PACIFIC JOURNAL OF MATHEMATICS
Vol. 166, No. 1, 1994

THE DISTRIBUTION MOD n OF FRACTIONS WITH BOUNDED PARTIAL QUOTIENTS

Doug Hensley

Given a reduced fraction c/d with $0 < c < d$, there is a unique continued fraction expansion of c/d as $[0; a_1, a_2, \ldots a_r]$ with $r \geq 1$, $0 \leq a_j$ for $1 \leq j \leq r$, and $a_r \geq 2$. For fixed positive integer n, the asymptotic distribution of the pair (c, d) mod n among the $n^2 \prod_{p|n}(1 - 1/p^2)$ possible pairs of congruence classes is uniform when averaged over the set $Q(x) := \{(c, d) : 0 < c < d \leq x, \gcd(c, d) = 1\}$ as $x \to \infty$. The main result is that if attention is restricted to the (rather thin) subset $Q_m(x)$ of relatively prime pairs (c, d) so that all the continued fraction convergents $a_j \leq m$, the same equidistribution holds. As a corollary, the relative frequency, both in $Q(x)$ and in $Q_m(x)$ for any fixed $m > 1$, of reduced fractions (c, d) so that $d \equiv b$ mod n, is asymptotic to $n^{-1} \prod_{p|gcd(b,n)}(1 - p^{-1}) \prod_{q|n}(1 - q^{-2})^{-1}$. These results lend further heuristic support to Zaremba's conjecture, which in this terminology reads that for some m (perhaps even $m = 2$) the set of denominators d occurring in $Q_m(x)$ includes all but finitely many natural numbers. The proofs proceed from some recent estimates for the asymptotic size of $Q_m(x)$. Thereafter, the argument is combinatorial.

1. Introduction. Among fractions c/d with $0 \leq c < d$, gcd $(c, d) = 1$, and $d \leq x$, asymptotically equal proportions have $(c, d) \equiv (0, 1)$ mod 2, $(c, d) \equiv (1, 0)$ mod 2, and $(c, d) \equiv (1, 1)$ mod 2. (The proof is immediate and is left to the reader.) The same equidistribution among classes $(a \bmod n, b \bmod n)$ with gcd (gcd (a, n), gcd $(b, n)) = 1$ holds by a fairly simple inclusion and exclusion calculation. Numerical experimentation and Occam's razor both suggest that the same equidistribution should hold when attention is restricted to fractions c/d of the form $[0; a_1, a_2, \ldots a_r]$ with $a_r > 1, r \geq 1$ and all $a_i \leq m$. So it is. But before giving the proof, a cautionary example may be in order. If, instead of restricting the partial quotients to lie in a set $PQ = \{1, 2, \dots m\}$, we take $m = 30, PQ = \{16, 21\}$, then the result fails. Indeed, of the 576 pairs (a mod 30, b mod 30) satisfying the condition above that gcd (gcd (a, n), gcd $(b, n)) = 1$, only 480 occur.

An easy consequence of equidistribution of (c mod n, d mod n) is that the proportion of fractions under consideration with $d \leq x$ and satisfying $d \equiv b$ mod n, but with no corresponding modular restriction on c, is asymptotically given by

$$n^{-1} \prod_{p|\ \gcd\ (b,n)} (1 - p^{-1}) \prod_{q|n} (1 - q^{-2})^{-1}. \tag{1}$$

The proof of this equidistribution is elementary in the absence of constraints on the partial quotients. Dealing with this constraint requires some recent results on the distribution of the denominators of fractions with bounded partial quotients ([**3**],[**4**]) . According to these papers, the number of such fractions, with denominator $d \leq x$, is given asymptotically by $C_m x^{D(m)}$ where $C_m, D(m) > 0$. As $D(m) \approx 1.06256$ for $m = 2$ and is increasing in m, there are more than enough such fractions for all large integers to occur as the denominator of such a fraction. Zaremba has conjectured that for some sufficiently large m, this is indeed the case [**8**], [**9**]. The smooth large-scale distribution proved in [**4**] for fractions of this type supports his conjecture, even with $m = 2$. It could well happen, though, that for some reason there are local fluctuations in this distribution so strong that infinitely many denominators are not represented. One possible source of local fluctuations is the prospect that some denominators, those with few small prime factors, occur more often than others. The effect, if it conforms to (1), would not be strong enough to prevent a Poisson process probabilistic model of the distribution in question from issuing an endorsement of the conjecture. As a consequence of our main result, (1) holds as well in the setting of bounded partial quotients, which gives further support to the conjecture: a plausible mechanism by which it might have failed is refuted.

The conjecture has been studied from other perspectives. Borosh [**1**] found computational evidence in favor of the conjecture for $n = 5, 4$, and perhaps 3, but for $m = 2$ there are a multitude of exceptions. On the other hand, the exponent 1.06256 in the asymptotic number of eligible fractions is barely sufficient to permit the truth of the conjecture. The heuristic mentioned above predicts no early end of exceptions in this case. For certain types of numbers, including powers of 2, Niederreiter [**6**] has proved that $m = 3$ works. This resolves a question raised in [**2**]. For a nice survey of 'bounded partial quotients', see [**7**].

2. Terminology and Preliminaries. Fix an integer $m \geq 2$. Let

$$\begin{aligned}(2) \qquad \mathcal{Q}_m(x) := \{\, c/d : 0 \leq c < d \leq x,\ &\gcd(c,d) = 1, \\ &\text{and there exist } r \geq 1, \text{ and } v_i, 1 \leq i \leq r \\ &\text{with } 1 \leq v_i \leq m, (1 \leq i \leq r), v_r > 1, \\ &\text{for which } c/d = [0; v_1, v_2, \dots v_r] \,\}.\end{aligned}$$

Also, let

$$\begin{aligned}(3) \quad &\mathcal{Q}_m(x, a \bmod n, b \bmod n) \\ &\quad := \{c/d : c/d \in \mathcal{Q}_m(x), c \equiv a \bmod n, \text{ and } d \equiv b \bmod n\}, \\ &\quad \mathcal{F}_m := \{v = (v_1, v_2, \dots v_r) : r \geq 1 \\ &\qquad\qquad \text{and } 1 \leq v_i \leq m \text{ for } 1 \leq i \leq r.\}\end{aligned}$$

Given $v \in \mathcal{F}_m$, let $\operatorname{lex}(v)$ denote the r in $v = (v_1, v_2, \dots v_r)$, and let $\langle v \rangle$ be the denominator of $[v] := [0; v_1, v_2, \dots v_r]$. Let $v^- := (v_1, v_2, \dots v_{r-1}), v_- := (v_2, v_3, \dots v_r)$, and $v_-^- := (v_-)^- = (v_2, v_3, \dots v_{r-1})$. Then

$$(4) \qquad [0; v_1, v_2, \dots v_r] = \langle v_- \rangle / \langle v \rangle.$$

Let $\{v\} := \langle v^- \rangle / \langle v \rangle$. Then reversing the sequence gives $[0; v_r, \dots v_1] = \{v\}$.

The four integers $\langle \cdot \rangle$ associated with v are the entries of the matrix

$$(5) \qquad \Gamma(v) := \begin{bmatrix} \langle v_-^- \rangle & \langle v_- \rangle \\ \langle v^- \rangle & \langle v \rangle \end{bmatrix} = \prod_{k=1}^{r} \begin{pmatrix} 0 & 1 \\ 1 & v_k \end{pmatrix},$$

$$\text{and } \det \Gamma(v) = (-1)^r = (-1)^{\operatorname{lex}(v)}.$$

Given $u, v \in \mathcal{F}_m$ with $u = (u_1, u_2, \dots u_r)$ and $v = (v_1, v_2, \dots v_s)$, let uv denote the concatenation $(u_1, u_2, \dots u_r, v_1, v_2, \dots v_s)$. Let u^k denote the concatenation of k copies of u. Then from (5),

$$\langle uv \rangle = \langle u \rangle \, \langle v \rangle (1 + \{u\}[v]). \tag{6}$$

Also, for $u \in \mathcal{F}_m, v \in \mathcal{F}_m$,

$$[\langle uv^- \rangle, \langle uv \rangle] = [\langle u^- \rangle, \langle u \rangle]\Gamma(v), \quad \Gamma(uv) = \Gamma(u)\Gamma(v), \tag{7}$$

$$\text{and } \Gamma(u^k) = (\Gamma(u))^k .$$

Let

$$\Gamma_n(u) := \begin{bmatrix} \langle u_-^- \rangle \bmod n & \langle u_- \rangle \bmod n \\ \langle u^- \rangle \bmod n & \langle u \rangle \bmod n \end{bmatrix}. \tag{8}$$

Then $\Gamma_n(u)$ is an element of the finite group G_n consisting of all two by two matrices over $\mathcal{Z}$ mod n with determinant$\equiv \pm 1$ mod n, with group operation multiplication mod n. Our main theorem asserts equidistribution of $\begin{bmatrix} \langle v_-^- \rangle & \langle v_- \rangle \\ \langle v^- \rangle & \langle v \rangle \end{bmatrix}$ mod n among the elements of G_n. With this, and with the modicum of information about G_n detailed in section 5, we can get the asymptotic distribution among v with $\langle v \rangle < x$ of $\langle v \rangle$ mod n. Though not uniform, it is even enough to support the heuristic argument for Zaremba's conjecture with $m = 2$.

Clearly $\{\Gamma_n(u) : u \in \mathcal{F}_m\}$ is a subgroup of G_n. In fact it is the whole group: In any finite group the set of all nonnegative powers of a fixed element is a subgroup. We take that fixed element here to be $\Gamma_n(1) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, and we take $u^* = 1^{k-1} \in \mathcal{F}_m$ where k is the order in G_n of $\Gamma_n(1)$. Then

$$\Gamma_n(u^*2) \equiv \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } \Gamma_n(2u^*) \equiv \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \tag{9}$$

These two matrices and their inverses generate the subgroup of G_n consisting of matrices of determinant 1, and since $\det \Gamma_n(u) \equiv -1 \bmod n$, the whole of G_n is generated. Now let

$$\mathcal{F}_m(x, u) := \{uw \in \mathcal{F}_m : \langle uw \rangle \le x\}, \quad \text{and} \tag{10}$$

$$\mathcal{F}_m(x,u,v) := \{uwv \in \mathcal{F}_m : \langle uwv \rangle \le x\}.$$

From [**4**] we have the following result:

LEMMA 1. *For every $m \ge 2$, there exists a function $g_m : [0,1] \to [1/4,4]$, twice differentiable, convex, and strictly decreasing, with $-4 < g_m'(t)/g_m(t) < 0$, and positive constants $D(m), K(m)$, such that for every $u \in \mathcal{F}_m$,*

(i) $\lim_{x\to\infty} x^{-D(m)} \# \mathcal{F}_m(x,u) = K(m) \ \langle u \rangle^{-D(m)} g_m(\{u\})/g_m(0)$ *and*

(ii) $\lim\limits_{x\to\infty} x^{-D(m)} \# \mathcal{F}_m(x,u,v)$
$= K(m) \ \langle u \rangle^{-D(m)} \langle v \rangle^{-D(m)} g_m(\{u\}) g_m([v])/(g_m(0))^2.$

These results are not known to hold uniformly across m, or across $u, v \in \mathcal{F}_m$. There is a less exact estimate which does hold uniformly:

LEMMA 2. *There exist constants $C_1, C_2 > 0$ such that given $m \ge 2$ and $u, v \in \mathcal{F}_m$,*

$$x^{-D(m)} \langle u \rangle^{D(m)} \langle v \rangle^{D(m)} \# \mathcal{F}_m(x,u,v) \in [C_1, C_2] \text{ if } x > 4\langle u \rangle \langle v \rangle.$$

This last follows by a short calculation, given below, from Theorem 2 of [**3**] to the effect that for arbitrary $m, x \ge 1$, $\#\mathcal{F}_m(x)$ is comparable to $x^{D(m)}$. For arbitrary u, v we have $\#\mathcal{F}_m(x,u,v) \le \#\mathcal{F}_m(x/(\langle u \rangle \langle v \rangle))$, and $\#\mathcal{F}_m(x,u,v) \ge \#\mathcal{F}_m(x/(4\langle u \rangle \langle v \rangle))$, since if $\langle uwv \rangle \le x$ then $x/(\langle u \rangle \langle v \rangle) \ge \langle w \rangle$ while if $x/(4\langle u \rangle \langle v \rangle) \ge \langle w \rangle$ then $\langle uwv \rangle \le x$.

In the application of (ii), $v = (m1)$. Sequences which end with an "m" followed by a "1" correspond to fractions with final partial quotient $m+1$. Other sequences correspond, in pairs, to individual fractions of $\mathcal{Q}_m$. Thus we first establish equidistribution mod n for general $\mathcal{F}_m(x,u)$ and $\mathcal{F}_m(x,u,m1)$, and then the corresponding equidistribution result for $\mathcal{Q}_m$ is immediate as the $y \in \mathcal{F}_m(x)$ with one-entry endings other than "1" correspond one-to one with elements of $\mathcal{Q}_m(x)$. Our main result, then is

THEOREM 1. *For every integer $m > 1$ and $n > 1$, and for every $u, v \in \mathcal{F}_m$, all possible values of $\Gamma_n(uwv)$, that is, all matrices with determinant $\equiv 1$ or -1 mod n, occur with asymptotically equal frequency among $w \in \mathcal{F}_m$ for which $\langle uwv \rangle \le x$ as $x \to \infty$.*

Let $\Gamma_n(c/d)$ denote $\Gamma_n($ the sequence u of partial quotients of $c/d)$.

COROLLARY 1. *For every integer $m > 1$ and $n > 1$, all possible values of $\Gamma_n(c/d)$, that is, all matrices with determinant $\equiv 1$ or $-1 \bmod n$, occur with asymptotically equal frequency among $c/d \in \mathcal{Q}_m$ for which $0 \le c < d \le x$ as $x \to \infty$.*

3. The tree structure of $\mathcal{F}_m$ and "bouquets". We get a natural tree structure on $\mathcal{F}_m$ if we declare an edge between u and uk whenever $u \in \mathcal{F}_m$ and $1 \le k \le m$. The root of the tree is the empty sequence, denoted " root", with $\langle \text{root} \rangle := 1, [\text{root}] := \{\text{root}\} := 0$. (This is consistent with our earlier definitions.)

A *bouquet* is a subset B of $\mathcal{F}_m$ such that

(I) If $b_1, b_2 \in B$, then b_2 is not a descendant of b_1 in the tree of $\mathcal{F}_m$.

(II) The mapping $b \to \Gamma_n(b)$ is a bijection from B to G_n. (Metaphorically, (II) says that every kind of flower is found once in the bouquet.)

Clearly, if $u, v \in \mathcal{F}_m$, and $\Gamma_n(uBv)$ denotes $\{\Gamma_n(ubv) : b \in B\}$, then

$$\Gamma_n(uBv) = G_n. \tag{11}$$

Now, we need some uniformity in the "stem lengths" $\langle b \rangle$ in our bouquet to make use of (i) and (11) above. Call a bouquet ϵ -balanced if for $b_1, b_2 \in B$,

$$\langle b_1 \rangle \le (1+\epsilon)\ \langle b_2 \rangle,\ |\{b_1\} - \{b_2\}| \le \epsilon, \qquad \text{and } |[b_1] - [b_2]| \le \epsilon. \tag{12}$$

LEMMA 3. *For every $m, n \ge 2$ and every $\epsilon > 0$, there exists an ϵ-balanced bouquet $B \subset \mathcal{F}_m$.*

Proof. We can ensure the second and third conditions in (12) by prefacing and suffixing each element of an arbitrary bouquet with sufficiently many ones, say $N(\epsilon)$ of them (the same number for each element),enough so that

$$\left|\{b\} - \left(\frac{\sqrt{5}-1}{2}\right)\right| \le \frac{\epsilon}{100} \text{ and } \left|[b] - \left(\frac{\sqrt{5}-1}{2}\right)\right| \le \frac{\epsilon}{100}. \tag{13}$$

Now let u_1 denote the sequence $1^{k_1 = \text{order }(\Gamma(1))}$ for which $\Gamma_n(u_1)$ is the identity matrix I, and let u_2 be the corresponding sequence $2^{k_2 = \text{order }(\Gamma(2))}$. A little algebra shows that there are positive constants J_1 and J_2 so that

$$(14) \qquad \langle 1^k \rangle = J_1 \left(1 + O\left(\frac{\sqrt{5}+1}{2}\right)^{-k}\right)\left(\frac{\sqrt{5}+1}{2}\right)^k$$

$$\text{and } \langle 2^k \rangle = J_2 \left(1 + O(\sqrt{2}-1)^k\right)(1+\sqrt{2})^k$$

Now given a bouquet B, not necessarily ϵ-balanced, we consider the problem of choosing k_i and $j_i, 1 \le i \le \#G_n = \#B$ so that all values of

$$\langle 1^{N(\epsilon)} b_i u_1^{k_i} u_2^{j_i} 1^{N(\epsilon)} \rangle$$

fall within a factor of $(1 \pm \epsilon)$ of each other. We assume $k_i, j_i \ge N(\epsilon)$. Now with $\lambda_1 := (\sqrt{5}+1)/2$ and $\lambda_2 := 1 + \sqrt{2}$, from (5) and (14) it follows that

$$\begin{aligned}(15) \quad \langle 1^{N(\epsilon)} b_i u_1^{k_i} u_2^{j_i} 1^{N(\epsilon)} \rangle &= \langle 1^{N(\epsilon)} b_i \rangle \; \langle u_1^{k_i} \rangle \langle u_2^{j_i} \rangle \; \langle 1^{N(\epsilon)} \rangle \\ &\cdot \left(1 + \{1^{N(\epsilon)} b_i\}[u_1^{k_i}]\right)\left(1 + \{u_1^{k_i}\}[u_2^{j_i}] + O(\epsilon/50)\right) \\ &\cdot \left(1 + \{u_2^{j_i}\}[1^{N(\epsilon)}] + O(\epsilon/50)\right) \\ &= \left((1 + \{1^{N(\epsilon)} b_i\}\lambda_1^{-1})(1 + \lambda_1^{-1}\lambda_2^{-1})^2 + O(\epsilon/10)\right) \\ &\quad \cdot \langle 1^{N(\epsilon)} b_i \rangle \; \langle 1^{N(\epsilon)} \rangle \; J_1 J_2 \lambda_1^{k_i \operatorname{lex}(u_1)} \lambda_2^{j_i \operatorname{lex}(u_2)}.\end{aligned}$$

Extracting common factors, it will suffice to take k_i and j_i so that for all choices of i_1 and i_2, if a_1 denotes

$$\log\langle 1^{N(\epsilon)} b_{i_1} \rangle + k_{i_1} \operatorname{lex}(u_1) \log \lambda_1 + j_{i_1} \operatorname{lex}(u_2) \log \lambda_2$$

and a_2 denotes

$$\log\langle 1^{N(\epsilon)} b_{i_2} \rangle + k_{i_2} \operatorname{lex}(u_1) \log \lambda_1 + j_{i_2} \operatorname{lex}(u_2) \log \lambda_2$$

then

$$(16) \qquad |a_1 - a_2| \le \epsilon/10.$$

But $(\log\lambda_2)/(\log\lambda_1)$ is irrational, since there is no solution in positive integers to $\lambda_1^j = \lambda_2^k$. Thus the sequences

$$\left(\frac{-\log\langle 1^{N(\epsilon)} b_i\rangle}{\operatorname{lex}(u_1)\log\lambda_1} + j\frac{\operatorname{lex}(u_2)\log\lambda_2}{\operatorname{lex}(u_1)\log\lambda_1}\right) \tag{17}$$

all contain infinitely many elements which, modulo 1, fall between 0 and $\epsilon/100$. For each i we take j_i to be such a j, and larger than $N(\epsilon)$. Then we choose k_i to put the integer parts of

$$\left(\frac{-\log\langle 1^{N(\epsilon)} b_i\rangle}{(\operatorname{lex}(u_1)\log\lambda_1)} + j_i\frac{\operatorname{lex}(u_2)\log\lambda_2}{\operatorname{lex}(u_1)\log\lambda_1} + k_i\right) \tag{18}$$

into agreement, and if necessary, we then add some constant to each k_i to bring all of them up to more than $N(\epsilon)$.

This procedure generates a set

$$B' := \{1^{N(\epsilon)} b_i u_1^{k_i} u_2^{j_i} 1^{N(\epsilon)} : 1 \le i \le \#G_n\}$$

which is ϵ-balanced by its construction, and still, by (11), a bouquet like B. This proves lemma 3. □

4. A limiting process. Let $\mathcal{F}_m(x, U, v) := \{y \in \mathcal{F}_m : \exists u \in U, w \in \mathcal{F}_m$ so that $y = uwv$ and $\langle uwv\rangle \le x\}$. Now for fixed $u, v \in \mathcal{F}_m$, we have from (ii) of lemma 1 an asymptotic formula for $\#\mathcal{F}_m(x, u, v)$. From this and the definition of an ϵ-balanced bouquet B, it follows that the values of Γ_n are distributed uniformly to within a factor of $(1 \pm 3\epsilon)$ on $\cup_{b\in B}\mathcal{F}_m(x, ub, v) = \mathcal{F}_m(x, uB, v)$. Now among all sequences $uwv \in \mathcal{F}_m$, we claim that these represent asymptotically a positive fraction of all of $\mathcal{F}_m(x, u, v)$. Indeed, from lemma 2, if $x > 4\langle ub\rangle\langle v\rangle$ for all $b \in B$ then since $\langle ub\rangle \le 2\langle u\rangle\langle b\rangle$ and since $0 < D(m) < 2$,

$$\begin{aligned}\frac{\#\mathcal{F}_m(x, ub, v)}{\#\mathcal{F}_m(x, u, v)} &\ge (C_1/C_2)\langle ub\rangle^{-D(m)}\langle u\rangle^{D(m)} \\ &\ge (C_1/C_2)(2\langle b\rangle)^{-D(m)}\end{aligned} \tag{19}$$

or equivalently, there exists $\delta > 0$ such that for all $u, v \in \mathcal{F}_m$, all $\epsilon > 0$ and all ϵ-balanced bouquets B, if $b \in B$ and $x > 8\langle u\rangle\langle b\rangle\langle v\rangle$ then

$$\#\mathcal{F}_m(x, uB, v) \ge \delta\#\mathcal{F}_m(x, u, v). \tag{20}$$

We have our foot in the door: near-uniform distribution holds on a nonzero percentage of $\mathcal{F}_m(u,v)$. The remaining sequences are the ones w of the form $w = uw'v$ where w' does not have the form bw'' for any $b \in B$. The strategy is that we can group these, too, into packages of the form $\mathcal{F}_m(urB, v)$ on which near-uniform distribution of values of Γ_n occurs.

Let $S_1 := B$, $R_1 := \{\text{"root"}\}$ (the set, that is.). Recursively define

$$(21)\, R_i := \{v \in \mathcal{F}_m : \begin{array}{l} \text{if } uw = v \text{ then } u \notin S_j \text{ for } j < i \text{ and} \\ \text{if } w \in \mathcal{F}_m \text{ then } vw \notin S_j \text{ for } j < i \text{and yet} \\ \exists w \in \mathcal{F}_m : v^{-}w \in S_j \ \text{ for some } j < i\}, \end{array}$$
$$\text{and} \qquad S_i := S_{i-1} \cup (\cup_{r \in R_i} rB)\,.$$

That is, R_i is the set of all v so that neither v, nor any ancestor or descendant, belongs to a prior S_j, but v^{-}, the parent of v, does have some (other) descendant belonging to a prior S_j.

Thus B and R_1 are disjoint, and for every $w \in \mathcal{F}_m$ with $\operatorname{lex}(w) \geq \max_{b\in B} \operatorname{lex}(b)$ there is a unique representation $w = cw'$, with $c \in B \cup R_1$. Similarly, for every $j \geq 1$ and every $w \in \mathcal{F}_m$ with sufficiently large $\operatorname{lex}(w)$, there is a unique representation $w = cw'$ with $c \in S_j \cup R_j$, and $S_j \cap R_j = \phi$. For every j and every $r \in R_j$, the values of Γ_n are approximately uniformly distributed on $\mathcal{F}_m(urb, v)$, and so also on $\cup_{r\in R_j} \mathcal{F}_m(urB, v) = \mathcal{F}_m(uRB, v)$ for x sufficiently large.

Apart from these uniformly distributed "packages" of the form $\{urbwv : \langle urbwv \rangle \leq x,\ r \in R_j, \text{ and } b \in B\}$, there are sequences $uw'v$ not of the form $rbwv$. These are distributed by Γ_n into G_n in an unknown way. On the other hand , for large j and x they are, we shall see, vanishingly rare as a proportion of $\mathcal{F}_m(x, u, v)$.

To prove this, we start with the weaker claim that there is a $\delta = \delta(B) > 0$ such that for all $b \in B$, all y,$v \in \mathcal{F}_m$ and $x > 8\langle yb\rangle\langle v\rangle$,

$$\frac{\#\mathcal{F}_m(x, yB, v)}{\#\mathcal{F}_m(x, y, v)} \geq \delta. \tag{22}$$

To establish (22) we refer to Lemma 2. From that lemma,

$$\#\mathcal{F}_m(x, y, v) \ll x^{D(m)}\langle y\rangle^{-D(m)}\ \langle v\rangle^{-D(m)},$$

while

$$\#\mathcal{F}_m(x, yB, v) \gg (\#G_n)\ \langle b\rangle^{-D(m)} x^{D(m)}\langle y\rangle^{-D(m)}\ \langle v\rangle^{-D(m)},$$

where b is an arbitrary element of B. (The implicit constants in "$\gg$" here are independent of y, v, B, or m.)

Now let $\mathcal{F}_m(x, y\overline{B}, v)$ denote that subset of $\mathcal{F}_m(x, y, v)$ consisting of all $z \in \mathcal{F}_m(x)$ of the form $z = ycv$ with c *not* of the form bw for any $b \in B$. Since $\mathcal{F}_m(x, yB, v) \cap \mathcal{F}_m(x, y\overline{B}, v) = \phi$, for large x,

$$\text{(23)} \qquad \frac{\#\mathcal{F}_m(x, y\overline{B}, v)}{\#\mathcal{F}_m(x, y, v)} \leq 1 - \delta, \text{ and}$$

$$\frac{\sum_{r \in R_j} \#\mathcal{F}_m(x, ur\overline{B}, v)}{\sum_{r \in R_j} \#\mathcal{F}_m(x, ur, v)} \leq 1 - \delta.$$

But from the definitions of $\overline{B}$ and of R_{j+1},

$$\text{(24)} \qquad \mathcal{F}_m(x, ur\overline{B}, v) = \bigcup_{\{\tilde{r} : r\tilde{r} \in R_{j+1}\}} \mathcal{F}_m(x, r\tilde{r}, v)$$

$$\text{so that } \sum_{r \in R_{j+1}} \#\mathcal{F}_m(x, ur, v) \leq (1 - \delta) \sum_{r \in R_j} \#\mathcal{F}_m(x, ur, v).$$

From (24) though, it follows that

$$\text{(25)} \qquad \lim_{j \to \infty} \left(\overline{\lim_{x \to \infty}} \frac{\#\mathcal{F}_m(x, uR_j, v)}{\#\mathcal{F}_m(x, u, v)} \right) = 0.$$

That is, the exceptional sequences, those not belonging to any S_i, are vanishingly rare as a proportion of $\#\mathcal{F}_m(x, u, v)$ as $x \to \infty$. The equidistribution of $\mathcal{F}_m(x, u, v)$ among the various values in G_n of $\Gamma_n(\cdot)$ is now immediate. This completes the proof of theorem 1.

5. Elementary observations about G_n. Not all pairs (c, d) occur as rows of elements of G_n, nor do all values of d occur with equal frequency. Thus, the distribution of $(c \bmod n, d \bmod n)$ in $\mathcal{Q}_m(x)$ cannot be expected to be uniform. Instead, we have the following arithmetic. Proofs are all routine and the details are left to the reader.

$$\text{(26)} \qquad \begin{aligned} &\#\{(c \bmod n, d \bmod n) : \\ &\quad \gcd(\gcd(c, n), \gcd(d, n)) = 1\} \\ &= n^2 \sum_{a \mid n} \frac{\mu(a)}{a^2} = n^2 \prod_{p \mid n} (1 - p^{-2}). \end{aligned}$$

Given (c mod n, d mod n) with $n > 2$ and

$$\gcd(\gcd(c,n), \gcd(d,n)) = 1,$$

there are $2n$ matrices $M = \begin{bmatrix} c & d \\ e & f \end{bmatrix} \bmod n$ for which $\det M \equiv \pm 1 \bmod n$. (If $n = 2$ there are two for each pair $(1,0)$, $(0,1)$ and $(1,1)$.)

$$\#G_n = 2n^3 \prod_{p|n} (1 - p^{-2}). \tag{27}$$

Given d mod n,

$$\begin{aligned} &\#\{c \bmod n : \gcd(\gcd(c,n), \gcd(d,n)) = 1\} \\ &\quad = n \prod_{p|\gcd(d,n)} \left(1 - \frac{1}{p}\right). \end{aligned} \tag{28}$$

Given d mod n with $n > 2$,

$$\begin{aligned} &\#\left\{(c,e,f) \bmod n : \begin{bmatrix} c & d \\ e & f \end{bmatrix} \bmod n \in G_n\right\} \\ &\quad = 2n^2 \prod_{p|\gcd(d,n)} \left(1 - \frac{1}{p}\right). \end{aligned} \tag{29}$$

(If $n = 2$, there are two matrices for $d \equiv 0$ and four for $d \equiv 1$.)

$$\begin{aligned} &(1/\#G_n)(\#\{\gamma \in G_n : \\ &\quad \gamma \text{ has } d \text{ in the upper right entry }\}) \\ &\quad = \frac{1}{n} \prod_{p|\gcd(d,n)} (1 - 1/p) \prod_{q|n} (1 - 1/q^2)^{-1}. \end{aligned} \tag{30}$$

From all this and the equidistribution theorem for $\mathcal{Q}_m$ we have the following corollaries:

COROLLARY 2. *As $x \to \infty$, for $\gcd(\gcd(c,n), \gcd(d,n)) = 1$,*

$$\begin{aligned} &\#\{(c'/d') \in \mathcal{Q}_m(x) : (c' \equiv c \bmod n, d' \equiv d \bmod n)\} \\ &\quad \approx \left(n^{-2} \prod_{q|n} (1 - q^{-2})^{-1}\right) \#\mathcal{Q}_m(x). \end{aligned} \tag{31}$$

COROLLARY 3. *Under the same conditions as in corollary 2 above,*

$$(32)\qquad \#\{(c'/d') \in \mathcal{Q}_m(x) : d' \equiv d \ mod\ n\}$$
$$\approx \left(n^{-1} \prod_{p|\ gcd\ (d,n)} (1-p^{-1}) \prod_{q|n} (1-q^{-2})^{-1} \right)$$

and likewise for fixed c' mod n.

REFERENCES

[1] I.Borosh, *Rational continued fractions with small partial quotients*, Notices Amer. Math. Soc. **23**:A-52, 1976. Abstracts 731-10-29.

[2] I.Borosh, H.Niederreiter, *Optimal multipliers for pseudo-random number generation by the linear congruential method*, BIT **23**:65-74, 1983.

[3] D. Hensley, *The distribution of badly approximable numbers, and continuants with bounded digits*, Number Theory, Proc. Intl. Number Theory Conf. , Quebec (1987), DeGruyter (1989), 371-385.

[4] D. Hensley, *The distribution of badly approximable rationals and continuants with bounded digits*, II, J. of Number Theory, **34** (1990), 293-334.

[5] D. E. Knuth, *Seminumerical Algorithms*, vol. II of The Art of Computer Programming, Addison-Wesley, 1981.

[6] H. Niederreiter, *Dyadic fractions with small partial quotients*, Monatshefte Math. **101** (1986), 309-315 .

[7] J. Shallit, *Real Numbers with Bounded Partial Quotients: A Survey*, L'Enseignement Mathèmatique, vol. **38** (1992), 151-187.

[8] S. K. Zaremba, *Good lattice points, discrepancy, and numerical integration*, Ann. Mat. Pure Appl. **73** (1966), 293-317.

[9] S. K. Zaremba, *La m'ethode des "bon treillis" pour le calcul des int'egrales multiples*, in S. K. Zaremba, editor, Applications of Number Theory to Numerical Analysis, Academic Press, NY, 1972, 39-119.

Received October 11, 1991 and accepted for publication October 4, 1993.

TEXAS A & M UNIVERSITY
COLLEGE STATION, TX 77843-3368.