Density and multiplicative structure of sets of integers

by

RAJAHN ALEXANDER (Urbana, Ill.)

0. Introduction. The main purpose of this paper is to extend the theory, begun by P. Erdős together with H. Davenport, of the logarithmic density of sequences of natural numbers. However, our method will give information on natural density, as well as on certain other asymptotic densities. (The reader unfamiliar with density theory will find the necessary definitions in Section One.)

Erdős and Davenport [3], [4] proved that for any set $M$ of natural numbers, the set $D(M)$ consisting of all numbers divisible by at least one member of $M$ possesses a logarithmic density. Earlier, Besicovitch [2] had shown that $D(M)$ need not possess a natural density. He also proved that a sequence having the property that no member divides another need not have zero natural density. Erdős [5] and Behrend [1] showed that such a sequence does possess zero logarithmic density, hence zero lower natural density. Using their result on $D(M)$, Erdős and Davenport proved that any sequence which does not have zero logarithmic density contains a division chain, that is, an infinite subsequence for which each member divides its successor.

The papers cited above tend to show that logarithmic density is a more accurate indicator of multiplicative structure than is natural density.

Section One of this paper consists of elementary results whose application to natural density is well known. In Section Two, we introduce a decomposition of a sequence which allows us to apply the ideas of Section One to logarithmic density. Finally, in Section Three, we sharpen the results of Erdős and Davenport on $D(M)$ and on division chains, and obtain new information on special division chains which exist in sets with positive natural density. For instance, if a sequence $C$ has positive natural density, then $C$ contains a subsequence $g_1, g_2 g_1, g_3 g_2 g_1, \ldots$ such that $g_{n+1}$ is divisible only by primes greater than $g_n$ raised

* The material in this paper is part of the author's doctoral dissertation submitted to Purdue University.
to the power $\log \log(q_1, \ldots, q_l)$. Also, our method will lead to a theorem, which complements a theorem of Erdős [7], on the irregularity of the prime divisors of almost all integers.

1. Basic definitions and ideas of asymptotic density.

1.1. Definition. Let $(\mu_k)$ be a sequence of countably additive measures on the subsets of $N$, the natural numbers. Assume limit $\mu_k N = 1$. Define $\mu^*(A) = \limsup \mu_k A$ and $\mu_*(A) = \liminf \mu_k A$ for $A$ in $N$. If $\mu^* A = \mu_* A$, let $\mu$ denote this number, and say that $A$ possesses $\mu$-density.

The following model will give all of the asymptotic densities which will interest us.

1.2. Definition. Let $(\epsilon_i)$ be an arbitrary sequence of positive real numbers. For $A$ in $N$, define

$$\mu(A) = \sum_{i=1}^{k} \epsilon_i (\mu^*_i, i \leq k) \sum_{i=1}^{k} \epsilon_i.$$ (1)

Natural density $\delta$ is obtained when $\epsilon_i = 1$ for each $i$, and logarithmic density $\epsilon$ is obtained when $\epsilon_i = \epsilon^{-i}$. For $l$ it is convenient to replace the denominator of (1) by $\log k$. We will always assume that functions involving the logarithmic function are suitably redefined for certain small values of the argument.

The following theorem is stated without proof.

1.3. Theorem. (a) If $A \subseteq B$, then $\mu_\leq A \leq \mu_\leq B$ and $\mu^* A \leq \mu^* B$.

(b) If $C \subseteq A \subseteq B$, then $\mu^* C \leq \mu^* A \leq \mu^* B$.

(c) If $A$ and $B$ are disjoint sets with $\mu$-density, then $\mu(A \cup B) = \mu(A) + \mu(B)$.

(d) If $A$ and $B$ possess $\mu$-density and $A \subseteq B$, then $\mu(B-A) = \mu(B) - \mu(A)$.

1.4. Definition. The sequence $(\epsilon_i)$ is called $\mu$-summable if $\mu F$ exists and $\mu F = \lim \mu F_j$. Since asymptotic densities are far from being countably additive set functions, $\mu$-summability is a strong condition.

1.5. Theorem. We always have limit $\mu F_j \leq \mu F$.

Proof. Since $\mu F_j \leq \mu F_{j+1}$, limit $\mu F_j$ exists. By 1.3(a), $\mu F_j \leq \mu F$ for each $j$. The result follows.

1.6. Corollary. If limit $\mu F_j = 1$, $\mu F = 1$.

Proof. Clearly, limit $\mu F_j \leq \mu F \leq \mu F \leq 1$.

1.7. Theorem. Suppose that there is a sequence of constants $(\epsilon_i)$, with $\sum \epsilon_i$ converging, so that for all $i$ and $k$, $\mu_\leq E_i \leq \epsilon_i$. Then $(\epsilon_i)$ is $\mu$-summable.

Proof. We only need show that $\mu F \leq \lim \mu F_j$, because of 1.5. For any $j$ and $k$ we have

$$\mu_\leq (F-F_j) = \mu F - \mu F_j \leq \sum_{i=1}^{\infty} \epsilon_i E_i \leq \sum_{i=1}^{\infty} \epsilon_i = R_i.$$ (4)

Thus for each $j$, $\mu^* F \leq \mu F_j \leq R_i$. The result follows.

1.8. Corollary. Suppose that $(\epsilon_i)$ is a sequence of pairwise disjoint sets. If $\mu_\leq E_i \leq \epsilon_i$ for all $i$ and $k$, then $(\epsilon_i)$ is $\mu$-summable.

Proof. Certainly $\sum \mu E_i \leq 1$. Put $E_i = E_i$ in 1.7.

1.9. Example. If $a = (a_1 < a_2 < \ldots)$, then $D(a_i)$, as defined previously, equals $\bigcup D(a_i)$. It is easily seen that, for any $i < k$, $\delta(\bigcup D(a_i)) \leq 1/\epsilon_i$. Thus if $\sum \delta(\bigcup D(a_i))$ converges, $\delta(\bigcup D(a_i)) = \lim \delta(\bigcup D(a_i))$ by 1.7.

In the special case where the $a_i$ are pairwise relatively prime, a routine computation shows that $\delta(\bigcup D(a_i)) = 1 - \prod (1 - 1/\epsilon_i)$.

1.10. Theorem. Let $(\epsilon_i)$ be $\mu$-summable with $G$ contained in $F$. If $\mu (G \cap E_i) = 0$ for each $i$, $\mu F = 0$.

Proof. Let $G_i = G \cap F_i$. Certainly $\mu F_i = 0$. We have $\mu G = \mu F - \mu (G \cap E_i) = \mu F - \mu F_i$. Since $\mu F_i = \mu F_i$, $\mu G = 0$.

1.11. Theorem. Let $(\epsilon_i)$ and $(\delta_i)$ be sequences of positive real numbers. Let $\epsilon$ and $\delta$ be the asymptotic densities induced by these sequences as in 1.2. Suppose that (i) $\sum \epsilon_i$ and $\sum \delta_i$ are divergent, and (ii) $\epsilon_i/\delta_i$ is monotone nonincreasing as $i$ increases. Then for any $A$,

$$\epsilon_i A \leq \delta_i A \leq \epsilon_i A \leq \delta_i A.$$ (5)

Proof. This is a well-known theorem on Norlund means. A complete discussion can be found in Hardy [8].

1.12. Corollary. For any $A$, $\delta_i A \leq \epsilon_i A \leq \epsilon_i A \leq \delta_i A$.

2. The properties of a certain multiplicative decomposition. In this section we shall always assume that $C = (c_1 < c_2 < \ldots)$ is an infinite set of natural numbers for which $c_i \geq 1$. Any sequence of integers will be increasing unless otherwise stated.

2.1. Lemma. If $p$ denotes a prime number, we have the inequalities

$$\log x < \prod ((1 - 1/p)^{-1}: p \leq x, x > 2) < M \log x,$$

where $M$ is an absolute constant.

2.2. Definition. If \( n \geq 1 \), let \( P(x) \) be the set of all natural numbers that are composed entirely of primes greater than \( x \).

2.3. Lemma. If \( a \) is any natural number and \( x \geq 2 \), then \( \delta(aP(x)) = (1/a) \int_{1}^{a} \left( 1 - \frac{1}{p} \right) \, dp \leq a \).

Proof. Note that \( E = N - P(x) \) consists of those numbers divisible by a prime not greater than \( x \). Hence, by 1.9, \( \delta E = 1 - \int_{1}^{a} \left( 1 - \frac{1}{p} \right) \, dp \leq a \). The result follows at once.

2.4. Definition. Let \( \Gamma \) be the family of all arithmetic functions \( f \) which satisfy \( f(n) \geq g(n) \) for \( n = 2, 3, \ldots \), where \( g(n) \) is the greatest prime divisor of \( n \).

2.5. Definition. Let \( C \) be a set of natural numbers and let \( f \) be an arbitrary member of \( \Gamma \). The \( f \)-primary part of \( C \), denoted by \( A(f, C) \), is defined to be the collection \( \{ a; c \in \epsilon \, f(c) \} \) for any \( f \). The \( f \)-secondary part of \( C \), denoted by \( B(f, C) \), is defined to be \( C - A(f, C) \). If there is no possibility of confusion, the sets just defined will be called \( A \) and \( B \), respectively.

The decomposition of \( C \) given in 2.5 together with the following representation theorem forms the basis of our method.

2.6. Theorem. Let \( f \) belong to \( \Gamma \) and \( f \) belong to \( \Gamma \). Then either \( c \) belongs to \( A \) or \( c \) may be uniquely represented as \( c = a \cdot s \), where \( a \) belongs to \( A \) and \( s \) belongs to \( P(a) \).

Proof. Suppose that \( c \) is an element of \( B \). Then \( c = q_{1}q_{2} \), where \( q_{1} \), belongs to \( P(f(c)) \) for at least one \( c_{1} \). Let \( c_{1} \) be the least member of \( C \) which satisfies this condition. If \( a_{1} \) does not belong to \( A \), then \( c_{1} = c_{1} \cdot s_{1} \), where \( s_{1} \) is contained in \( P(f(c)) \); and \( c = c_{1} \cdot s_{2} \cdot s_{3} \). Since \( f(n) \geq g(n) \), \( s_{2} \cdot s_{3} \) belongs to \( P(f(c)) \), and we have a contradiction. Thus \( c \) has at least one representation in the desired form.

To demonstrate the uniqueness of the representation, we prove that if \( a_{1} \) and \( a_{2} \) are distinct members of \( A \), then the sets \( a_{1}P(f(a_{1})) \) and \( a_{2}P(f(a_{2})) \) are actually disjoint. Suppose \( a_{1} \cdot s_{1} = a_{2} \cdot s_{2} \) (this number need not belong to \( C \)), where \( s_{1} \) is in \( P(f(a_{1})) \) and \( s_{2} \) is in \( P(f(a_{2})) \). We may assume without loss of generality that \( g(a_{1}) \) does not exceed \( g(a_{2}) \). Then \( a_{1} \cdot s_{1} \) and \( a_{2} \cdot s_{2} \) are relatively prime, and hence \( a_{1} = a_{2} \cdot s_{2} \). Since \( s_{1} \neq 1 \), \( s_{2} \) is contained in \( P(f(a_{1})) \) because \( s_{2} \) divides \( s_{1} \). This contradicts the definition of \( A \).

2.7. Examples. (i) Let \( C = \{ 2, 3, 4, \ldots \} \) and \( f(n) = g(n) \). We easily see that \( A \) consists of all powers of prime numbers. In fact for any \( C \) and \( f \), \( A \) will always contain the least member of \( C \) and any prime powers which happen to lie in \( C \).

(ii) Let \( C \) be a sequence for which no number divides another. Certainly \( A = C \) for any \( f \).

(iii) Let \( C = \{ a^{n} \} \) for an integer \( d > 1 \) and \( f(n) = n \). It is seen that \( A \) contains \( d \) together with numbers of the form \( ds \) where \( s \) is composed of primes not greater than \( d \). However, many other numbers belong to \( A \).

(iv) Let \( C = \{ 2, 3, 4, \ldots \} \) and \( f(n) = g(n) + 2 \). Here \( A \) is made up of powers of primes together with numbers \( p^{n} q^{n} \) where \( p \) and \( q \) are prime twins.

(v) Let \( C = \{ p + q; \, t = 0, 1, \ldots, \tau, s = 1, f = g \} \). In this situation \( A \) cannot be described in a simple structure; Dirichlet’s theorem at least says that \( A \) contains infinitely many primes.

It is obvious that if \( f_{1}(n) \leq f_{2}(n) \) for each \( n \), then \( A(f_{1}, C) \subset A(f_{2}, C) \) for any \( C \). Questions about the fine structure of \( A \) are very difficult, but we can say quite a bit about the density of \( A \) under a wide range of conditions.

The next theorem exploits an idea first used by Erdős [5].

2.8. Theorem. Let \( f \) belong to \( \Gamma \), and let \( C \) be arbitrary. Then we have

\[ \sum_{\epsilon \in A} \frac{1}{\epsilon} \leq M, \]

where \( M \) is the constant in 2.1.

Proof. In the demonstration of 2.6, we proved that if \( i \) and \( j \) are distinct, then \( \epsilon_{i}P(f(\epsilon_{i})) \) and \( \epsilon_{j}P(f(\epsilon_{j})) \) are disjoint sets. By 2.3, \( \delta \epsilon_{i}P(f(\epsilon_{i})) = (1/a) \left( 1 - \frac{1}{p} \right) \, dp \leq \epsilon_{i} \). Hence by 2.1 this number is greater than \( 1/a_{n} \log f(a_{n}) \). Since the sum of the densities of a collection of disjoint sets does not exceed one, we may conclude that for any \( n \),

\[ \sum_{\epsilon_{i} = \epsilon} \frac{1}{\epsilon} \leq 1. \]

If need be, we allow \( a \) to tend to infinity to obtain the result.

2.9. Definition. We define \( \Gamma' \) to be those \( f \) in \( \Gamma \) for which there exists a real number \( K = K(f) \) such that \( f(n) \leq K^{n} \) for each \( n \).

2.10. Theorem. Let \( C \) be arbitrary set of natural numbers. If \( f \) belongs to \( \Gamma' \), then \( L = 0 \).

Proof. Assume that \( A \) is infinite, and let \( K \) satisfy \( f(n) \leq n^{K} \). Then since \( \log f(n) \leq K \log n \), it follows that

\[ \sum_{\epsilon_{i} = \epsilon} \frac{1}{\epsilon} \leq KM. \]

Next choose \( k \) so that \( \sum_{\epsilon_{i} = \epsilon} \frac{1}{\epsilon} < \epsilon/2 \). Now if \( n \) is so large that

\[ (1/\log n) \sum_{\epsilon_{i} = \epsilon} \frac{1}{\epsilon} < \epsilon/2, \]

then...
The next theorem, which relates the decomposition to $l$-summability, is our principal result on the density of $B(f, \infty)$.

2.16. Theorem. Let $\Gamma$ be a set of natural numbers and let $f$ be any element in $\Gamma$. Suppose that \[ |C \cap \alpha P(f(a))| \leq |C| \] exists for each $a$ in $A$. Then the sequence of sets \[ C \cap \alpha P(f(a)) \] is $l$-summable. In other words, $\sum l |C \cap \alpha P(f(a))|$ exists and is equal to $\sum l |C \cap \alpha P(f(a))|$. 

Proof. If $\Omega$ is finite, the result is clear by the finite additivity of $l$. If $\Omega$ is infinite, let $a$ be a fixed member of $\Omega$, and consider the following series of inequalities:

\[
\sum |1| \leq |C \cap \alpha P(f(a))|, b \leq n
\]

\[
\leq \sum |1| \leq |C \cap \alpha P(f(a))|, b \leq n
\]

\[
\leq (1/a) \prod (1 - \log p)^{-1}; f(a) < p \leq n \quad \text{(by 2.15)}
\]

\[
= (1/a) \prod (1 - \log p)^{-1}; f(a) < p \leq n
\]

Thus for any $a$ and $n$,

\[
l_0 |C \cap \alpha P(f(a))| \leq M (a \log f(a))^{-1} = L_0.
\]

We know from 2.8 that $\sum L_0 < \infty$. We may now apply 1.7 to conclude that the family of sets is $l$-summable.

2.17. Corollary. If $lA = 0$ and if $|C \cap \alpha P(f(a))|$ exists for each $a$ in $A$, then $l0 = \sum |C \cap \alpha P(f(a))|$. 

Proof. By 2.16, $lB$ exists and equals the above sum. Since $lA = 0$, $lB = 0$.

The following is an obvious special case.

2.18. Corollary. If $f$ belongs to $\Gamma$' and $l |C \cap \alpha P(f(a))| = 0$ for each $a$ in $A$, then $l0 = 0$.

2.19. Remark. The above results give us a two-fold attack on a sequence $C$ since the convergence of $\sum |a \log f(a)|^{-1}$ gives information on $A$, and the $l$-summability of the sets $|a \log f(a)|$ gives information on $B$.

3. Some applications of the decomposition.

3.1. Definition. A set of natural numbers $C$ will be called a multiplicative set if $C = D(M)$ for a set of natural numbers $M$ which does not contain 1.

3.2. Definition. An infinite set $C$ will be called a division chain if $c_i$ divides $c_{i+1}$ for each $i$. 

3.3. Theorem (Erdős, Behrend). If C has the property that no member divides another, then $I'C = 0$.

Proof. Let $f = g$, a member of $I'$. Here $A = C$, and $I'C = 0$ by 2.10. We can easily strengthen 3.3. The following is a simple example of the method mentioned in 2.19.

3.4. Theorem. If C has the property that each member of C divides only finitely many members of C, then $I'C = 0$.

Proof. Let $f = g$ so that $I'A = 0$. Note that $I'(a) = aP(|f(a)|) = 0$ for each $a$ in $A$ since the set intersection must be finite. Apply 2.16.

3.5. Lemma. If C is a multiplicative set and $f$ is any member of $I'$, then $I'B = \sum |aP(f(a))| = a + A$.

Proof. Since C is multiplicative, $C \cap aP(f(a)) = aP(f(a))$. Now $|aP(f(a))| = aP(|f(a)|)$, and we may apply 2.16.

3.6. Theorem (Erdős-Davenport). Let $C'$ be a multiplicative set. Then $I'C = 0$ exists and equals $I'C$.

Proof. Let $f = g$, so that $I'A = 0$; $I'B$ exists by 3.5. Thus $I'C$ exists. We know $I'C \leq I'C = \sum |aP(f(a))|$. Also, $I'C = I'B = \sum |aP(f(a))|$. The last inequality follows from 1.5.

3.7. Corollary. If $C$ is a multiplicative set and $f$ is any member of $I'$, then $I'A = 0$.

Proof. We know that $I'B$ and $I'C$ exist by 3.5 and 3.6, respectively. Hence $I'A = I'C = I'B$.

3.8. Remark. Another proof of 3.6 can be made along the following line: Any multiplicative set can be written as a disjoint union of arithmetic progressions so that the collection of least members of these progressions has the property that any one divides at most finitely many others. This collection has zero logarithmic density by 3.3. It is an easy consequence of 1.8 that this union possesses the desired density.

3.9. Theorem. Let $C$ be a multiplicative set, and let $f$ belong to $I'$. Then $I'A = 0$.

Proof. By 2.14 we know that $I'A = 0$. Since $C$ is multiplicative, $I'A$ exists and therefore must be zero.

We now prove three theorems about division chains. The first two sharpen the result of Erdős and Davenport mentioned in the introduction; the third needs a stronger hypothesis, which certainly would be satisfied by a set with positive natural density.

3.10. Theorem. Let $K_1, K_2, \ldots$ be any sequence of positive numbers. If $C$ does not possess zero logarithmic density, then $C$ contains a division chain of the form $g_1, g_2, g_3, \ldots$, where $g_i$ is composed entirely of primes greater than $\alpha_1g_1 \cdots g_i$.

Proof. For each $i$, $\alpha_i(n) = n^\alpha_i$ belongs to $I'$. Now there exists $\alpha_1$ in $A(f_i)$ so that $I'C = 0$, where $C = C \cap aP(f_i(a))$. Otherwise, $I'C = 0$ by 3.8. Likewise, there exists $\alpha_2$ in $A(f_i, C_3)$ so that $I'C_3 = 0$, where $C_3 = C_1 \cap aP(f_i(a))$. Continuing inductively, we construct the sequence $\alpha_1, \alpha_2, \ldots$. It is seen from the construction that $\alpha_{i+1} = \alpha_i + \alpha_i$, where $\alpha_i$ belongs to $P(f_i(a))$. Set $\alpha_1 = g_1$ and $\alpha_{i+1} = g_i$ for $i > 1$. Thus $\alpha_i = g_i$.

3.11. Theorem. Suppose that $I'C = 0$, and that $\{f_i\}$ is an arbitrary sequence of functions in $I'$. Then $C$ contains a division chain of the form $r_1, r_2, \ldots$, where $g_i$ belongs to $P(f_i(r))$ and $r_1$ divides $r_i$, for each $i$.

Proof. If $M = D(E)$ is any multiplicative set, then we know that $I'(f_i, M) = 0$ for each $i$, by 3.9. Thus there exists $\alpha_i$ in $A(f_i, D(E))$ such that $I'C = 0$, where $C = C \cap aP(f_i(a))$, or else $I'C = 0$ by 1.10. Likewise, there exists $\alpha_i$ in $A(f_i, D(C))$ such that $I'C = 0$, where $C = C \cap aP(f_i(a))$. Inductively we form the sequence $\alpha_1, \alpha_2, \ldots$. By our method of construction, $\alpha_{i+1} = \alpha_i + \alpha_i$, where $\alpha_i$ belongs to $C$ and $\alpha_i$ belongs to $P(f_i(a))$, and $\alpha_i$ is some positive integer. If we put $r_1 = \alpha_1$ and $g_i = \alpha_i$, we obtain a division chain in $C$ that is of the desired form.

3.12. Theorem. If $C$ is a set of natural numbers for which $I'C$ is positive, and $h$ is an arbitrary element of $Q$, then $C$ contains a division chain of the form $q_1, q_2, q_3, \ldots$, where $q_i$ is composed of primes greater than $q_1, q_2, q_3, \ldots$ raised to the power $h(q_1, q_2, q_3, \ldots)$.

Proof. Let $f(n) = n^{h(n)}$, and consider $A(f, C)$. In the proof of 2.14 we showed that $I'A = 0$, where $A$ is the density function associated with $h$ (see 2.12). Since the family of sets $aP(f(a))$ is $\lambda$-summable, we have $\lambda$-summable. Thus there is an $\alpha_i$ in $A$ so that $I'C = 0$, where $C = C \cap aP(f_i(a))$. Otherwise we would conclude that $I'C = 0$ by 1.10; this cannot be the situation since $0 < I'C \leq \lambda$. We may now proceed by our usual inductive construction technique (repeated use of 2.14 and 1.10) to form the division chain $\alpha_1, \alpha_2, \alpha_3, \ldots$, where $\alpha_{i+1} = \alpha_i + \alpha_i$, and $\alpha_i$ belongs to $P(f_i(a))$. The proper form is obtained by setting $\alpha_i = g_i$ and $\alpha_{i+1} = g_i$ for $i = 1, 2, \ldots$. One might wonder whether the conclusion of 3.12 would follow from the weaker assumption that $I'C > 0$. The following theorem shows that 3.10 is a best possible result.

3.13. Theorem. Let $P(n)$ be any arithmetic function which tends to infinity with $n$. Then there is a sequence of integers with positive upper logarithmic density which contains no division chain of the form $d_i < d_{i+1} < \ldots$, where $d_i = \alpha_i + \alpha_i$, and $\alpha_i$ belongs to $P(f_i(a))$ for each $i$.

Proof. Let $\varepsilon > 0$ be fixed, and consider an integer $x$ in the interval $(n, n^{1+\varepsilon})$. The density of integers $x$, where $\varepsilon$ is composed of primes greater
than \( x^{2/n} \), is less than \( M [x \Psi(x) \log x]^{-1} \), where \( M \) is as in \( 2.1 \). Thus if we let \( x \) range over \( (n, n^{1+\varepsilon}) \), the density of all such multiples of \( x \) is less than

\[
2 M \int_0^{n^{1+\varepsilon}} [x \Psi(x) \log x]^{-1} dx.
\]

Since \( \Psi(n) \) becomes large with \( n \), the integral tends to zero as \( n \) becomes large.

Let \( \delta > 0 \) be fixed and choose the positive numbers \( \varepsilon_1, \varepsilon_2, \ldots \) so that \( 2 \sum \varepsilon_j < \delta \). For each \( i \), choose \( n_i \), so that

1. the density of integers of the form \( ax \), where \( x \) belongs to \( (n_i, n_i^{1+\varepsilon_j}) \) and \( s \) is a product of primes greater than \( x^{1/\varepsilon} \), is less than \( \delta \varepsilon_j \);

2. the density of integers of the form \( x' \) in \( (n_j, n_j^{1+\varepsilon_j}) \), where \( x' \) belongs to \( (n_j, n_j^{1+\varepsilon_j}) \) for some \( j < i \) and \( s' \) is a product of primes greater than \( x'^{1/\varepsilon} \), is less than \( 2 \sum \varepsilon_j, j < i \).

If we form a sequence by taking for each \( i \) those members of \( (n_i, n_i^{1+\varepsilon_i}) \) which are not of the form \( x' \) described above, then the sequence does not have a division chain of the appropriate form. The upper logarithmic density of the sequence is greater than \( [\varepsilon/(1+\varepsilon)] - \delta \), a number which can be made as close to one as is desired.

However, we note that the methods used previously would produce a division chain for which \( a_{i+1} | a_i \), is composed of primes greater than \( n^{1/\varepsilon} \) for any sequence \( \varepsilon_1 < \varepsilon_2 < \ldots \), where

\[
\sum (\log n_i)^{-1} \leq K \log \log x \quad (i.o.)
\]

for some positive \( K \).

3.14. Definition. If \( C = \{2, 3, 4, \ldots \} \) and \( f \) belongs to \( \Gamma \), we will denote \( A(f, C) \) and \( B(f, C) \) by \( A(f) \) and \( B(f) \), respectively. We call \( A(f) \) the \( f \)-primitive integers.

It was noted in \( 2.7 \) that the \( f \)-primitive integers are the powers of prime integers. The next few results show that in certain respects, primitive integers are generalizations of prime (or power) integers.

3.15. Theorem. Let \( f \) be any member of \( \Gamma \) and let \( n \) be greater than one; then \( n \) possesses a unique factorization \( n = a_1 a_2 \cdots a_r \), where each \( a_i \) is an \( f \)-primitive integer and \( a_{i+1} \mid P(f(a_i)) \).

Proof. Suppose that \( n \) does not belong to \( A(f) \). Then \( n = a_1 a_2 \) where \( a_1 \) belongs to \( P(f(a_1)) \). If \( a_2 \) is not in \( A(f) \), it may be factored as \( a_2 = \alpha \beta \) with \( \alpha \) in \( P(f(\alpha)) \). This process must terminate with some \( \beta \), and \( n \) has at least one factorization in the desired form.

If we have two such factorizations \( n = a_1 a_2 \cdots a_r = \alpha'_1 \alpha'_2 \cdots \alpha'_r \), then \( a_1 a_2 \cdots a_r = \alpha'_1 \alpha'_2 \cdots \alpha'_r \) since \( s \) is in \( P(f(a_i)) \) and \( s' \) is in \( P(f(\alpha'_i)) \). Theorem 2.6 demands that \( a_i = a'_i \). We may proceed inductively to show that \( a_i = a'_i \) for \( i = 1, \ldots, r \).

3.16. Definition. The canonical factorization of \( n \) given by 3.14 will be called the \( f \)-factorization of \( n \).

3.17. Theorem. If \( f \) belongs to \( \Gamma \) and \( \ell(A(f)) = 0 \), then \( \delta(A(f)) = 0 \).

Proof. Since \( \ell(B(f)) = \sum \delta(\alpha P(f(a))) : \alpha \in A(f) \) = 1, we have from 1.6 that the sets \( \{\alpha P(f(a)) \} \) are \( \delta \)-sumnable. Hence \( \delta(B(f)) = 1 \) and \( \delta(A(f)) = 0 \).

3.18. Theorem. Let \( f \) be a member of \( \Gamma \) for which \( \delta(A(f)) = 0 \). If \( B(f) \) is the set of all positive integers whose \( f \)-factorization has at most \( r \) factors, then \( \delta(B(f)) = 0 \).

Proof. Suppose that the assertion is true when \( r = k \). Note that \( F = E_{k+1} - F_k \) is the collection of all numbers that have precisely \( k+1 \) factors in their \( f \)-factorization. Now observe that for any \( \alpha \in A(f) \), \( F \cap \alpha P(f(a)) = \{ \alpha \\} \), where \( \alpha \) is a subset of \( E_k \). Hence \( \delta(\alpha) = 0 \). Thus \( F \) is contained in \( \bigcup \{\alpha P(f(a)) : \alpha \in A(f)\} \), the union of a \( \delta \)-sumnable family of sets. Since \( F \) intersects each element of this family in a set of zero natural density, \( \delta(F) = 0 \) by 1.10. Hence \( \delta(E_{k+1}) = 0 \).

The next theorem concerns the irregularity of the prime factors of almost all integers. Erdős [7] has obtained a related result.

3.19. Theorem. Let \( r \) be an arbitrary positive integer, and let \( f(n) = g(n)^{\log h} \) where \( h \) belongs to \( \Omega \). Except for a set of zero natural density, each positive integer \( n \) has the following property: If \( p_1, p_2, \ldots, p_r \) are the prime factors of \( n \) in order of increasing size, then \( p_{r+1} \) exceeds \( p_i \) for at least \( r \) values of \( i \).

Proof. Consider \( G \), \( C - E_k \), where \( E_k \) is as in 3.17. By 3.9, \( \ell(A(f)) = 0 \); hence \( \delta(A(f)) = 0 \) by 3.16. Therefore \( \delta(E_k) = 0 \) by 3.17. If \( n \) belongs to \( G \), let \( p_i \) be the largest prime divisor of \( a_i \), and \( p_{i+1} \) is the smallest prime divisor of \( a_{i+1} \). We see that \( p_{i+1} \) is contained in \( P(f(p_i)) \).

The final result shows that 3.19 does not hold for functions which grow faster than those in \( \Gamma' \).

3.20. Theorem. Suppose \( f(n) = n^{\log h} \) where \( \sum (\log h)^{n+1} \) converges. Then \( \ell(A(f)) > 0 \).

Proof. Suppose \( \ell(A(f)) = 0 \). Then the ideas of 3.18 show that

\[
\ell(\bigcup A_n) = 0 \quad \text{where} \quad A_n \text{ consists of those integers with precisely } h \text{ factors in their } f \text{-factorization. If } A_n \text{ is those integers with at least } n \text{ factors in their } f \text{-factorization, } A(f, A_n) = A_n \text{ and}
\]

\[
\ell(B(f, A_n)) = \sum \left\lfloor \frac{1}{\alpha} \right\rfloor \left( \frac{1}{1 - \frac{1}{p}} : \frac{1}{p} \leq f(a), 1 \leq p \leq A_n, \right) \right\rfloor \quad \text{for each } n.
\]
However, as $n$ becomes large, the least element in $A_n$ becomes large; and the sum, which is dominated by $M \sum [(ah(a) \log a)^{-1}; a \in A_n]$, tends to zero. This contradiction gives the result. Professor Erdős has pointed out that it is possible to prove that $\delta[A(f)]$ exists.

In conclusion, I wish to express my deep appreciation to my advisor, Professor Robert Zink. Also, I wish to thank Professor Paul Erdős for a number of helpful discussions.

References


UNIVERSITY OF ILLINOIS

Recu par la Rédaction le 10.1.1966

АКТА АРИТМЕТИКА

XII (1967)

О рациональных точках некоторых кривых высшего рода

В. А. Демьяново (Москва)

Способ нахождения точек алгебраической кривой рода $g > 1$, рациональных над заданным полем $K$ конечной степени, неизвестен. Существует лишь предположение, что такая кривая имеет в $K$ только конечное число точек.

Значительные большие результаты получены при исследовании кривых первого рода. Мордец [1] доказал, что совокупность точек кривой первого рода на абсолютной области рациональности $R(1)$ образует коммутативную группу с конечным числом образующих.

Таким образом, существует такое конечное число рациональных точек $P_1, P_2, \ldots, P_r$, что любая рациональная точка $P$ представима в виде

$$P = n_1P_1 + n_2P_2 + \ldots + n_rP_r$$

с некоторыми целыми $n_1, n_2, \ldots, n_r$. Позднее доказательство Морделла было несколько упрощено и значительно обобщено Вейлем [2].

В настоящей работе мы будем рассматривать кривые

(1)

$$x^4 + y^4 = A$$

и

(2)

$$x^4 + y^4 = A$$

при определенных ограничениях, накладываемых на ранг кривых первого рода:

(3)

$$u^4 - A = v^2$$

и

(4)

$$u^4 + 1 = Au^3, \quad v^4 + 1 = Au^3, \quad u^4 + v^4 = A.$$

В частности, мы установили, что если ранг одной из кривых (4) над полем $R(V - 3)$ не превышает 2, то кривая (2) не имеет в этом поле точек, за исключением случаев: $A = 1, \{a, y\} = \{e_1, 0\}, \{0, e_2\}; A = 2, \{a, y\} = \{e_1, e_2\}, e_1^4 = e_2^4 = 1$. Аналогичный результат будет также получен и для кривой (1), рассматриваемой над полем $R(V - 1)$. 