mathbb{K}}$. Conjugating the above relation by an element of the Galois group of $\mathbb{K}/\mathbb{Q}$ which leaves $a^{1/2}$ invariant but maps $s^{1/2}$ to $-s^{1/2}$ (which exists because of our hypothesis on s), we also get that

$$a^{1/2}g^{n/2} + s^{1/2}y = \beta_i'\zeta',$$

where β_i' and ζ' are conjugates of β_i and ζ, respectively. Summing up the two relations we arrive at

$$2a^{1/2}g^{n/2} = \beta_i\zeta + \beta_i'\zeta'.$$

The above equation can be rewritten as

$$A_1X_1 + A_2X_2 = 1,$$

where $A_1 = \beta_i(2a^{1/2})^{-1},\ A_2 = \beta_i'(2a^{1/2})^{-1}$, $X_1 = \zeta g^{-n/2}$ and $X_2 = \zeta' g^{-n/2}$. This is an equation of the form (2.1) whose solutions (X_1, X_2) obviously satisfy the non-degeneracy condition (2.2). The indeterminates (X_1, X_2) belong to a subgroup of $(\mathbb{C}^*)^2$ of rank at most $2(1+3) = 8$ because the unit group of $\mathcal{O}_{\mathbb{K}}$ has rank at most 3. Thus, by Lemma 2.1, there are at most $\exp(12^6 \cdot 9)$ solutions (we note that in the case of equations with only three units we can get a better numerical bound by using the estimate of [**2**]). Let us now see that every solution determines n uniquely. Indeed, if X_1 is known and $X_1 = \zeta g^{n/2}$, then by computing norms over $\mathbb{Q}$ we get

$$N_{\mathbb{K}/\mathbb{Q}}(X_1) = N_{\mathbb{K}/Q}(\zeta)N_{\mathbb{K}/Q}(g^{n/2}) = g^{dn/2}.$$

https://doi.org/10.1017/S001309150700123X Published online by Cambridge University Press

Thus, n is uniquely determined by X_1. Therefore, the number of possibilities for n even is at most $\tau(b)^4 \exp(12^6 \cdot 9) = O(1)$, which completes the proof for the case of the linear polynomial $f(X)$.

When $f(X) = aX^2 + bX + c$ is quadratic, we replace $f(X)$ by $af(X) = (aX+b)^2 - \Delta$, where $\Delta = b^2 - 4ac \neq 0$. Let $v(n) = ag^n + b$. Assuming that $s \neq 1$, the relation $\mathbb{Q}(\sqrt{u(n)}) = \mathbb{Q}(\sqrt{s})$ leads again to a solution (n, y) with positive integers n and y of the equation $u(n) = sy^2$. We rewrite this as

$$v(n)^2 - sy^2 = \Delta,$$

and then further as

$$(v(n) - s^{1/2}y)(v(n) + s^{1/2}y) = \Delta.$$

Writing $\mathbb{K} = \mathbb{Q}(\sqrt{s})$, the previous argument leads to a relation of the type

$$v(n) = \Delta_i \zeta + \Delta_i' \zeta',$$

for some $i = 1, \dots, t$ and $\zeta \in \mathcal{O}_{\mathbb{K}}^*$, where now $\Delta_1, \dots, \Delta_t$ are generators of all the possible principal ideal divisors of Δ in $\mathcal{O}_{\mathbb{K}}$. Note that $t \leqslant \tau(\Delta)^2$. The above relation leads now to the equation

$$A_1X_1 + A_2X_2 + A_3X_3 = 1, \tag{3.2}$$

where $A_1 = -(a/b)$, $A_2 = \Delta_i/b$, $A_3 = \Delta_i'/b$ and $X_1 = g^n$, $X_2 = \zeta$, $X_3 = \zeta'$. Therefore, (X_1, X_2, X_3) is in a subgroup of $(\mathbb{C}^*)^3$ of rank at most $3(1+1) = 6$. If $A_1X_1 = 1$, then n is uniquely determined. If $A_2X_2 = 1$, then ζ is uniquely determined, and therefore so is ζ'. Thus, $v(n) = \Delta_i\zeta + \Delta_i'\zeta'$ is uniquely determined; therefore, n is uniquely determined. The same argument applies when $A_3X_3 = 1$. All other solutions to equation (3.2) are non-degenerate. It follows from Lemma 2.1 that there are at most $\exp(18^9 \cdot 7)$ such solutions (X_1, X_2, X_3). It is clear that X_1 determines n. This completes the proof when $f(X)$ is quadratic and thus completes the proof of the whole theorem.

4. Character sums

For the proof of Theorem 1.3, we need some bounds for character sums. For an odd integer m, we use (k/m) to denote, as usual, the Jacobi symbol of k modulo m. For an integer m coprime to g we write t_m for the multiplicative order of g modulo m.

The following result generalizes those of [**6**,**17**], which apply only to linear polynomials. In turn, it can also be extended in various directions. However, we choose to present it in the simple special case which is needed for the purpose of this paper.

Lemma 4.1. *Let $f(X) \in \mathbb{Z}[X]$ be a fixed polynomial of degree $\deg f \geqslant 2$ without multiple roots. For any primes $\ell \neq p$ such that $t_\ell > \ell^{1/2}$ and $t_p > p^{1/2}$, we have*

$$\sum_{n=M+1}^{M+N} \left(\frac{f(g^n)}{\ell p}\right) \ll \left(\frac{N}{t_{\ell p}} + 1\right) t_{\ell p}^{1/2} (\ell p)^{1/4} \log(\ell p).$$

https://doi.org/10.1017/S001309150700123X Published online by Cambridge University Press

Proof. We assume that ℓ and p are large enough, since otherwise the bound is trivial.

According to the general principle of reducing incomplete sums to complete ones, it is enough to prove that, uniformly over all integers k, we have

$$\sum_{n=1}^{t_{\ell p}} \left(\frac{f(g^n)}{\ell p}\right) \boldsymbol{e}\left(\frac{kn}{\ell p}\right) \ll t_{\ell p}^{1/2} (\ell p)^{1/4}, \tag{4.1}$$

where for a complex number z we set, as usual, $\boldsymbol{e}(z) = \exp(2\pi \mathrm{i} z)$ (see, for example, [**10**, § 12.2]).

We can now assume that

$$t_{\ell p} \geqslant (\ell p)^{1/2}, \tag{4.2}$$

since otherwise the bound is trivial.

Using the periodicity property of g^n, we may write

$$\begin{aligned}\sum_{n=1}^{t_{\ell p}} \left(\frac{f(g^n)}{\ell p}\right) \boldsymbol{e}\left(\frac{kn}{\ell p}\right) &= \frac{1}{t_{\ell p}} \sum_{m=1}^{t_{\ell p}} \sum_{n=1}^{t_{\ell p}} \left(\frac{f(g^{n+m})}{\ell p}\right) \boldsymbol{e}\left(\frac{k(n+m)}{\ell p}\right) \\ &= \frac{1}{t_{\ell p}} \sum_{m=1}^{t_{\ell p}} \boldsymbol{e}\left(\frac{km}{\ell p}\right) \sum_{n=1}^{t_{\ell p}} \left(\frac{f(g^{n+m})}{\ell p}\right) \boldsymbol{e}\left(\frac{kn}{\ell p}\right).\end{aligned}$$

Therefore,

$$\left|\sum_{n=1}^{t_{\ell p}} \left(\frac{f(g^n)}{\ell p}\right) \boldsymbol{e}\left(\frac{kn}{\ell p}\right)\right| \leqslant \frac{1}{t_{\ell p}} \sum_{m=1}^{t_{\ell p}} \left|\sum_{n=1}^{t_{\ell p}} \left(\frac{f(g^m g^n)}{\ell p}\right) \boldsymbol{e}\left(\frac{kn}{\ell p}\right)\right|. \tag{4.3}$$

Now, using the Cauchy inequality, we derive

$$\begin{aligned}\left(\sum_{m=1}^{t_{\ell p}} \left|\sum_{n=1}^{t_{\ell p}} \left(\frac{f(g^m g^n)}{\ell p}\right) \boldsymbol{e}\left(\frac{kn}{\ell p}\right)\right|\right)^2 &\leqslant t_{\ell p} \sum_{m=1}^{t_{\ell p}} \left|\sum_{n=1}^{t_{\ell p}} \left(\frac{f(g^m g^n)}{\ell p}\right) \boldsymbol{e}\left(\frac{kn}{\ell p}\right)\right|^2 \\ &\leqslant t_{\ell p} \sum_{x=1}^{\ell p} \left|\sum_{n=1}^{t_{\ell p}} \left(\frac{f(g^n x)}{\ell p}\right) \boldsymbol{e}\left(\frac{kn}{\ell p}\right)\right|^2 \\ &= t_{\ell p} \left|\sum_{n,m=1}^{t_{\ell p}} \boldsymbol{e}\left(\frac{k(n-m)}{\ell p}\right)\right| \left|\sum_{x=1}^{\ell p} \left(\frac{f(g^m x) f(g^n x)}{\ell p}\right)\right| \\ &\leqslant t_{\ell p}^2 \sum_{n=1}^{t_{\ell p}} \left|\sum_{x=1}^{\ell p} \left(\frac{f(x) f(g^n x)}{\ell p}\right)\right|.\end{aligned}$$

Using the multiplicativity property of complete sums (see, for example, [**10**, § 12.3]), we write

$$\sum_{x=1}^{\ell p} \left(\frac{f(x) f(g^n x)}{\ell p}\right) = \sum_{x=1}^{\ell} \left(\frac{f(x) f(g^n x)}{\ell}\right) \sum_{x=1}^{p} \left(\frac{f(x) f(g^n x)}{p}\right). \tag{4.4}$$

https://doi.org/10.1017/S001309150700123X Published online by Cambridge University Press

For a fixed prime ℓ, the Weil bound (see [**10**, Theorem 11.23]), implies that, unless the polynomial $F_n(X) = f(X)f(g^n X)$ is a perfect square modulo ℓ, we have

$$\sum_{x=1}^{\ell} \left(\frac{f(x)f(g^n x)}{\ell} \right) \ll \ell^{1/2}.$$

Since $f(X)$ is without multiple roots if ℓ is large enough, it follows that $f(X)$ is not a perfect square modulo ℓ. Thus, $F_n(X) = f(X)f(g^n X)$ is a perfect square modulo ℓ only if $f(X)$ and $f(g^n X)$ have a common root modulo ℓ. In this case, we have

$$R(g^n) \equiv 0 \pmod{\ell}, \tag{4.5}$$

where $R(Y) = \mathrm{Res}_X(f(X), f(XY)) \in \mathbb{Z}[Y]$ is the resultant with respect to X of $f(X)$ and $f(XY)$. It is clear that $R(Y)$ is a non-zero polynomial whose coefficients depend only on the coefficients of the polynomial $f(X)$. Thus, the congruence $R(y) \equiv 0 \pmod{\ell}$ has $O(1)$ solutions in residue classes y modulo ℓ once ℓ is large. This clearly puts g^n in $O(1)$ residue classes modulo ℓ, and thus puts n into $O(1)$ residue classes modulo t_ℓ. For each such n, we estimate the corresponding character sum over u trivially as ℓ.

Applying now the above argument to both the sums on the right-hand side in (4.4), we get that

$$\sum_{n=1}^{t_{\ell p}} \left| \sum_{x=1}^{\ell p} \left(\frac{f(x)f(g^n x)}{\ell p} \right) \right| \ll t_{\ell p}(\ell p)^{1/2} + \frac{t_{\ell p}}{t_p} \ell^{1/2} p + \frac{t_{\ell p}}{t_\ell} \ell p^{1/2} + \ell p.$$

The assumptions that $t_\ell > \ell^{1/2}$ and $t_p > p^{1/2}$ imply that the first term dominates the second and the third terms, while the assumption (4.2) implies that it also dominates the last term. Thus,

$$\sum_{m=1}^{t_{\ell p}} \left| \sum_{n=1}^{t_{\ell p}} \left(\frac{f(g^m g^n)}{\ell p} \right) \boldsymbol{e}\left(\frac{an}{\ell p} \right) \right| \ll t_{\ell p}^{3/2} (\ell p)^{1/4},$$

which, after substitution in inequality (4.3), implies inequality (4.1) and concludes the proof. □

5. Some arithmetic functions

To be able to apply Lemma 4.1, we need to show that for many primes ℓ the multiplicative order of g modulo ℓ is sufficiently large. We have the following result, which can be derived in an identical way to [**11**, Lemma 20] using the concrete value of α given by (1.1).

Lemma 5.1. *There exists a constant $\gamma > 0$, such that for at least $\gamma z / \log z$ primes $\ell \leqslant z$, we have $t_\ell \geqslant \ell^\alpha$.*

We note that Lemma 5.1 implies that there exist constants $c > 0$ and $C > 1$ with the property that there is a set $\mathcal{L}_z$ containing at least $cz/\log z$ primes $\ell \in [z, Cz]$ such that $t_\ell \geqslant \ell^\alpha$ for all $\ell \in \mathcal{L}_z$. We write $\omega_z(k)$ for the number of prime factors $\ell \in \mathcal{L}_z$ of k.

https://doi.org/10.1017/S001309150700123X Published online by Cambridge University Press

Lemma 5.2. *The bound*

$$\sum_{n=M+1}^{M+N} \omega_z(u(n)) \ll \frac{Nz^{1-\alpha}}{\log z} + z$$

holds uniformly over $M \geqslant 0$, $N \geqslant 1$ *and* $z > 1$.

Proof. We have

$$\begin{aligned}\sum_{n=M+1}^{M+N} \omega_z(u(n)) &\ll \sum_{n=M+1}^{M+N} \sum_{\substack{\ell \in \mathcal{L}_z,\\ \ell \mid u(n)}} 1 \\ &= \sum_{\ell \in \mathcal{L}_z} \sum_{\substack{n=M+1,\\ \ell \mid u(n)}}^{M+N} 1 \\ &\leqslant \sum_{\ell \in \mathcal{L}_z} \left(\frac{N}{t_\ell} + 1\right) \\ &\leqslant \frac{N}{z^\alpha} \#\mathcal{L}_z + z \\ &\ll \frac{Nz^{1-\alpha}}{\log z} + z,\end{aligned}$$

which concludes the proof. □

6. Proof of Theorem 1.3

We keep the previous notation. Let us fix some sufficiently large real $z > 1$. We note that if $k \geqslant 1$ is a perfect square, then

$$\sum_{\ell \in \mathcal{L}_z} \left(\frac{k}{\ell}\right) \geqslant \#\mathcal{L}_z - \omega_z(k).$$

Let $\mathcal{N}_z$ be the set of integers $n \in [M+1, M+N]$ with $\omega_z(u(n)) \leqslant \frac{1}{2}\#\mathcal{L}_z$, and let $\mathcal{E}_z$ be the set of remaining integers $n \in [M+1, M+N]$.

By Lemma 5.2, we have

$$\#\mathcal{E}_z \leqslant \frac{Nz^{1-\alpha}/\log z + z}{\frac{1}{2}\#\mathcal{L}_z} \ll Nz^{-\alpha} + \log z. \tag{6.1}$$

From now on, we look at $n \in \mathcal{N}_z$ for which $\mathbb{Q}(\sqrt{u(n)}) = \mathbb{Q}(\sqrt{s})$. For such a value of n, we have that $su(n)$ is a perfect square and that $s \mid u(n)$. In particular, $\omega_z(su(n)) = \omega_z(u(n))$. Thus, if for some $n \in \mathcal{N}_z$ we have $\mathbb{Q}(\sqrt{u(n)}) = \mathbb{Q}(\sqrt{s})$, then

$$\sum_{\ell \in \mathcal{L}_z} \left(\frac{su(n)}{\ell}\right) \geqslant \#\mathcal{L}_z - \omega_z(su(n)) = \#\mathcal{L}_z - \omega_z(u(n)) \geqslant \tfrac{1}{2}\#\mathcal{L}_z.$$

https://doi.org/10.1017/S001309150700123X Published online by Cambridge University Press

In particular,

$$(\tfrac{1}{2}\#\mathcal{L}_z)^2 Q_u(s;M,N) \leqslant \sum_{n=M+1}^{M+N} \biggl(\sum_{\ell\in\mathcal{L}_z} \biggl(\frac{su(n)}{\ell} \biggr) \biggr)^2 + (\tfrac{1}{2}\#\mathcal{L}_z)^2 \#\mathcal{E}_z,$$

which we rewrite as

$$Q_u(s;M,N) \ll z^{-2}(\log z)^2 \sum_{n=M+1}^{M+N} \biggl(\sum_{\ell\in\mathcal{L}_z} \biggl(\frac{su(n)}{\ell} \biggr) \biggr)^2 + \#\mathcal{E}_z. \tag{6.2}$$

Squaring out, changing the order of summation and separating the 'diagonal term' $N\#\mathcal{L}_z$ corresponding to $\ell = p$, we see that

$$\sum_{n=M+1}^{M+N} \biggl(\sum_{\ell\in\mathcal{L}_z} \biggl(\frac{su(n)}{\ell} \biggr) \biggr)^2 \leqslant N\#\mathcal{L}_z + \sum_{\substack{\ell,p\in\mathcal{L}_z,\\ \ell\neq p}} \sum_{n=M+1}^{M+N} \biggl(\frac{su(n)}{\ell p} \biggr). \tag{6.3}$$

The estimates (6.2) and (6.3) yield

$$\begin{aligned} Q_u(s;M,N) &\ll \frac{(\log z)^2}{z^2} \biggl(N\#\mathcal{L}_z + \sum_{\substack{\ell,p\in\mathcal{L}_z,\\ \ell\neq p}} \sum_{n=M+1}^{M+N} \biggl(\frac{su(n)}{\ell p} \biggr) \biggr) + \#\mathcal{E}_z \\ &\ll \frac{N\log z}{z} + Nz^{-\alpha} + \log z + \frac{(\log z)^2}{z^2} \sum_{\substack{\ell,p\in\mathcal{L}_z,\\ \ell\neq p}} \sum_{n=M+1}^{M+N} \biggl(\frac{su(n)}{\ell p} \biggr). \end{aligned} \tag{6.4}$$

Applying Lemma 4.1 to the inner sum, we get

$$\begin{aligned} \sum_{\substack{\ell,p\in\mathcal{L}_z,\\ \ell\neq p}} \sum_{n=M+1}^{M+N} \biggl(\frac{su(n)}{\ell p} \biggr) &\ll \sum_{\substack{\ell,p\in\mathcal{L}_z,\\ \ell\neq p}} \biggl(\frac{N}{t_{\ell p}} + 1 \biggr) t_{\ell p}^{1/2} (\ell p)^{1/4} \log(\ell p) \\ &\ll N(\log z) \sum_{\substack{\ell,p\in\mathcal{L}_z,\\ \ell\neq p}} \frac{(\ell p)^{1/4}}{t_{\ell p}^{1/2}} + z^{3/2}(\log z)(\#\mathcal{L}_z)^2 \\ &\ll N(\log z) \sum_{\substack{\ell,p\in\mathcal{L}_z,\\ \ell\neq p}} \frac{(\gcd(\ell-1,p-1))^{1/2}(\ell p)^{1/4}}{(t_\ell t_p)^{1/2}} + \frac{z^{7/2}}{\log z}. \end{aligned}$$

Therefore,

$$\sum_{\substack{\ell,p\in\mathcal{L}_z,\\ \ell\neq p}} \sum_{n=M+1}^{M+N} \biggl(\frac{su(n)}{\ell p} \biggr) \ll Nz^{-\alpha+1/2}(\log z) \sum_{\substack{\ell,p\in\mathcal{L}_z,\\ \ell\neq p}} (\gcd(\ell-1,p-1))^{1/2} + \frac{z^{7/2}}{\log z}. \tag{6.5}$$

https://doi.org/10.1017/S001309150700123X Published online by Cambridge University Press

Furthermore,

$$\sum_{\substack{\ell,p\in\mathcal{L}_z,\\ \ell\neq p}} (\gcd(\ell-1,p-1))^{1/2} \ll \sum_{1\leqslant d\leqslant Cz} d^{1/2} \sum_{\substack{p,\ell\in\mathcal{L}_z,\\ d\mid\ell-1,\\ d\mid p-1}} 1 \ll \sum_{1\leqslant d\leqslant Cz} d^{1/2}\biggl(\frac{Cz}{d}\biggr)^2$$

$$\ll z^2 \sum_{d\leqslant Cz} \frac{1}{d^{3/2}} \ll z^2.$$

Substituting this bound in (6.5), we obtain

$$\sum_{\substack{\ell,p\in\mathcal{L}_z,\\ \ell\neq p}} \sum_{n=M+1}^{M+N} \biggl(\frac{su(n)}{\ell p}\biggr) \ll Nz^{5/2-\alpha}\log z + \frac{z^{7/2}}{\log z}.$$

Inserting the last estimate into (6.4), and ignoring the terms $Nz^{-1}\log z$, $Nz^{-\alpha}$ and $\log z$, which are dominated by others, we derive

$$Q_u(s;M,N) \ll Nz^{1/2-\alpha}(\log z)^3 + z^{3/2}\log z.$$

Choosing $z = N^{1/(1+\alpha)}(\log N)^{2/(1+\alpha)}$ yields the desired result.

References

1. R. C. Baker and G. Harman, Shifted primes without large prime factors, *Acta Arith.* **83** (1998), 331–361.
2. F. Beukers and H. P. Schlickewei, The equation $x + y = 1$ in finitely generated groups, *Acta Arith.* **78** (1996), 189–199.
3. L. Caporaso, J. Harris and B. Mazur, Uniformity of rational points, *J. Am. Math. Soc.* **10** (1997), 1–35.
4. P. Corvaja and U. Zannier, Diophantine equations with power sums and universal Hilbert sets, *Indagationes Math.* **9** (1998), 317–332.
5. P. Cutter, A. Granville and T. J. Tucker, The number of fields generated by the square root of values of a given polynomial, *Can. Math. Bull.* **46** (2003), 71–79.
6. E. Dobrowolski and K. S. Williams, An upper bound for the sum $\sum_{n=a+1}^{a+H} f(n)$ for a certain class of functions f, *Proc. Am. Math. Soc.* **114** (1992), 29–35.
7. P. Erdős and R. Murty, On the order of $a \pmod p$, in *Proc. 5th Canadian Number Theory Association Conf.*, pp. 87–97 (American Mathematical Society, Providence, RI, 1999).
8. J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, Linear equations in variables which lie in a multiplicative group, *Annals Math.* **155** (2002), 807–836.
9. D. R. Heath-Brown, The square sieve and consecutive squarefree numbers, *Math. Annalen* **266** (1984), 251–259.
10. H. Iwaniec and E. Kowalski, *Analytic number theory* (American Mathematical Society, Providence, RI, 2004).
11. P. Kurlberg and C. Pomerance, On the period of the linear congruential and power generators, *Acta Arith.* **119** (2005), 149–169.
12. F. Pappalardi, On the order of finitely generated subgroups of $\mathbb{Q}^* \pmod p$ and divisors of $p-1$, *J. Number Theory* **57** (1996), 207–222.

https://doi.org/10.1017/S001309150700123X Published online by Cambridge University Press

13. R. D. Patterson, A. J. van der Poorten and H. C. Williams, Characterization of a generalized Shanks sequence, *Pac. J. Math.* **230** (2007), 185–215.

14. D. Shanks, On Gausss class number problems, *Math. Comp.* **23** (1969), 151–163.

15. A. J. van der Poorten and H. C. Williams, On certain continued fraction expansions of fixed period length, *Acta Arith.* **89** (1999), 23–35.

16. H. C. Williams, Some generalizations of the S_n sequence of Shanks, *Acta Arith.* **69** (1995), 199–215.

17. H. B. Yu, Estimates of character sums with exponential function, *Acta Arith.* **97** (2001), 211–218.

https://doi.org/10.1017/S001309150700123X Published online by Cambridge University Press