Journal of Integer Sequences, Vol. 17 (2014),
Article 14.4.8

Cyclic Products of Purely Periodic Irrationals

C. R. Carroll
Department of Mathematics
Texas A&M University
Kingsville, TX 78363
USA
c-carroll@tamuk.edu

Abstract

Let $(a_0, \cdots, a_{k-1})$ be a sequence of positive integers and m a positive integer. We prove that "almost every" real quadratic unit ϵ of norm $(-1)^k$ admits at least m distinct factorizations into a product of purely periodic irrationals of the form

$$\epsilon = [\overline{a_0; a_1, \ldots, a_{k-1}, x, y}] \times [\overline{a_1; a_2, \ldots, x, y, a_0}] \times \cdots \times [\overline{y; a_0, \ldots, a_{k-1}, x}].$$

Periods exhibited in this expression are not assumed minimal. The analogous assertion holds for real quadratic units $\epsilon > 1$ with prime trace and $m = 1$. The proofs are based on the fact that an integral polynomial map of the form $f(x, y) = axy + by + cx + d$, $\gcd(a, bc) = 1$, $a > 1$, $b, c > 0$, assumes almost every positive integral value and almost every prime value when evaluated over the positive integers.

1 Introduction

To a sequence of positive integers $\nu = (a_0, a_1, a_2, \ldots, a_{k-1})$, $k \geq 1$, we associate the real quadratic unit $\epsilon > 1$ obtained by taking the following product of purely periodic quadratic irrationals

$$\epsilon = \prod_{i=0}^{k-1} [\overline{a_i; a_{i+1}, \ldots, a_{k-1}, a_0, a_{i-1}}]. \tag{1}$$

Deviating from the standard convention we allow periods exhibited in this expression to be multiples of the minimal period. This convention is retained throughout. An induction shows that $\epsilon > 1$ is a quadratic unit [13]. Alternatively, this fact follows easily from the matrix approach to the continued fraction algorithm (see van der Poorten [12] and §4); from this point of view (1) corresponds to the matrix relation

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \epsilon \begin{pmatrix} \alpha \\ 1 \end{pmatrix} \tag{2}$$

where

$$\alpha = [\overline{a_0; a_1, \ldots, a_{k-1}}].$$

Note from (2) that ϵ has norm $(-1)^k$.

Every real quadratic unit $\epsilon > 1$ has a trivial factorization of the form given in (1). Let N denote the trace of ϵ. For ϵ with norm -1 we have $\epsilon = [\overline{N;}]$; otherwise when the norm is $+1$ we have $\epsilon = [\overline{1; N-2}] \times [\overline{N-2; 1}]$.

We call a product of the form given in (1) a *cyclic factorization* of the corresponding unit ϵ. Such factorizations are of interest from a variety of different points of view. Distinct factorizations of ϵ may be taken to represent distinct conjugacy classes of hyperbolic matrices in $GL(2, \mathbb{Z})$ with dominant eigenvalue ϵ. These classes, in the study of hyperbolic automorphisms of the torus, correspond to topological conjugacy classes of homeomorphisms, the invariants ϵ and ν having natural topological interpretations [1]. By a result due to Latimer and MacDuffee [7] there is a further identification with ideal classes of the order $\mathbb{Z}[\epsilon]$. If ϵ_0 is the fundamental unit of $\mathbb{Q}[\sqrt{d}]$ (d square-free), then, as explained by Yamamoto [13], the field class number $h(d)$ can be identified with the number of cyclic factorizations of ϵ_0 satisfying the special condition that the factors have discriminant d.

With the aid of a computer the complete family of cyclic factorizations of a real quadratic unit $\epsilon > 1$, for ϵ not too large, can be determined. Looking at such families one observes in general a profusion of cyclic factorizations, the associated sequences ν displaying a great deal of randomness. A natural question is the extent to which these sequences ν may vary over the family of factorizations determined by a unit ϵ. We call a sequence of integers whose terms are known with the exception of d integers in fixed positions a *d-pattern*. We consider the extent to which units ϵ admit cyclic factorizations instantiating a given d-pattern. If the length of the pattern is odd, it may be assumed the corresponding units have norm -1, a condition noted above to be necessary.

For a 1-pattern $\nu(x) = (a_0, \ldots, a_{k-1}, x)$, $k \geq 2$, it is not hard to see that a significant proportion of real quadratic units $\epsilon > 1$ of norm $(-1)^{k+1}$ have no factorization instantiating $\nu(x)$. This is a consequence of the fact that the existence of a corresponding cyclic factorization would induce a constraint on the congruence class, relative to certain moduli, of the trace of ϵ. The same constraint arises also for certain d-patterns, $d > 1$, for instance for the patterns $(a, x, a-1, a+1, y)$, $a > 1$. However, if a d-pattern has at least two adjacent free variables, a corresponding cyclic factorization almost always exits. We prove

Theorem 1. *Let $\nu = (a_0, a_1, \cdots, a_{k-1})$ be a sequence of positive integers and m be an arbitrary positive integer. Almost every real quadratic unit $\epsilon > 1$ of norm $(-1)^k$ admits a* *factorization over $\mathbb{Q}[\epsilon]$ of the form*

$$\epsilon = [\overline{a_0; a_1, \ldots, a_{k-1}, x, y}] \times [\overline{a_1; a_2, \ldots, x, y, a_0}] \times \cdots \times [\overline{y; a_0, \ldots, a_{k-1}, x}]. \tag{3}$$

The integers x, y may be selected in at least m different ways. Furthermore, if $\nu \neq (1)$ almost every unit whose trace belongs to a fixed integer translate of the primes has at least one such factorization.

The argument given extends to certain 2-patterns whose free variables are not adjacent. Moreover, Theorem 1 immediately generalizes to finite families of sequences. Fix a finite family of sequences $\mathcal{F}$ with lengths of a single parity. For example we may take $\mathcal{F}$ to consist of all sequences of odd (resp., even) length whose length and terms satisfy fixed upper bounds. Then almost every real quadratic unit $\epsilon > 1$ of norm -1 (resp., $+1$) has a cyclic factorization of the form given in (3) for each $\nu \in \mathcal{F}$. In the contrary direction, we see in §2 that given a fixed sequence ν of length k there exist infinitely many real quadratic units $\epsilon > 1$ of norm $(-1)^k$ that have no corresponding cyclic factorization. If Dickson's conjecture is correct, then given a finite family $\mathcal{F}$ as above, these units may be taken to have no cyclic factorization corresponding to any sequence $\nu \in \mathcal{F}$.

The sense in which units are to be considered generic can be made precise as follows. Let $\epsilon_{(i,+)}$, $i \geq 3$, (resp., $\epsilon_{(i,-)}$, $i \geq 1$) denote the real quadratic unit of magnitude greater than one with trace i and norm $+1$ (resp., -1). The magnitude of such a unit is well approximated by its trace (since $\left|\epsilon_{(i,\pm)} - i\right| < 1$). Let $\mathcal{T}_+$ (resp., $\mathcal{T}_-$) be the set of traces i of units of the form $\epsilon_{(i,+)}$ (resp., $\epsilon_{(i,-)}$) that satisfy a given statement. The statement will be said to hold of *almost every* unit ϵ_k of norm $+1$ (resp., -1) or, also, of a *generic unit* of this type, if and only if the corresponding subset of $\mathcal{T}_+$ (resp., of $\mathcal{T}_-$) is of asymptotic density one in the integers. The same approach can be employed to define genericity relative to any infinite subset of units $\epsilon_{(i,+)}$ (resp., $\epsilon_{(i,-)}$); in particular, the trace i may be taken to be prime. It is not hard to show that almost every real quadratic unit $\epsilon_{(i,+)}$ (resp., $\epsilon_{(i,-)}$) is a fundamental unit [10].

The proof of Theorem 1 rests on the following result on the representation of integers by polynomials. Let $f(x, y) = axy + by + cx + d$ be an integral polynomial such that $a > 1$, $b, c \in \mathbb{Z}^+$, and $\gcd(a, bc) = 1$. Let P denote the set of primes.

Theorem 2. *Let $R_f = \{f(x, y) : x, y \in \mathbb{Z}^+\}$. Fix $m \in \mathbb{Z}^+$. Then: (i) $R_f \cap \mathbb{Z}^+$ is of asymptotic density one within the set of positive integers, each element of the set being represented by at least m distinct pairs of positive integers (x, y); (ii) $R_f \cap P$ is of relative asymptotic density one in P.*

Assertion (i) follows quickly from the fact that, given a fixed modulus a, almost every integer has at least one divisor in each residue class $r \bmod a$, $\gcd(r, a) = 1$ [2]. S.K. Stein [11] obtains a more general factorization result from which he derives (i) with $m = 1$ and $d = 0$. The proof of (ii) relies on Dirichlet's and de la Vallée Poussin's theorems, together with a modern variant of Euler's product identity for arithmetic progressions. The relative density of the set of primes that is represented by a general two-variable integral quadratic polynomial over the integers was investigated in well-known work of Iwaniec [5]. Their results imply that the above polynomials $f(x,y)$ assume a set of prime values of positive relative density when evaluated over the integers. We should note that in contrast with the restricted class of polynomials considered here, which assume a set of integer values of asymptotic density one, the usual number-theoretic focus is on polynomials that assume a sparse set of integer values. It is possible to extend the argument given for (ii) to a more general class of integral polynomials of the form $f(x,y) = (rx+ty)(ux+my)+bx+cy+d$, subject to various restrictions on the parameters, but this level of generality is not needed for our purposes.

In §2-3 a proof of Theorem 2 is given. The derivation of Theorem 1 is given in §4.

2 The representation of positive integers

Let $f(x,y) = a\,xy + by + cx + d$ be an integral polynomial whose coefficients satisfy

$$a > 1, \quad b, c > 0, \quad \gcd(a, bc) = 1. \tag{4}$$

We consider the positive integral values taken by $f(x,y)$ over the positive integers. This set may be identified with $f(\mathbb{Z}^+ \times \mathbb{Z}^+)$ up to a possible finite number of non-positive values that may arise when $d < 0$.

Given $N \in \mathbb{Z}^+$ we say $f(x,y)$ *represents* N if there exist integers $x,\ y \in \mathbb{Z}^+$ such that $f(x,y) = N$; it should be emphasized that the representation we are considering is over the positive integers, an assumption necessitated by our later arguments (see §4). We will say $f(x,y)$ represents a set $B \subset \mathbb{Z}^+$ if it represents each element of B in the above sense.

Fix an infinite set of positive integers B and let $A \subset B$. Then the *asymptotic density* (or *natural density*) of A relative to B is defined to be the limit

$$d_B(A) = \lim_{k \to \infty} \frac{|A \cap \{1, 2, \ldots, k\}|}{|B \cap \{1, 2, \ldots, k\}|}$$

provided it exists. If $d_B(A) = 1$ we will say that *almost every element of B lies in A* or, alternatively, that *A is of full density in B*. On occasion the reference to B is omitted, in which case it is to be assumed $B = \mathbb{Z}^+$.

In this section we show that any polynomial $f(x,y)$ satisfying the conditions stated in (4) represents almost every positive integer, or $d_{\mathbb{Z}^+}(f(\mathbb{Z}^+ \times \mathbb{Z}^+) \cap \mathbb{Z}^+) = 1$.

We recall some basic facts. Let B be an infinite set of integers and let $\mathcal{C}$ be the collection of all subsets of B having well-defined asymptotic density relative to B. It is well-known that $\mathcal{C}$ is closed under finite disjoint unions and under complementation but is not closed under intersection and hence does not form an algebra. A useful property of d_B is that it is additive over disjoint sets in $\mathcal{C}$. Below we list several additional useful properties [8, pp. 79–80].

Lemma 3. *Let B be an infinite subset of positive integers and $A \subset B$.*

(i) *If* A *is finite then* $d_B(A) = 0$.

(ii) *Assume* A *has well-defined density, given by* $d_B(A) = d$. *If* A^c *is the complement of* A *in* B *then* $d_B(A^c) = 1 - d$.

(iii) *Let* A_i, $1 \le i \le k$, *be a collection of subsets of* B *for which* $d_B(A_i) = 1$. *Then the asymptotic density of* $\bigcap_{i=1}^k A_i$ *exists and is given by* $d_B(\bigcap_{i=1}^k A_i) = 1$.

(iv) *Assume* $A_1 \subset A_2$ *are nested subsets of* B *with well-defined asymptotic densities. Then* $d_B(A_1) \le d_B(A_2)$.

(v) *Let* A *be any subset of positive integers. Fix* $k_1 \in \mathbb{Z}^+$ *and* $k_2 \in \mathbb{Z}$. *Then* $d_{\mathbb{Z}^+}(A) = d$ *if and only if* $d_{\mathbb{Z}^+}(k_1\,A + k_2 \cap \mathbb{Z}^+) = d/k_1$.

(vi) *If* A_1, $A_2 \subset B$ *satisfy* $d_B(A_1) = 1$ *and* $d_B(A_2) = d$ *then the density of* $A_1 \cap A_2$ *relative to* B *is well-defined and given by* $d_B(A_1 \cap A_2) = d$.

We consider now the positive integers N represented by $f(x, y)$. A standard approach to finding solutions of an equation of the form $a\,xy + by + cx + d = N$ is to rewrite it as

$$aN - (ad - bc) \quad = \quad (ax + b)(ay + c). \tag{5}$$

From this equation we see that N is represented by $f(x, y)$ exactly when $aN - (ad - bc)$ is the product of two integers greater than a which belong to suitable residue classes modulo a. Of course, such a factorization need not exist; in particular $aN - (ad - bc)$ may be prime. By Dirichlet's theorem

Theorem 4 (Dirichlet)**.** *Every arithmetic progression of the form* $a\,x + b$, *with* a, b *non-zero integers satisfying* $a > 0$ *and* $\gcd(a, b) = 1$, *contains infinitely many primes. In fact, the sum of the reciprocals of the primes generated by such a progression diverges.*

Given that the fixed parameters of (5) satisfy $\gcd(a, ad - bc) = 1$, by Dirichlet's theorem the integer $aN - (ad - bc)$ is prime for infinitely many positive integral values of N; hence these values cannot be represented by $f(x, y)$. On the other hand we will see now that $f(x, y)$ represents almost every positive integer. This is a consequence of the fact that the divisors of an integer are in general well-distributed over residue classes. As stated by Erdős [2],

Proposition 5. *Let* $a \in \mathbb{Z}^+$, $a > 1$. *Let* $F(a)$ *denote the set of positive integers that have at least one divisor congruent to* k *modulo* a *for every integer* k *relatively prime to* a. *Then* $F(a)$ *is of full asymptotic density in* $\mathbb{Z}^+$.

By Lemma 3 (vi) this observation extends to any subset $S \subset \mathbb{Z}^+$ of positive asymptotic density; that is, $d_S(S \cap F(a)) = 1$. With this fact in hand it is easy to see that for almost every positive integer N there exist non-negative integers x, y satisfying (5).

Let T be the affine transformation given by $T(N) = a\,N - (ad - bc)$. The set $T(\mathbb{Z}^+)$ may include a finite number of non-positive integers which can be ignored since for any solution $x, y > 0$ of (5) the right-hand side of the equation must be positive. Accordingly let $B = T(\mathbb{Z}^+) \cap \mathbb{Z}^+$. Consider the subset $B_1 = B \cap F(a)$. Since by Lemma 3 (v) $d_{\mathbb{Z}^+}(B) = 1/a$, we have $d_{\mathbb{Z}^+}(B_1) = 1/a$ as well.

An element $m = T(N')$ of B_1 must satisfy the congruence $m \equiv bc \pmod{a}$. Given that $\gcd(b, a) = 1$, it follows m has a factorization of the form $m = m_1 m_2$ with $m_1 \equiv b \pmod{a}$ and hence with $m_2 \equiv c \pmod{a}$. Therefore (5) has a solution in non-negative integers x, y for $N = N'$ and indeed for any $N \in T^{-1}(B_1)$.

Consider now the asymptotic density of $T^{-1}(B_1)$. To simplify notation put $l = ad - bc$. Let $D_k = T^{-1}(B_1) \cap \{1, 2, \ldots, k\}$. Then $T(D_k) = B_1 \cap \{1, 2, \ldots, ak - l\}$ must be a set of the same cardinality, say n_k. Hence we may express the asymptotic density of B_1 as

$$d_{\mathbb{Z}^+}(B_1) = \lim_{k\to\infty} \frac{n_k}{ak + l} = \frac{1}{a} \lim_{k\to\infty} \frac{n_k}{k}.$$

Recalling that $d_{\mathbb{Z}^+}(B_1) = 1/a$ this shows $\lim_{k\to\infty} \frac{n_k}{k} = 1$. Therefore $T^{-1}(B_1)$ is of full density.

We now know that for almost every positive integer N there exist non-negative integers x, y satisfying (5). It remains to be shown that there exist multiple positive solutions.

Let $\mathbb{Z}(a; s)$ denote the set of all positive integers m that are congruent to s modulo a.

Proposition 6. *Let k be an arbitrary positive integer and let $a, b, c \in \mathbb{Z}^+$ such that $a > 1$ and $\gcd(a, bc) = 1$. Then almost every integer $m \in \mathbb{Z}(a; bc)$ admits at least k distinct factorizations of the form $m = (xa + b)(ya + c)$, where x, $y \in \mathbb{Z}^+$.*

Proof. Let s, $k \in \mathbb{Z}^+$ and q be a prime such that $s > 2k + \left\lfloor \frac{c}{a} \right\rfloor$ and $q > b + s\,a$. Since $\gcd(a, b) = 1$ the integers $b + i\,a$, $0 < i \le s$, are relatively prime to qa. Note that they represent s distinct reduced residue classes modulo qa. By the remark following Proposition 5, $\mathbb{Z}(a; bc)$ contains a subset $\mathbb{Z}_1(a; bc)$ of full relative density whose elements have divisors in each of these residue classes. Fix $m' \in \mathbb{Z}_1(a; bc)$. Then, given any residue class $b + i_0\, a$ mod qa, $0 < i_0 \le s$, we may write m' as a product of positive integers $m' = m_1 m_2$ where

$$m_1 \equiv b + i_0\, a \pmod{qa}.$$

Since $m_1 m_2 \equiv b m_2 \equiv b\,c \pmod{a}$ it follows that $m_2 \equiv c \pmod{a}$. Put $\overline{c} = c - \left\lfloor \frac{c}{a} \right\rfloor$. We may write

$$m' \;=\; m_1\, m_2 \;=\; (b + i_0\, a + i_1\, qa)\,(\overline{c} + j_0\, a)$$

for non-negative integers i_1 and j_0. Notice that $m_1 = b + xa$ with $x = i_0 + i_1 q > 0$. When i_0 varies the factor m_1 determines at least s distinct residue classes modulo qa. We have $j_0 \le \left\lfloor \frac{c}{a} \right\rfloor$ for at most $\left\lfloor \frac{c}{a} \right\rfloor + 1$ values. In the remaining cases m_2 is of the form $c + ya$ with $y > 0$. Thus we have products $m' = (b + xa)(c + ya)$ with x, y positive and with at least $2\,k$ choices for the first factor. These factorizations are distinct unless $b = c$, in which case there are still at least k distinct factorizations. $\square$

We now are in a position to conclude

Corollary 7. *Fix $k \in \mathbb{Z}^+$. Let $f(x, y) = axy + by + cx + d$ be an integral polynomial such that $a, b, c > 0$, $a > 1$, and $\gcd(a, bc) = 1$. Then there exists a set of positive integers N of full asymptotic density such that $f(x, y) = N$ for at least k distinct pairs of positive integers (x, y).*

An alternative proof of Corollary 7 can be given starting from the following reformulation of $a\,xy + by + cx + d = N$, $a \neq 0$:

$$N \;=\; (ax + b)y + cx + d.$$

The idea, roughly, is as follows. Since $\gcd(a, b) = 1$ Dirichlet's theorem yields an infinite sequence of distinct primes $p_i = a\,x_i + b$. Each value of the index i in turn determines a corresponding arithmetic progression $p(x_i, y) = p_i\,y + (c\,x_i + d)$ in the variable y. By a result due to C. A. Rogers [3, p. 242] the asymptotic density of the positive integers that are realized by at least one of these progressions is bounded below by the asymptotic density of the set of positive integers that are divisible by at least one of the primes p_i. This density is known to be 1 provided the sum $\sum_{j=1}^{\infty} \frac{1}{p_i}$ diverges [8], a fact which in the case at hand is a consequence of Dirichlet's theorem. Consequently $T(x, y)$ represents almost every positive integer over $\mathbb{Z}^+ \times \mathbb{Z}^+$. A trick similar to that used in the proof of Proposition 6 is needed to obtain multiple representations.

3 The representation of primes

Corollary 7 gives no information about the representation of sets of integers of asymptotic density zero. In this section we consider the representation of primes. We show

Proposition 8. *Let $f(x, y) = a\,xy + by + cx + d$ be an integral polynomial whose coefficients satisfy $a > 1$, $b, c > 0$, and $\gcd(a, bc) = 1$. Then $f(x, y)$ represents (over the positive integers) a set of primes p of full relative density.*

Remark 9. Since the integer d is arbitrary, $f(x, y)$ also represents a subset of full relative density of any fixed integer translate of the primes.

The proof of Proposition 8 is based on Dirichlet's theorem and the following additional classical results. De la Vallée Poussin established that the primes generated by an arithmetic progression are equidistributed among the possible residue classes. Let P be the set of primes and $P_{a,b}$ the set of primes generated by the arithmetic progression $a\,x + b$, $a > 0$, $\gcd(a, b) = 1$. We have

Theorem 10 (de la Vallée Poussin)**.**

$$\lim_{k \to \infty} \frac{|P_{a,b} \cap \{1, 2, \ldots, k\}|}{|P \cap \{1, 2, \ldots, k\}|} = \frac{1}{\phi(a)}$$

,

where ϕ denotes Euler's totient function.

We also rely on the following variant of Euler's famous product identity for primes generated by an arithmetic progression [6]:

Theorem 11. *Let a, b be integers such that $a > 0$ and $\gcd(a, b) = 1$. Then*

$$\prod_{q \in P_{a,b}} \left(1 - \frac{1}{q}\right) = 0.$$

To establish Proposition 8, we consider the families of primes generated by arithmetic progressions obtained by evaluating the polynomials $f(x, y) = (a\,x + b)\,y + cx + d$ at selected values of x.

To fix ideas let us consider an arbitrary pair of arithmetic progressions $q_1\,y + r_1$, $q_2\,y + r_2$, with q_1, q_2 distinct odd primes and r_1, r_2 relatively prime to q_1, q_2, respectively. We wish to determine the relative asymptotic density of the set of primes A generated by these progressions, $A = P_{q_1,r_1} \cup P_{q_2,r_2}$. This is most conveniently accomplished by computing the relative asymptotic density of the complementary set of primes $P - A$. Notice that only finitely many primes $q_c \in P - A$ can belong to one of the four residue classes $0 \pmod{q_i}$, $r_i \pmod{q_i}$, $i = 1, 2$. The remaining primes q_c are distributed across $(q_1 - 2)(q_2 - 2)$ possible pairs of residue classes. Let $k_1 \pmod{q_1}$, $k_2 \pmod{q_2}$ be such a pair, with the residues k_i taken to be reduced modulo q_i, $i = 1, 2$. By the Chinese remainder theorem the condition that the prime q_c belong to this pair of classes is equivalent to a condition of the form

$$q_c \equiv s_3 \pmod{q_1 q_2}, \tag{6}$$

with s_3 a fixed integer such that $1 \leq s_3 \leq q_1 q_2 - 1$. Since k_1, $k_2 \neq 0$, we have $\gcd(s_3, q_1\,q_2) = 1$. Applying Theorem 10 we see that the set of all primes satisfying (6) has relative density

$$d_P(P_{q_1 q_2, s_3}) = \lim_{k \to \infty} \frac{|P_{q_1 q_2, s_3} \cap \{1, 2, \ldots, k\}|}{|P \cap \{1, 2, \ldots, k\}|} = \frac{1}{\phi(q_1\,q_2)} = \frac{1}{(q_1 - 1)(q_2 - 1)}.$$

Since this computation does not depend on which of the $(q_1 - 2)(q_2 - 2)$ pairs of residue classes under consideration is selected, the total number of primes in $P - A$ is asymptotic to

$$(q_1 - 2)\,(q_2 - 2)\,\frac{1}{(q_1 - 1)(q_2 - 1)} = \left(1 - \frac{1}{q_1 - 1}\right)\left(1 - \frac{1}{q_2 - 1}\right)$$

The argument generalizes to any number k of progressions. Thus we have

Lemma 12. *Let q_j, $1 \leq j \leq k$, be k distinct primes and r_j corresponding integers such that* $\gcd(q_j, r_j) = 1$. *Let $A = \bigcup_{j=1}^{k} P_{q_j, r_j}$. Then the asymptotic density of A within the set of primes is given by*

$$1 - \prod_{j=1}^{k} \left(1 - \frac{1}{q_j - 1}\right)$$

This fact can be extended to the case of an infinite union $\bigcup_{j=1}^{\infty} P_{q_j,r_j}$ by applying Lemma 3 (iv) to the nested sequence of sets

$$A_i = \bigcup_{j=1}^{i} P_{q_j,r_j}, \quad i \in \mathbb{Z}^+.$$

We obtain

Lemma 13. *Let q_j be an infinite sequence of distinct primes and r_j a corresponding sequence of integers satisfying $\gcd(q_j, r_j) = 1$. Then $\bigcup_{j=1}^{\infty} P_{q_j,r_j}$ is a set of full density within the set of primes provided*

$$\prod_{j=1}^{\infty} \left(1 - \frac{1}{q_j - 1}\right) = 0.$$

The proof of Proposition 8 is now straightforward. Assume the polynomial

$$f(x,y) = axy + by + cx + d = (ax+b)y + cx + d$$

satisfies the hypotheses of Proposition 8. By Dirichlet's theorem the values of $ax+b$ are prime for an increasing sequence of positive integers x_i. We write $p_i = a\,x_i + b$, $r_i = cx_i + d$. Consider the arithmetic progression in y given by $f(x_i, y) = p_i\,y + r_i$. If $\gcd(p_i, r_i) = 1$, Dirichlet's theorem can be applied a second time.

Lemma 14. *There exists an integer i_0 such that for $i \geq i_0$*

$$\gcd(p_i, r_i) = \gcd(ax_i + b, c\,x_i + d) = 1.$$

Proof. Since $a \neq 1$ and $\gcd(a, c) = 1$, it follows $a \neq c$.

Case (i): $a > c$. For x_i sufficiently large necessarily $0 < cx_i + d < ax_i + b$. Since $p_i = ax_i + b$ is prime $\gcd(p_i, cx_i + d) = 1$.

Case (ii): $a < c$. Since $\gcd(a, c) = 1$ we have $c = k\,a + c'$ for positive integers k and c' with $0 < c' < a$. Thus we may write

$$\begin{aligned} f(x_i, y) &= (ax_i + b)y + (k\,a + c')x_i + d \\ &= (ax_i + b)(y + k) + c'x_i + d' \end{aligned}$$

where $d' = d - k\,b$. Again, for x_i sufficiently large $0 < c'x_i + d' < ax_i + b$. Hence $\gcd(ax_i + b, cx_i + d) = \gcd(ax_i + b, (cx_i + d) - k(ax_i + b)) = \gcd(ax_i + b, c'x_i + d') = 1$. □

Hence we may apply Dirichlet's theorem to the progressions $p_i y + r_i$ for sufficiently large values of the index i, say, $i \geq i_0$; accordingly, $f(x,y)$ represents the primes P_{p_i,r_i} for $i \geq i_0$.

Consider $\bigcup_{i=i_0}^{\infty} P_{p_i,r_i}$. Theorem 11 yields

$$\prod_{i=i_0}^{\infty} \left(1 - \frac{1}{p_i - 1}\right) \;\leq\; \prod_{i=i_0}^{\infty} \left(1 - \frac{1}{p_i}\right) \;=\; 0.$$

It follows by Lemma 13 that the set of primes $\bigcup_{i=i_0}^{\infty} P_{p_i,r_i}$ is of full density in the primes. Therefore $f(x,y)$ represents, over the positive integers, a set of primes of full relative density, completing the proof of Proposition 8.

4 Periods prescribed up to two adjacent integers

There exists a well-known correspondence, mentioned already in §1, between certain matrix products and continued fractions. In particular, the following two statements may be regarded as equivalent:

(i) $\alpha = [\overline{a_0; a_1, \ldots, a_{k-1}}]$ with k a fixed multiple of the minimal period).

(ii) For some unit $\epsilon \in \mathbb{Q}[\alpha]$, $\epsilon > 1$,

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \epsilon \begin{pmatrix} \alpha \\ 1 \end{pmatrix}. \tag{7}$$

From the second equation we obtain a corresponcing factorization of ϵ, as follows. Let α_m, $m \geq 0$ denote the purely periodic irrational obtained by cyclically permuting the period of the expansion of α so that a_m occurs as the initial element, i.e.,

$$\alpha_m = [\overline{a_m; a_{m+1}, \cdots, a_{k-1}, a_0, \cdots, a_{m-1}}].$$

Notice that $\alpha_{i+k} = \alpha_i$. A computation yields

$$\begin{pmatrix} a_m & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} \alpha_m \\ 1 \end{pmatrix} = \frac{1}{\alpha_{m+1}} \begin{pmatrix} \alpha_{m+1} \\ 1 \end{pmatrix}. \tag{8}$$

The k matrices occurring in (7) may be eliminated by repeatedly multiplying each side of the equation by the inverse of the left-most matrix and applying the equality of Equation (8) to the right-hand side of the equation. After the k-th multiplication we are left with

$$\begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \frac{\epsilon}{\alpha_0 \alpha_{k-1} \cdots \alpha_1} \begin{pmatrix} \alpha \\ 1 \end{pmatrix}.$$

Hence

$$\epsilon \;=\; \alpha_0\, \alpha_1 \ldots \alpha_{k-1}. \tag{9}$$

We call a matrix of the type arising in Equation (7)—that is, either a single matrix of the form $\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$, $a \in \mathbb{Z}^+$, or a finite product of such matrices—a *CF-matrix* of *depth* k. Such matrices have a simple characterization [12, Proposition 3]: namely, they are the non-negative elements $A = \begin{pmatrix} s_1 & s_2 \\ s_3 & s_4 \end{pmatrix}$ of $GL(2, \mathbb{Z})$ for which $s_1 \geq \max(s_2, s_3)$. By an elementary induction if $s_1 \neq 1$ the inequality is strict, $s_1 > \max(s_2, s_3)$.

One may easily verify that an arbitrary CF-matrix A of depth k in addition satisfies the following properties: $\mathtt{Det}(A) = (-1)^k$; $s_1, s_2, s_3 > 0$; $\gcd(s_1, s_2) = \gcd(s_1, s_3) = 1$.

Given a sequence of positive integers $\nu = (a_0, a_1, \cdots, a_{k-1})$, let

$$M_\nu(x, y) = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} y & 1 \\ 1 & 0 \end{pmatrix} \tag{10}$$

and let $\epsilon_\nu(x,y) > 1$ denote the dominant eigenvalue of $M_\nu(x,y)$. Writing

$$\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \prod_{0\le i\le k-1} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix},$$

we obtain the following expression for the trace of $M_\nu(x,y)$ (which by the Cayley-Hamilton theorem also gives the trace of its eigenvalues)

$$T_\nu(x,y) = b_1xy + b_2y + b_3x + b_1 + b_4.$$

Thus if $N \in \mathbb{Z}^+$ is represented by the polynomial $T_\nu(x,y)$—that is, $N = T_\nu(x_0,y_0)$ for some choice of positive integers $x_0,\ y_0$—then $\epsilon_\nu(x_0,y_0)$ is the dominant eigenvalue of the matrix $M_\nu(x_0,y_0)$ and by (9) it follows that $\epsilon_\nu(x_0,y_0)$ admits the cyclic factorization

$$[\overline{a_0; a_1, \ldots, a_{k-1}, x_0, y_0}] \times [\overline{a_1; a_2, \ldots, x_0, y_0, a_0}] \times \cdots \times [\overline{y_0; a_0, \ldots, a_{k-1}, x_0}].$$

By the characterization of CF-matrices provided above the polynomial $T_\nu(x,y)$ satisfies the hypotheses of Theorem 2 provided $\nu \neq (1)$. When $\nu = (1)$, $T_\nu(x,y) = (x+1)(y+1)$. In the former case, applying Theorem 2, and in the latter, noting that composite integers form a set of integers of asymptotic density one, we may conclude that $T_\nu(x,y)$ represents almost every positive integer N in at least m different ways. Turning to the representation of primes, assuming $\nu \neq (1)$, by Theorem 2 almost every prime is represented as well. This yields Theorem 1.

5 Acknowledgement

The author is grateful to an anonymous referee for helpful comments and corrections.

References

[1] R. Adler, C. Tresser, and P. A. Worfolk. Topological conjugacy of linear endomorphisms of the 2-torus, *Trans. Amer. Math. Soc.* **349** (1997), 1633–1652.

[2] P. Erdős. On the distribution of divisors of integers in the residue classes (mod d), *Bul. Soc. Math. Gréce (N.S.)* **6** (1965), fasc.1, 27–36.

[3] H. Halberstam and K. F. Roth. *Sequences*, Springer, New York, 1983.

[4] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*, 6th ed., Oxford University Press, 2008.

[5] H. Iwaniec. Primes represented by quadratic polynomials in two variables, *Acta Arith.* **24** (1974), 435–459.

[6] A. Languasco and A. Zaccagnini. A note on Mertens' formula for arithmetic progressions, *J. Number Theory* **127** (2007), 37–46.

[7] C. Latimer and C. C. MacDuffee. A correspondence between classes of ideals and classes of matrices, *Ann. of Math.* **34** (1933), 313–316.

[8] W. Narkiewicz. *Number Theory,* World Scientific, Singapore, 1983.

[9] P. A. B. Pleasants. The representation of primes by quadratic and cubic polynomials, *Acta Arith.* **12** (1966), 131–163.

[10] V. G. Sprindzŭk. The distribution of the fundamental units of real quadratic fields, *Acta Arith.* **25** (1973/74), 405–409.

[11] S. K. Stein. The density of the product of arithmetic progression, *Fibonacci Quart.* **11** (1973), 145–152.

[12] A. J. van der Poorten. Fractions of the period of the continued fraction expansion of quadratic integers, *Bull. Austral. Math. Soc.* **44** (1991), 155–169.

[13] Y. Yamamoto. Real quadratic number fields with large fundamental units, *Osaka J. Math.* **8** (1971), 261–270.

2010 *Mathematics Subject Classification*: Primary 11A55; Secondary 11N32, 37D20.
Keywords: simple continued fraction, purely periodic irrational, prime represented by quadratic polynomial, linear automorphism of the torus, Anosov automorphism.

Received May 3 2013; revised version received March 21 2014. Published in *Journal of Integer Sequences*, March 22 2014.

Return to Journal of Integer Sequences home page.