Publ. Math. Debrecen
83/1-2 (2013), 227–239
DOI: 10.5486/PMD.2013.5677

On the powers of integers and conductors of quadratic fields

By NİHAL BİRCAN (Çankırı, Berlin) and MICHAEL E. POHST (Berlin)

Abstract. We consider non-zero integers of the maximal order $\mathcal{O} = O_F$ of the quadratic field $F = \mathbb{Q}(\sqrt{d}\,)$ where $d \in \mathbb{Z}$ is square-free. Let p be an odd prime and $0 \neq \alpha \in O_F$. Using the embedding into $\mathrm{GL}(2,\mathbb{R})$ we obtain bounds for the first $\nu \in \mathbb{N}$ such that $\alpha^\nu \equiv 1 \bmod p$. For a conductor f, we then study the smallest positive integer $n = n(f)$ such that $\alpha^n \in \mathcal{O}_f$. We obtain bounds for $n(f)$ and for $n(fp^k)$. The most interesting case is where α is the fundamental unit of $\mathbb{Q}(\sqrt{d}\,)$.

1. Introduction

We consider quadratic fields $F = \mathbb{Q}(\sqrt{d}\,)$ where $d \in \mathbb{Z}$ is square-free. We write $d = 4q + r$ with $r \in \{1, 2, 3\}$. The algebraic integers α of $\mathbb{Q}(\sqrt{d}\,)$ are given by

$$\alpha = \begin{cases} a + b\sqrt{d},\ \ a, b \in \mathbb{Z} & \text{if } r = 2, 3 \\ \dfrac{1}{2}(a + b\sqrt{d}\,),\ \ a, b \in \mathbb{Z},\ \ a + b \in 2\mathbb{Z} & \text{if } r = 1. \end{cases} \tag{1.1}$$

Throughout the paper α denotes a non-zero integer of F. Let p be an odd prime. First we study the problem to find small exponents n such that $\alpha^n \equiv 1 \bmod p$. We will extensively use Legendre symbols.

We adapt the classical Chebyshev polynomials T_n and U_n (for detailed information see [9] Section 5.7, [1] Chapter 22) by defining

$$t_n(x) = t_n(x; s) = 2s^{n/2} T_n\left(\frac{x}{2\sqrt{s}}\right), \tag{1.2}$$

Mathematics Subject Classification: 11R11, 11R04, 42C05.
Key words and phrases: Chebyshev polynomials, conductor, integer of quadratic field.

$$u_n(x) = u_n(x; s) = s^{n/2} U_n \left(\frac{x}{2\sqrt{s}} \right) \tag{1.3}$$

for $n \in \mathbb{N}_0$ where s is the norm of a non-zero integer in the quadratic field F. These are unimodular polynomials with integer coefficients. For technical reasons we use this modification of Chebyshev polynomials for treating the cases $d \equiv 1 \bmod 4$ and $d \equiv 2, 3 \bmod 4$ simultaneously. In Section 6 we present all properties of these adapted polynomials which we use for proving our results. Then we specialize the results of the paper [2] about $\mathrm{GL}(2, \mathbb{Z})$ to quadratic fields. For previous works on this subject see e.g. [4], [5], [6].

In Section 2, we consider 2×2 matrices over the rational integers and show how the integers of any quadratic field $F = \mathbb{Q}(\sqrt{d}\,)$ can be embedded into $\mathrm{GL}(2, \mathbb{R})$. We also prove that $\alpha^n \equiv 1 \bmod p$ holds if and only if $A^n \equiv I \bmod p$ where the matrix A is the image of α. In the next sections we consider non-zero integers α of F and especially units α. In these sections we apply the results of [2] to the case of quadratic fields. Let f denote a conductor for F. In Section 5, we give upper estimates for

$$n(f) := \min\{\nu \in \mathbb{N} : \alpha^\nu \in \mathcal{O}_f\}$$

and also for $n(fp^k)$ where $k \in \mathbb{N}$ and p is an odd prime.

2. The embedding of algebraic integers of $\mathbb{Q}(\sqrt{d}\,)$ into $\mathrm{GL}(2, \mathbb{R})$

Let $A \in \mathrm{GL}(2, \mathbb{C})$, that is

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{C},\ ad - bc \neq 0. \tag{2.1}$$

We always write

$$x := \operatorname{tr} A = a + d, \quad s := \det A = ad - bc. \tag{2.2}$$

Proposition 2.1. *For $n \in \mathbb{N}$ we have*

$$A^n = u_{n-1}(x) A - s u_{n-2}(x) I, \tag{2.3}$$

$$A^n = \frac{1}{2} t_n(x) I + u_{n-1}(x)(A - \frac{1}{2} x I). \tag{2.4}$$

This proposition is known in various forms. For instance, (2.3) with $s = 1$ is Lemma 3.1.3 in [8] where $p_n = u_{n-1}$ and $q_n = u_{n-2}$. The last matrix in (2.4) has zero trace and it follows that

$$\operatorname{tr} A^n = t_n(x). \tag{2.5}$$

With the notation (2.1) we can write (2.4) as

$$A^n = \begin{pmatrix} \frac{1}{2}t_n(x) + \frac{1}{2}(a-d)u_{n-1}(x) & bu_{n-1}(x) \\ cu_{n-1}(x) & \frac{1}{2}t_n(x) - \frac{1}{2}(a-d)u_{n-1}(x) \end{pmatrix}. \tag{2.6}$$

Now, we consider algebraic integers α of $\mathbb{Q}(\sqrt{d})$ in the notation (1.1). We define a homomorphism φ of the multiplicative semigroup of non-zero integers α into $\mathrm{GL}(2,\mathbb{R})$. For $r = 2, 3$ we set (see e.g. [3, p. 38])

$$\varphi(\alpha) := A = \begin{pmatrix} a & b \\ bd & a \end{pmatrix} \tag{2.7}$$

whereas for $r = 1$ we set

$$\varphi(\alpha) := A = \begin{pmatrix} \frac{1}{2}(a+b) & b \\ qb & \frac{1}{2}(a-b) \end{pmatrix}. \tag{2.8}$$

It can be checked that this indeed defines an injective homomorphism. We have

$$s = \det A = \mathrm{Norm}(\alpha) = \begin{cases} a^2 - b^2 d & \text{if } r = 2, 3 \\ \frac{1}{4}(a^2 - b^2 d) & \text{if } r = 1, \end{cases} \tag{2.9}$$

$$x = \mathrm{tr}\, A = \begin{cases} 2a & \text{if } r = 2, 3 \\ a & \text{if } r = 1. \end{cases} \tag{2.10}$$

Since $A^n = \varphi(\alpha^n)$ and φ is injective, it follows from (2.6) that

$$\alpha^n = \begin{cases} \frac{1}{2}t_n(2a) + u_{n-1}(2a)b\sqrt{d} & \text{if } r = 2, 3 \\ \frac{1}{2}t_n(a) + \frac{1}{2}u_{n-1}(a)b\sqrt{d} & \text{if } r = 1. \end{cases} \tag{2.11}$$

Proposition 2.2. *If p is an odd prime and α_k, α_m are integers of $\mathbb{Q}(\sqrt{d})$ then $\alpha_k \equiv \alpha_m \bmod p$ if and only if $\varphi(\alpha_k) \equiv \varphi(\alpha_m) \bmod p$.*

Proof. We prove only the more complicated case $r = 1$ (see (1.1)). The statement can be proved in a similar way for $r = 2, 3$.

First we assume $\alpha_k \equiv \alpha_m \bmod p$ and we prove $\varphi(\alpha_k) \equiv \varphi(\alpha_m) \bmod p$. For $\alpha_k \equiv \alpha_m \bmod p$ with

$$\alpha_k = \frac{1}{2}\left(a_k + b_k\sqrt{d}\right), \quad \alpha_m = \frac{1}{2}\left(a_m + b_m\sqrt{d}\right).$$

we have $a_k \equiv a_m \bmod p$ and $b_k \equiv b_m \bmod p$. This implies $a_k+b_k \equiv a_m+b_m \bmod p$ and $a_k - b_k \equiv a_m - b_m \bmod p$. Since p is odd we obtain

$$\frac{1}{2}(a_k + b_k) \equiv \frac{1}{2}(a_m + b_m) \bmod p, \quad \frac{1}{2}(a_k - b_k) \equiv \frac{1}{2}(a_m - b_m) \bmod p.$$

Then (2.8) yields $\varphi(\alpha_k) \equiv \varphi(\alpha_m) \bmod p$.

Now we assume $\varphi(\alpha_k) \equiv \varphi(\alpha_m) \bmod p$ and prove $\alpha_k \equiv \alpha_m \bmod p$. Using the definition in (2.8) we can write

$$\varphi(\alpha_j) = \begin{pmatrix} \frac{1}{2}(a_j + b_j) & b_j \\ q b_j & \frac{1}{2}(a_j - b_j) \end{pmatrix}$$

for $j = k, m$. We immediately see that $b_k \equiv b_m \bmod p$, $\frac{1}{2}(a_k + b_k) \equiv \frac{1}{2}(a_m + b_m) \bmod p$ and $\frac{1}{2}(a_k - b_k) \equiv \frac{1}{2}(a_m - b_m) \bmod p$ and obtain $a_k \equiv a_m \bmod p$, hence $\alpha_k \equiv \alpha_m \bmod p$. $\square$

Proposition 2.3. *If $p \nmid b$, $p \nmid d$ then $\alpha^n \equiv 1 \bmod p$ if and only if $A^n \equiv I \bmod p$.*

Proof. (a) First, we assume $\alpha^n \equiv 1 \bmod p$. For $r = 2, 3$,

$$\alpha^n = \frac{1}{2}t_n(x) + u_{n-1}(x)b\sqrt{d} \equiv 1 \bmod p$$

with $p \nmid b$, $p \nmid d$ and x was defined in (2.10). Since $u_{n-1}(x) \equiv 0 \bmod p$ by (2.11) we get $\frac{1}{2}t_n(x) \equiv 1 \bmod p$. Hence, $A^n = \frac{1}{2}t_n(x)I + u_{n-1}(x)(A - \frac{1}{2}xI) \equiv I \bmod p$. For $r = 1$, namely, $\alpha^n = \frac{1}{2}t_n(x) + \frac{1}{2}u_{n-1}(x)b\sqrt{d}$, the proof is similar.

(b We assume $A^n \equiv I \bmod p$. Then

$$A^n = \frac{1}{2}t_n(x)I + u_{n-1}(x)\left(A - \frac{1}{2}xI\right) \equiv I \bmod p$$

and we want to prove $\alpha^n = \frac{1}{2}t_n(x) + u_{n-1}(x)b\sqrt{d} \equiv 1 \bmod p$ for $r = 2, 3$. By (2.6) we have $bu_{n-1}(x) \equiv 0 \bmod p$. Because of $b \not\equiv 0 \bmod p$ we get $u_{n-1}(x)(A - \frac{1}{2}xI)v \equiv 0 \bmod p$ and $\mathrm{tr}(A - \frac{1}{2}xI) \equiv 0 \bmod p$, hence

$$u_{n-1}(x)\begin{pmatrix} * & b \\ bd & * \end{pmatrix} \equiv 0 \bmod p.$$

This implies $u_{n-1}(x)b \equiv 0 \bmod p$. From (2.6) we obtain $\frac{1}{2}t_n(x) \equiv 1 \bmod p$ for the cases $r = 2, 3$ and $r = 1$, hence $\alpha^n \equiv 1 \bmod p$. $\square$

3. Non-zero integers α of F

In this section, we specialize the results of [2] to the case of quadratic fields using the embedding introduced in Section 2. We note that we allow d to be negative. Again we write $d = 4q + r$ and $s = \mathrm{Norm}(\alpha)$ for non-zero integers α of $F = \mathbb{Q}(\sqrt{d}\,)$ as in (1.1).

Let p be an odd prime. We assume that $p \nmid d$, $p \nmid b$ and that

$$a^2 - 4s \not\equiv 0 \bmod p \text{ for } r = 2,3, \quad a^2 - s \not\equiv 0 \bmod p \text{ for } r = 1. \tag{3.1}$$

Throughout the rest of the paper let x be the trace and s be the norm of α as defined in (2.10) and (2.9). Since t_n and u_n are polynomials with integer coefficients the identities in Section 6 can be transferred into congruences. We let ℓ be the Legendre symbol

$$\ell := \left(\frac{x^2 - 4s}{p}\right). \tag{3.2}$$

Then $p - \ell$ becomes $= p \mp 1$ for $\ell = \pm 1$.

Theorem 3.1. *Let p be an odd prime with $p \nmid d$, $p \nmid b$ and $s = \mathrm{N}(\alpha) \neq 0$. Let ℓ be the Legendre symbol defined above. We set $\sigma = 1$ for $\ell = +1$ and $\sigma = s$ for $\ell = -1$. Then*

$$t_{p-\ell}(x) \equiv 2\sigma \bmod p, \quad u_{p-\ell-1}(x) \equiv 0 \bmod p.$$

We sum up the further results in the following table.

	$r = 2,3$	$r = 1$
$\left(\frac{s}{p}\right) = +1$	$t_{\frac{p-\ell}{2}}(2a)^2 \equiv 4\sigma \bmod p$, $u_{\frac{p-\ell}{2}-1}(2a) \equiv 0 \bmod p$	$t_{\frac{p-\ell}{2}}(a)^2 \equiv 4\sigma \bmod p$, $u_{\frac{p-\ell}{2}-1}(a) \equiv 0 \bmod p$
$\left(\frac{s}{p}\right) = -1$	$t_{\frac{p-\ell}{2}}(2a) \equiv 0 \bmod p$, $(a^2 - s)u_{\frac{p-\ell}{2}-1}(2a)^2 \equiv \sigma \bmod p$	$t_{\frac{p-\ell}{2}}(a) \equiv 0 \bmod p$, $(a^2 - 4s)u_{\frac{p-\ell}{2}-1}(a)^2$ $\equiv 4\sigma \bmod p$.

This is [2, Theorem 4.1] specialized to our present situation.

The proof in [2] uses Chebyshev polynomials. In the present context of quadratic fields, many of the previous formulas can be proved by other methods, see for instance [3], [7, Theorem 1.7].

4. Units of F

First we consider the case $s = \mathrm{Norm}(\alpha) = +1$. Again we let ℓ be the Legendre symbol defined in (3.2), and x is defined in (2.10).

The following results are obtained by specializing the results in Sections 5 and 6 of [2]. The Legendre polynomials t_n and u_{n-1} depend only on x and s as defined in (2.9) and (2.10); the specific form (1.1) of α is not important.

Proposition 4.1. *Let $k \in \mathbb{N}$ divide $p-\ell$ and we assume that $\ell = \left(\frac{x^2-4s}{p}\right) \neq 0$. If $x \equiv t_k(y) \bmod p$ for some $y \in \mathbb{Z}$ then, with $n = \frac{p-\ell}{k}$,*

$$t_n(x) \equiv 2 \bmod p, \quad u_{n-1}(x) \equiv 0 \bmod p, \quad \alpha^n \equiv 1 \bmod p. \tag{4.1}$$

For a proof compare [2, Theorem 5.1].

For the special case that $k = 2^j$ we can say much more. We construct $x_0, \ldots, x_m$ recursively by the following rule. Let $x_0 = x$. For $\left(\frac{x+2}{p}\right) = -1$ we set $m = 0$ and stop. Now let $\left(\frac{x+2}{p}\right) = +1$ and suppose that $x_0, \ldots, x_k$ have already been constructed such that $2^k \mid (p-\ell)$ and

$$x_{\nu-1} \equiv t_2(x_\nu) \bmod p, \ ((x_\nu^2 - 4)/p) = \ell \quad \text{for } 1 \leq \nu \leq k. \tag{4.2}$$

For $2^{k+1} \nmid (p-\ell)$ or $\left(\frac{x_k+2}{p}\right) = -1$ we set $m = k$ and stop. Otherwise we have $2^{k+1} \mid (p-\ell)$ and $\left(\frac{x_k+2}{p}\right) = +1$. Then there exists x_{k+1} subject to $x_k + 2 \equiv x_{k+1}^2 \bmod p$ and thus $x_k = t_2(x_{k+1})$. It follows from (4.2) that

$$((x_k-2)/p) = ((x_k+2)/p)((x_k-2)/p) = ((x_k^2-4)/p) = \ell$$

and therefore $((x_{k+1}^2-4)/p) = ((x_k-2)/p) = \ell$. This completes our construction. We note that $2^m \mid (p-\ell)$.

Theorem 4.2. *Let $\mathrm{N}(\alpha) = 1$, $\ell = \left(\frac{x^2-4}{p}\right) \neq 0$ and $x_0, \ldots, x_m$ be constructed as above. Then*

$$t_{(p-\ell)/2^k}(x) \equiv 2 \bmod p \quad \text{for } k = 0, \ldots, m, \tag{4.3}$$

$$t_{(p-\ell)/2^{m+1}}(x) \equiv -2 \bmod p \quad \text{or } 2^{m+1} \nmid (p-\ell). \tag{4.4}$$

The proof is analogous to that of [2, Theorem 5.4].

Corollary 4.3. *Let $s = \mathrm{N}(\alpha) = 1$, $\ell = \left(\frac{x^2-4}{p}\right) \neq 0$ and let $x_0, \ldots, x_m$ be constructed as above. Setting $n = (p-\ell)/2^m$ we have*

$$u_{n-1}(x) \equiv 0 \bmod p, \quad \alpha^n \equiv 1 \bmod p. \tag{4.5}$$

For $2^{m+1} \mid (p-\ell)$ we additionally get

$$u_{\frac{n}{2}-1}(x) \equiv 0 \bmod p, \quad \alpha^{n/2} \equiv -1 \bmod p. \tag{4.6}$$

These bounds are best possible: $2^{m+2} \mid (p-\ell)$ implies $u_{\frac{n}{2}-1}(x) \not\equiv 0 \bmod p$.

Proof. Because of $s = 1$ and $x^2 - 4 \not\equiv 0 \bmod p$ it follows from (6.1) and (4.3) that $u_{n-1} \equiv 0 \bmod p$ and therefore $A^n \equiv I \bmod p$ by (2.4). By Proposition 2.3 we have $\alpha^n \equiv 1 \bmod p$. This proves (4.5). For $2^{m+1} \mid (p-\ell)$ the congruences (4.6) follow from (4.4) analogously. Finally, we let $2^{m+2} \mid (p-\ell)$. Then it follows from (4.4) that $t_{n/2}(x) \equiv -2 \bmod p$ so that $t_{n/4}(x) \equiv 0 \bmod p$ by the recursion formula for $t_n(x)$ which is similar to that for $u_n(x)$ in Section 6. Hence, $u_{\frac{n}{4}-1}(x) \not\equiv 0 \bmod p$. $\square$

Now we consider the more complicated case of units with norm -1, i.e.q $t_n(x) = t_n(x; -1)$. As before we set $\ell := \left(\frac{x^2-4s}{p}\right)$ and assume that (3.1) with $s = -1$ holds. We set $n = \frac{p-\ell}{2}$. Because of $(-1/p) = (-1)^{(p-1)/2}$ Theorem 3.1 (with $\sigma = \ell$) yields

$$t_{2n}(x) \equiv 2\ell \bmod p, \quad t_n(x)^2 \equiv 4\ell \bmod p, \quad u_{n-1}(x) \equiv 0 \bmod p \qquad \text{for } p \equiv 1 \bmod 4, \tag{4.7}$$

$$t_{2n}(x) \equiv 2\ell \bmod p, \quad t_n(x) \equiv 0 \bmod p, \quad u_{n-1}(x) \not\equiv 0 \bmod p \qquad \text{for } p \equiv 3 \bmod 4. \tag{4.8}$$

Then (6.3) implies that

$$t_{2(p-\ell)}(x) \equiv 2 \bmod p. \tag{4.9}$$

Hence, $t_n(x) \equiv \pm 2 \bmod p$ if and only if $p \equiv 1 \bmod 4$ and $\ell = +1$. Assuming the latter we obtain from (6.7) with $t_2(x; -1) = x^2 + 2$ that

$$t_{2n}(x; -1) = t_n(x^2 + 2; 1) \quad \text{for } n \in \mathbb{N}. \tag{4.10}$$

Because of $\left(\frac{-1}{p}\right) = +1$ there exists $j \in \mathbb{Z}$ with $j^2 \equiv -1 \bmod p$. We now assume that $x \not\equiv 0 \bmod p$ and $x \not\equiv \pm 2j \bmod p$. This implies

$$(x^2 + 2)^2 - 4 = x^2(x^2 + 4) \not\equiv 0 \bmod p. \tag{4.11}$$

Similar to Section 4, we construct numbers $y_0, \ldots, y_m$ subject to the initial condition $y_0 = x^2 + 2$ instead of $x_0 = x$. It follows from (4.11) that also $((y_0^2 - 4)/p) = \ell$. We have $y_0 + 2 = x^2 + 4$ and therefore $((y_0 + 2)/p) = \ell = +1$. Hence, the first step of our construction can always be carried out resulting in $m \geq 1$. The construction stops if $((y_m + 2)/p) = -1$ or $2^{m+1} \nmid (p-1)$.

Theorem 4.4. *Let* $\mathrm{N}(\alpha) = -1$, $p \equiv 1 \bmod 4$, $a^2 + 4 \not\equiv 0 \bmod p$, $\ell = +1$ *and let* $y_0, \ldots, y_m$ *be constructed as above. Then* $m \geq 1$ *and*

$$t_{(p-1)/2^k}(x) \equiv 2 \bmod p \quad \textit{for} \;\; k = 0, \ldots, m-1, \tag{4.12}$$

$$t_{(p-1)/2^m}(x) \equiv \begin{cases} -2 \bmod p & \textit{for } \ 2^{m+1} \mid (p-l), \\ 0 \bmod p & \textit{for } \ 2^{m+1} \nmid (p-\ell). \end{cases} \tag{4.13}$$

See [2, Theorem 6.1] for the proof. The next result is not a surprise because of $\mathrm{N}(\alpha^2) = 1$. The proof is similar to that of Corollary 4.3, so we omit it.

Corollary 4.5. *Under the assumptions of Theorem 4.4, we now write* $n = (p-\ell)/2^{m-1}$. *Then* (4.5) *holds, and in case* $2^{m+1} \mid (p-\ell)$ *then* (4.6) *is also fulfilled. These bounds are best possible: For* $2^{m+1} \mid (p-\ell)$ *we have* $u_{\frac{n}{4}-1}(x) \not\equiv 0 \bmod p$.

Theorem 4.6. *Let* $\mathrm{N}(\alpha) = -1$ *and* k *be odd with* $k \mid (p-\ell)$. *We put* $n = (p-\ell)/k$. *If* $x^2 + 4 \not\equiv 0 \bmod p$ *and* $x \equiv t_k(y; -1) \bmod p$ *for some* $y \in \mathbb{Z}$ *then*

$$t_{2n}(x) \equiv 2 \bmod p, \quad t_n(x) \equiv 2\ell \bmod p, \quad \alpha^n \equiv \ell \bmod p. \tag{4.14}$$

Proof. This was shown more generally in [2]. □

5. Estimates for conductors

We continue to study the quadratic field $F = \mathbb{Q}(\sqrt{d})$ with $d > 0$ and $r \in \{1, 2, 3\}$. The order with conductor $f \in \mathbb{N}$ is

$$\mathcal{O}_f = \begin{cases} \{a' + b' f\sqrt{d} : a', b' \in \mathbb{Z}\} & \text{if } r = 2, 3, \\ \left\{ \dfrac{1}{2}(a' + (f-1)b') + \tfrac{1}{2} b' f \sqrt{d} : a', b' \in \mathbb{Z}, \ 2 \mid a' + b' \right\} & \text{if } r = 1. \end{cases} \tag{5.1}$$

We fix an integer α of $\mathbb{Q}(\sqrt{d})$ with $s = \mathrm{N}(\alpha) \neq 0$. Let x be given by (2.10). Again we use the notation in (1.1). The most interesting case is that α is the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Following Halter–Koch we define

$$n(f) = n(f, \alpha) := \min\{\nu \in \mathbb{N} : \alpha^\nu \in \mathcal{O}_f\}. \tag{5.2}$$

Lemma 5.1. *Let* $b \neq 0$ *be given by (1.1) and* s, x *by (2.9). We write*

$$c := \gcd(b, f), b_0 := b/c, f_0 = f/c. \tag{5.3}$$

Then we have

$$n(f) = n(f_0) = \min\{\nu \in \mathbb{N} : u_{\nu-1}(x; s) \equiv 0 \bmod f_0\}. \tag{5.4}$$

Proof. By (2.9) and (2.10) we have

$$\alpha^\nu \in \mathcal{O}_f \Leftrightarrow bu_{\nu-1}(x) \equiv 0 \bmod f.$$

Since $\gcd(b_0, f_0) = 1$ it follows by (5.3) that

$$\alpha^\nu \in \mathcal{O}_f \Leftrightarrow b_0 u_{\nu-1}(x) \equiv 0 \bmod f_0 \Leftrightarrow u_{\nu-1}(x) \equiv 0 \bmod f_0.$$

We note that b has not been replaced by b_0. Therefore we still have $u_{\nu-1}(x) = u_{\nu-1}(x; s)$ with x and s unchanged. □

Let $g \in \mathbb{N}$ and $\gcd(b, g) = \gcd(f, g) = 1$. Then it follows from (5.4) and (6.5) that $u_{n(f)n(g)-1}(x; s) \equiv 0 \bmod \operatorname{lcm}(f, g)f$. Hence, we get

$$n(fg) \le n(f)n(g) \quad \text{for } \gcd(f, g) = 1. \tag{5.5}$$

For an odd prime p we define

$$q(p) = q(p; \alpha) := \min\{\nu \in \mathbb{N} : u_{\nu-1}(x; s) \equiv 0 \bmod p\}. \tag{5.6}$$

The results of Sections 3 and 4 provide upper estimates for $q(p)$. These results depend explicitly on x and s, and implicitly on a, b and d in (1.1).

First let $\ell = \left(\frac{x^2-4s}{p}\right) \neq 0$. For $s = 1$ it follows from Corollary 4.3 that

$$q(p) \le \frac{p-\ell}{2^m}, \quad \text{and} \quad q(p) \le \frac{p-\ell}{2^{m+1}} \quad \text{for } 2^{m+1} \mid (p-\ell).$$

If $s = -1$, $p \equiv 1 \bmod 4$ and $\ell = +1$ then it follows from Corollary 4.5 that

$$q(p) \le \frac{p-\ell}{2^{m-1}} \quad \text{and} \quad q(p) \le \frac{p-\ell}{2^m} \quad \text{for } 2^m \mid (p-\ell).$$

Now let $x^2 - 4s \equiv 0 \bmod p$. Then for all $\nu \in \mathbb{N}$ it follows from (6.1) that $2^{\nu-1}u_{\nu-1}(x; s) \equiv \nu x^{\nu-1} \bmod p$. We conclude that $q(p) = p$ for $p \nmid s$ and $q(p) = 2$ for $p \mid s$.

Theorem 5.2. *For $\gcd(f, b) = 1$ and $p \nmid f$ we have*

$$n(p^k f) \le q(p)p^{k-1}n(f) \quad \textit{for all } k \ge 1. \tag{5.7}$$

Proof. We use induction on k. By (5.4) and (6.5) we have $u_{q(p)n(f)-1}(x;s) \equiv 0 \bmod f$. By (5.6) and (6.5) this congruence also holds modulo p. Since $\gcd(f,p)=1$ it follows that the congruence is true also modulo pf. Hence (5.7) holds for $k=1$ in view of (5.4).

Now let (5.7) hold for k. We write $\nu = q(p)p^{k-1}n(f)$ and have, by (5.7),

$$u_{\nu-1}(x;s) \equiv 0 \bmod p^k f. \tag{5.8}$$

We apply (6.1) with $n=p$ and with s^ν instead of s. The binomial coefficients in the sum are divisible by the prime p. Because of $2^{p-1} \equiv 1 \bmod p$ we get for $z \in \mathbb{Z}$

$$u_{p-1}(z;s^\nu) \equiv (z^2-4s^\nu)^{(p-1)/2} \bmod p.$$

For $z = t_\nu(x;s)$ we obtain by (6.2) that

$$u_{p-1}(t_\nu(x;s);s^\nu) \equiv \left[(x^2-4s)u_{\nu-1}(x;s)\right]^{\frac{p-1}{2}} \equiv 0 \bmod p. \tag{5.9}$$

Here we used (5.8) for $k \geq 1$. Now we apply (6.4) with $m=p$ and $n=\nu$. By (5.8) and (5.9) we obtain

$$u_{q(p)p^k-1}(x;s) = u_{p\nu-1}(x;s) \equiv 0 \bmod p^{k+1}f.$$

Hence, it follows from (5.4) that $n(p^{k+1}f) \leq q(p)p^k$. □

Theorem 5.3. *Let $f \in \mathbb{N}$ be odd and let f_0 be defined as in* (5.3). *We write*

$$f_0 = \prod_{\nu=1}^{\mu} {p_\nu}^{k_\nu} \quad (k_\nu \in \mathbb{N}) \tag{5.10}$$

with different primes p_ν. Then

$$n(f) \leq \prod_{\nu=1}^{\mu} \left(q(p_\nu){p_\nu}^{k_\nu-1}\right). \tag{5.11}$$

Proof. Let $g_0 = 1$ and for $1 \leq \lambda \leq \mu$

$$g_\lambda = \prod_{\nu=1}^{\lambda} {p_\nu}^{k_\nu} \quad (1 \leq \lambda \leq \mu).$$

Then $g_\lambda = p^{k_\lambda} g_{\lambda-1}$ and $p_\lambda \nmid g_{\lambda-1}$. Hence we obtain from Theorem 5.2 applied to f_0 that

$$n(f_\lambda) \leq q(p_\lambda)p^{k_\lambda-1}n(f_{\lambda-1}).$$

Hence, (5.11) with f replaced by f_0 follows by induction. Finally, we use that Lemma 5.1 implies $n(f) = n(f_0)$. □

6. Addendum: useful formulas for Chebyshev polynomials

We present several formulas which we need in proving our results. We put our emphasis on the polynomials u_n defined in (1.3) (see [9, Section 5.7] and [2]). For odd n and $x, s \in \mathbb{C}$, we have

$$u_{n-1}(x;s) = \frac{1}{2^{n-1}} \sum_{k=0}^{(n-3)/2} \binom{n}{2k+1} x^{n-2k-1}(x^2-4s)^k + \frac{1}{2^{n-1}}(x^2-4s)^{\frac{n-1}{2}}. \quad (6.1)$$

The recursion formula $u_{n+1}(x) = xu_n(x) - su_{n-1}(x)$ shows that

$$u_0(x) = 1, \quad u_1(x) = x, \quad u_2(x) = x^2 - s, \quad u_3(x) = x^3 - 2sx,$$
$$u_4(x) = x^4 - 3sx^2 + s^2, \quad u_5(x) = x^5 - 4sx^3 + 2s^2x.$$

Furthermore, $t_n(x;s)$ and $u_n(x;s)$ are polynomials in $\mathbb{Z}[x,s]$. For $n \in \mathbb{N}$ we have

$$(x^2-4s)u_{n-1}(x;s)^2 = t_n(x;s)^2 - 4s^n \quad (6.2)$$

$$t_n(x;s)^2 = t_{2n}(x;s) + 2s^n. \quad (6.3)$$

We need a relation for products which involves different parameters.

$$u_{mn-1}(x;s) = u_{m-1}(t_n(x;s);s^n)\ u_{n-1}(x;s) \quad (m,n \in \mathbb{N}). \quad (6.4)$$

It follows that for $\mu \in \mathbb{N}$ and $x, s \in \mathbb{Z}$

$$u_{n-1}(x;s) \equiv 0 \bmod \mu \Rightarrow u_{mn-1}(x;s) \equiv 0 \bmod \mu. \quad (6.5)$$

To prove (6.4) it is sufficient to consider $\frac{x}{2\sqrt{s}} = \cos\theta$ with real θ. Then it follows from (1.2), (1.3) and the properties [9, p. 257] of the T_n and U_n that

$$t_n(x;s) = 2s^{\frac{n}{2}}\cos(n\theta), \quad u_{m-1}(x;s) = s^{\frac{m-1}{2}}\frac{\sin(m\theta)}{\sin\theta}. \quad (6.6)$$

By (1.3) and (1.2) we therefore have

$$\begin{aligned} u_{m-1}(t_n(x;s);s^n) &= s^{n\frac{m-1}{2}} U_{m-1}\left(\frac{1}{2s^{n/2}t_n(x;s)}\right) \\ &= s^{n\frac{m-1}{2}} U_{m-1}(\cos(n\theta)) = s^{\frac{mn-n}{2}}\frac{\sin(mn\theta)}{\sin n\theta}. \end{aligned}$$

Now we multiply by $u_{n-1}(x;s)$. Using (6.6) we obtain

$$u_{m-1}(t_n(x;s);s^n)u_{n-1}(x;s) = s^{\frac{mn-1}{2}} \frac{\sin(mn\theta)}{\sin n\theta} = u_{mn-1}(x;s)$$

using (6.6) again.

In Section 4 we use the following relation between the polynomials $t_n(x;s)$ with different parameters s. If $s \neq 0$ and $m, n \in \mathbb{N}$ then

$$t_{mn}(x;s) = t_n(t_m(x;s);s^m). \tag{6.7}$$

Indeed, (1.2) and the composition property $T_{mn} = T_n \circ T_m$ imply that

$$t_{mn}(x;s) = 2(s^m)^{n/2} T_n\left(T_m\left(\frac{x}{2\sqrt{s}}\right)\right) = t_n\left(\frac{1}{2\sqrt{s}^m} T_m\left(\frac{x}{2\sqrt{s}}\right);s^m\right)$$

from which (6.7) follows using (1.2).

Acknowledgements. The authors would like to thank Prof. Dr. F. Halter-Koch for suggesting the interesting problem of Section 5, Prof. Dr. Christian Pommerenke for the identity (6.4) and also Prof. Dr. Attila Pethő and the referees for their valuable comments and remarks.

References

[1] M. Abramowitz and I. A. Stegun, Handbook of Mathematical Functions, *Dover Publications, New York*, 1972.

[2] N. Bircan and C. Pommerenke, On Chebyshev polynomials and GL$(2,\mathbb{Z}/p\mathbb{Z})$, *Bull. Math. Soc. Sci. Math. Roumanie* **55**(103), no. 4 (2012), 353–364.

[3] E. J. Barbeau, Pell's equation, *Springer Verlag, New York*, 2003.

[4] J. Denef, The Diophantine Problem for Polynomial Rings of Positive Characteristic, Logic Colloquium 78, *North-Holland Publishing Company*, 1979.

[5] J. H. Jaroma, On the rank of apparition of composite N in Lehmer sequences, *Nonlinear Analysis* **63** (2005), e1081–e1086.

[6] P. Kiss, On rank of apparition of primes in Lucas sequences, *Publ. Math. Debrecen* **36** (1989), 147–151.

[7] D. H. Lehmer, An extended theory of Lucas functions, *Ann. of Math.* **31** (1930), 419–448.

[8] C. Maclachlan and A. W. Reid, The arithmetic of hyperbolic 3-manifolds, *Springer-Verlag, New York*, 2003.

[9] W. Magnus, F. Oberhettinger and R. P. Soni, Formulas and Theorems for the Special Functions of Mathematical Physics, *Springer-Verlag, Berlin*, 1966.

NİHAL BİRCAN
BERLIN UNIVERSITY OF TECHNOLOGY
INSTITUTE FOR MATHEMATICS, MA 3-2
STRASSE DES 17. JUNI 136
D-10623 BERLIN
GERMANY

AND

ÇANKIRI KARATEKIN UNIVERSITY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS
TR 18100, ÇANKIRI
TURKEY

E-mail: bircan@math.tu-berlin.de

MICHAEL E. POHST
BERLIN UNIVERSITY OF TECHNOLOGY
INSTITUTE FOR MATHEMATICS, MA 3-2
STRASSE DES 17. JUNI 136
D-10623 BERLIN
GERMANY

E-mail: pohst@math.tu-berlin.de

(Received October 12, 2012; revised February 14, 2013)