INTEGER PARTS OF POWERS OF QUADRATIC UNITS

DANIEL CASS

(Communicated by Larry J. Goldstein)

ABSTRACT. Let \( \alpha > 1 \) be a unit in a quadratic field. The integer part of \( \alpha^n \), denoted \([\alpha^n]\), is shown to be composite infinitely often. Provided \( \alpha \neq (1 + \sqrt{5})/2 \), it is shown that the number of primes among \([\alpha], [\alpha^2], \ldots, [\alpha^n]\) is bounded by a function asymptotic to \( c \cdot \log^2 n \), with \( c = 1/(2 \log 2 \cdot \log 3) \).

Let \( \alpha > 1 \) be a unit in a quadratic field \( \mathbb{Q}(\sqrt{D}) \), with \( D > 1 \) a square-free rational integer. It is known in some cases that the integer parts \([\alpha^n]\) of powers of \( \alpha \) (\( n = 1, 2, 3, \ldots \)) are composite infinitely often [1]. We show this in general, the proof guaranteeing in fact that infinitely many of the \([\alpha^n]\) are divisible by \( [\alpha] \). (There is one exceptional case \( \alpha = (1 + \sqrt{5})/2 \) wherein \([\alpha] = 1 \); here infinitely many of the \([\alpha^n]\) are divisible by \([\alpha^2] > 1 \).

Define \( f_\alpha(x) \) to mean the number of \( n, 1 \leq n \leq x \), for which \([\alpha^n]\) happens to be prime. We derive a bound on \( f_\alpha(x) \) which is independent of both \( \alpha \) and \( \mathbb{Q}(\sqrt{D}) \) (except that we require \( \alpha \neq (1 + \sqrt{5})/2 \)), namely

\[ f_\alpha(x) \leq 1 + B(x), \]

where \( B(x) \) denotes here, and in what follows, the number of positive integers \( \leq x \) of the form \( 2^r 3^s, r \geq 0, s \geq 0 \).

HEURISTIC REMARK. As \( x \to \infty \) the function \( 1 + B(x) \) is asymptotic to \( c \log^2 x \), where \( c = 1/(2 \log 2 \cdot \log 3) \). If one says "\( m \) is prime with probability \( 1/\log m \)," then \([\alpha^n]\) is prime with probability about \( 1/n \log \alpha \). Summing this for \( n \leq x \) we expect \( \sim (1/\log \alpha) \log x \) primes in the sequence \([\alpha^n]\), \( 1 \leq n \leq x \). The latter function grows more slowly than \( c \log^2 x \), so in this sense the bound \( 1 + B(x) \) is not at odds with probability.

We show first that for \( \alpha \) with norm \( N(\alpha) = -1 \), \([\alpha]\) divides \([\alpha^n]\) for all odd \( n \). This reduces us to the norm 1 case, in which we show that, if \([\alpha^n]\) is prime, then \( n \) is of the form \( 2^r 3^s \) (giving the above bound).

LEMMA 1. Suppose \( \alpha > 1 \) is a unit of \( \mathbb{Q}(\sqrt{D}) \) with \( D > 1 \) squarefree. Write \( t_n \) for \([\alpha^n]\), and let \( N(\beta) \) denote the norm and \( \beta' \) the conjugate of \( \beta \) for \( \beta \) any integer of \( \mathbb{Q}(\sqrt{D}) \). Then:

(a) If \( N(\alpha) = 1 \), then \( t_n = (\alpha^n + \alpha^{-n}) - 1 \).

(b) If \( N(\alpha) = -1 \), then

\[ t_n = \begin{cases} \alpha^n - \alpha^{-n}, & \text{if } n \text{ is odd,} \\ (\alpha^n + \alpha^{-n}) - 1, & \text{if } n \text{ is even.} \end{cases} \]
PROOF. \( N(\alpha) = 1 \) means \( \alpha \alpha' = 1 \), so \( \alpha' = \alpha^{-1} \). Write \( \alpha^n \) in the form \((a_n + b_n \sqrt{D})/2\); then \( a_n \) and \( b_n \) are rational integers, and we have \( a_n = \alpha^n + \alpha^{-n} \), so that \( \alpha^n = a_n - \alpha^{-n} \). Since \( 0 < \alpha^{-n} < 1 \), part (a) follows.

Now assume \( N(\alpha) = -1 \). Then \( \alpha \alpha' = -1 \) so \( \alpha' = -\alpha^{-1} \). Then \( a_n = \alpha^n + \alpha^{-n} = \alpha^n + (-\alpha^{-1})^n = \alpha^n + (-1)^n \alpha^{-n} \). If \( n \) is odd, then from \( a_n = \alpha^n - \alpha^{-n} \) we have \( \alpha^n = a_n + \alpha^{-n} \), and since \( 0 < \alpha^{-n} < 1 \), \( t_n = [\alpha^n] = a_n = \alpha^n - \alpha^{-n} \).

If \( n \) is even, then from \( a_n = \alpha^n + \alpha^{-n} \) we conclude as in case (a) that \( t_n = \alpha^n + \alpha^{-n} - 1 \). \( \square \)

**Lemma 2.** Suppose \( N(\alpha) = -1 \) and set \( t_n = [\alpha^n] \). Then whenever \( m \geq n \) we have the four following multiplication formulas for \( t_m t_n \), depending on the parity of \( m \) and \( n \):

(a) \( m \) odd, \( n \) odd: \( t_m t_n = t_{m+n} - t_{m-n} \),
(b) \( m \) even, \( n \) odd: \( t_m t_n = t_{m+n} - t_{m-n} - t_n \),
(c) \( m \) odd, \( n \) even: \( t_m t_n = t_{m+n} + t_{m-n} - t_m \),
(d) \( m \) even, \( n \) even: \( t_m t_n = t_{m+n} + t_{m-n} + t_m - t_n + 1 \).

Furthermore, in the case \( N(\alpha) = +1 \), formula (d) holds (without the parity restriction) for any \( m, n \) with \( m \geq n \). In all the formulas \( t_0 \) is allowed and is 1.

**Proof.** Substitute for \( t_m \) and \( t_n \) their expressions from Lemma 1; the formulas follow (after some algebra).

**Lemma 3.** Suppose \( N(\alpha) = -1 \) and \( t_n = [\alpha^n] \). Then we have the congruences (to the modulus \( t_1 \)):

\[
t_n \equiv \begin{cases} +1, & n \text{ even}, \\ 0, & n \text{ odd}. \end{cases}
\]

**Proof.** We have \( t_0 \equiv 1 \), \( t_1 \equiv 0 \). Apply Lemma 2 with \( n = 1 \). Then we only use formulas (a) and (b), and to the modulus \( t_1 \) they both read

\[
0 \equiv t_{m+1} - t_{m-1}.
\]

Therefore \( t_2 \equiv t_0 \equiv 1 \), \( t_3 \equiv t_1 \equiv 0 \), and so on.

Note that (except when \( \alpha = (1 + \sqrt{5})/2 \), when \( t_1 = 1 \)), on considering when \([\alpha^n]\) is composite where \( N(\alpha) = -1 \), the preceding lemma allows us to consider only \( [\alpha^2], [\alpha^4], \ldots \), i.e. the sequence \([\beta^n] = [\alpha^{2n}]\), where \( \beta = \alpha^2 \) has norm +1. That \( \alpha = (1 + \sqrt{5})/2 \) is the only quadratic unit for which \( t_1 = [\alpha] = 1 \) follows easily from \( 4N(\alpha) = a^2 - Db^2 \).

**Lemma 4.** Suppose \( N(\beta) = +1 \) \((\beta > 1)\) and \( t_n = [\beta^n] \). Then we have the congruences in the following table, to the modulus \( t_1 \):

\[
\begin{array}{cccccc}
 n \mod 6 & 0 & 1 & 2 & 3 & 4 & 5 \\
t_n \mod t_1 & 1 & 0 & -2 & -3 & -2 & 0
\end{array}
\]

**Proof.** In formula (d) of Lemma 2 (which applies here in all cases \( m \geq n \)) put \( n = 1 \); to the modulus \( t_1 \) the formula reads

\[
0 \equiv t_{m+1} + t_{m-1} - t_m + 1,
\]

which gives the \( t_m \) (mod \( t_1 \)) recursively, producing the above table. \( \square \)
COROLLARY. Regardless of \( N(\alpha) \), \([\alpha]\) divides \([\alpha^n]\) infinitely often. If \( \alpha \neq (1 + \sqrt{5})/2 \), this \([\alpha]\) is > 1.

LEMMA 5. Suppose \( N(\gamma) = +1 \) (\( \gamma > 1 \)) and set \( t_n = [\gamma^n] \). Then if \( t_n \) is prime, \( n \) is of the form \( 2^r 3^s \).

PROOF. First note that \( t_1 > 1 \) since \( N(\gamma) = +1 \) precludes \( \gamma = (1 + \sqrt{5})/2 \). It follows that \( t_h > 1 \) for \( h \geq 1 \).

Suppose \( n \) is not of the form \( 2^r 3^s \). Then \( n \) has a factor \( 6k + 5 \) or \( 6k + 7 \) with \( k \geq 0 \). Write \( n = h(6k + 5) \) or \( n = h(6k + 7) \), with \( h \geq 1 \). Then Lemma 4 with \( \beta = \gamma^h \) shows that \( t_n \) is divisible by \( t_h \), and \( 1 < t_h < t_n \) so that \( t_n \) is composite. \( \square \)

COROLLARY. If \( N(\gamma) = +1 \) and \( f_\gamma(x) \) denotes the number of primes among \( t_1, t_2, \ldots, t_n \) with \( n = [x] \), then \( f_\gamma(x) \leq B(x) \).

THEOREM 1. Suppose \( \alpha > 1 \) (\( \alpha \neq (1 + \sqrt{5})/2 \)) is a unit in some quadratic field \( \mathbb{Q}(\sqrt{D}) \), \( D > 1 \) squarefree. With \( f_\alpha(x) \) as above, then

\[
 f_\alpha(x) \leq 1 + B(x).
\]

This bound is independent of \( \alpha \) and \( \mathbb{Q}(\sqrt{D}) \).

PROOF. First suppose \( N(\alpha) = -1 \). Since \( \alpha \neq (1 + \sqrt{5})/2 \), \([\alpha]\) > 1 and Lemma 3 imply that \([\alpha^n]\) is composite if \( n \) is odd and \( \geq 3 \). \( f_\alpha(x) \) is then at most \( 1 + e \), where \( e \) is the number of primes among \([\alpha^2], [\alpha^4], \ldots, [\alpha^{n'}] \) (where \( n' \) is either \( n \) or \( n - 1 \)). By Corollary to Lemma 5 with \( \beta = \alpha^2 \), the latter number is at most \( B(x/2) \leq B(x) \); the bound holds.

When \( N(\alpha) = +1 \), Corollary to Lemma 5 already gives the bound. \( \square \)

REMARK. Let \( \alpha = (1 + \sqrt{5})/2 \). If \( n \) is odd and composite, say \( n = n_1 n_2 \) with \( n_1, n_2 \) odd and \( \geq 3 \), then \([\alpha^{n_1}] > 1 \) and Lemma 3 shows that \([\alpha^n]\) is divisible by \([\alpha^{n_1}]\). Hence among the odd powers only \([\alpha^p]\) (with \( p \) an odd prime) can be primes.

REFERENCES


DEPARTMENT OF MATHEMATICS, ST. JOHN FISHER COLLEGE, ROCHESTER, NEW YORK 14618