UNIQUE FACTORIZATION IN MULTIPLICATIVE SYSTEMS

R. D. JAMES AND IVAN NIVEN

In discussing unique factorization and ideal theory, C. C. MacDuffee [1, p. 122] cites the multiplicative system of positive integers of the form $1+7k$ as an example where unique factorization fails, since $792=22\cdot 36=8\cdot 99$, and 8, 22, 36, 99 are all primes in the system. H. Davenport [2, p. 21] uses positive integers of the form $1+4k$ for the same purpose, with the numerical case $693=9\cdot 77=21\cdot 33$. In this paper we examine all multiplicative systems made up of arithmetic progressions, and decide the question of unique factorization.

For a fixed positive integer n, let M be a multiplicatively closed system of positive integers such that if $x\in M$ and $y\equiv x \pmod n$, $y>0$, then $y\in M$. It will be assumed that n is the smallest positive integer which can be used to define M. For example the set M of all positive integers congruent to 1, 3, or 5 modulo 6 is also the set congruent to 1 modulo 2, and in this case $n=2$. We divide the integers $1, 2, \cdots, n$ into two classes: the set A, $\phi(n)$ in number, of those relatively prime to n, and the others in set B, $n-\phi(n)$ in number.

THEOREM. *M has unique factorization if and only if $M\cap A=A$, $M\cap B=0$, i.e. if and only if M consists of all positive integers relatively prime to n.*

The proof will be in several parts, and will employ the following additional notation. Write $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ where the p_i are primes of I, the set of all positive integers. Numbers m belonging to M which cannot be factored in M are called pseudo-primes.

Case 1. $M\cap A=A$, $M\cap B=0$. Thus $m\in M$ if and only if $(m, n)=1$ and so the pseudo-primes of M are the primes of I with $p_1, p_2, \cdots, p_r$ deleted. Unique factorization in M is implied by that in I.

Case 2. $M\cap B\neq 0$, $M\cap A=0$. To any $m\in M$ there corresponds $b\in(M\cap B)$ such that $m\equiv b \pmod n$, whence $(m, n)=(b, n)$. For any b_i in $M\cap B$, define $d_i=(b_i, n)$, so that $d_i>1$. Among the elements of $M\cap B$, choose b_1 so that its corresponding d_1 is a minimum. Thus $(b_1, n)=d_1$ with say $b_1=d_1q_1$ and $n=d_1q_2$, $(q_1, q_2)=1$. Choose distinct primes $\pi_1>n$ and $\pi_2>n$ of the form q_1+xq_2, and also the prime π_3 of the form $1+xn$. Since $\pi_1>n$ we have $(\pi_1, n)=1$ and $\pi_1\notin M$. Similarly π_2, π_3, $\pi_1\pi_3$, and $\pi_2\pi_3$ are not in M.

Next we establish that $d_1\pi_1\pi_3$, which is of the form b_1+xn, is a

Presented to the Society, May 1, 1954; received by the editors November 5, 1953.

pseudo-prime in M. For any nontrivial factorization in M would be either of the form $(\delta_1)(\delta_2\pi_1\pi_3)$ or $(\delta_1\pi_1)(\delta_2\pi_3)$ where $\delta_1\delta_2 = d_1$ with $1 < \delta_1 < d_1$. But these are not valid factorizations in M, inasmuch as δ_1 and $\delta_1\pi_1$ are not in M, since $(\delta_1, n) = (\delta_1\pi_1, n) = \delta_1 < d_1$ would contradict the minimum principle used in the selection of d_1. Similarly $d_1\pi_2\pi_3$ is a pseudo-prime in M.

Also $d_1\pi_1$ and $d_1\pi_2$ are pseudo-primes in M. For any nontrivial factorization of $d_1\pi_1$ in M would have the form $(\delta_1)(\delta_2\pi_1)$ with $1 < \delta_1 < d_1$, but as before δ_1 is not in M.

The proof of Case 2 is completed by observing that

$$(d_1\pi_1)(d_1\pi_2\pi_3) = (d_1\pi_2)(d_1\pi_2\pi_3),$$

each term in parentheses being a pseudo-prime, and the factorizations being different since $\pi_1 \neq \pi_2$.

Case 3. $A \neq A \cap M \neq 0$. Let $a \in M$, so that $a^{\phi(n)} \in M$, and $a^{\phi(n)} \equiv 1 \pmod{n}$, so that $1 \in M$. Let α be a member of A which is not in M. Since $\alpha^{\phi(n)} \in M$, there is a least exponent $e > 1$ such that $\alpha^e \in M$. Choose distinct primes $\pi_1 > n$ and $\pi_2 > n$ of the form $\alpha + xn$, and it follows that π_1^e and π_2^e are pseudo-primes in M. Also $\pi_1\pi_2^{e-1}$ and $\pi_2\pi_1^{e-1}$ are pseudo-primes in M, so the proof is complete by the factorization

$$(\pi_1^e)(\pi_2^e) = (\pi_1\pi_2^{e-1})(\pi_2\pi_1^{e-1}).$$

Case 4. $M \cap A = A$, $B \neq M \cap B \neq 0$. As in Case 1, the pseudo-primes of M include all primes p such that $(p, n) = 1$. But since $M \cap B \neq 0$, there are other pseudo-primes of M, and we now prove that these others have no prime factors apart from the prime factors of n.

If q is any pseudo-prime with $(q, n) > 1$, write $q = q_1q_2$ where the prime factors of q_1 are also prime factors of n, but $(q_2, n) = 1$. We can readily prove that $q_2 = 1$. For the congruence $\mu q_2 \equiv 1 \pmod{n}$ has a positive solution μ, and all of μ, q_2, q, μq are in M. Thus $\mu q \equiv q_1 \pmod{n}$, so q_1 is in M. Thus $q = q_1q_2$ is a factorization in M, and $(q, n) > 1$ implies $(q_1, n) > 1$ and $q_1 \neq 1$, so $q_2 = 1$ since q is a pseudo-prime.

Thus we have established that the pseudo-primes of M are of two types: (1) all primes p with $(p, n) = 1$; (2) at least one pseudo-prime q whose prime factors are contained in the set $p_1, p_2, \cdots, p_r$, the prime factors of n. Let us order these primes so that precisely $p_1, \cdots, p_h$ are the prime factors of these pseudo-primes, with $1 \leqq h \leqq r$.

LEMMA 1. *M lacks unique factorization if it contains more than h pseudo-primes of type (2) above.*

PROOF. If we have $h+1$ distinct pseudo-primes

$$q_j = p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \cdots p_h^{\alpha_{hj}}, \qquad j = 1, 2, \cdots, h+1,$$

we can solve the h equations

$$\sum_{j=1}^{h+1} x_j \alpha_{ij} = 0, \qquad i = 1, 2, \cdots, h,$$

for integral values x_j not all zero. Thus we would have

$$\prod_{j=1}^{h+1} q_j^{x_j} = 1$$

and multiplying both sides by $q_j^{-x_j}$ in all cases of negative x_j, we obtain a counter-example to unique factorization.

LEMMA 2. *Let p be any one of the primes $p_1, \cdots, p_h$. If no pseudo-prime of M is of the form p^i, then M has infinitely many pseudo-primes of type* (2).

PROOF. There is no loss of generality in taking $p = p_1$. Now M contains a pseudo-prime with p_1 as a factor, say

$$q = p_1^{\beta_1} p_2^{\beta_2} \cdots p_h^{\beta_h}$$

where $\beta_1 > 0$ and $\beta_2 + \beta_3 + \cdots + \beta_h > 0$ by the hypothesis of the lemma. For $j = 1, 2, 3, \cdots$, choose positive x_j to satisfy $x_j \equiv p_1^j \pmod{n/p_1^{\alpha_1}}$ and $x_j \equiv 1 \pmod{p_1}$. Choose a positive integer γ so that $\gamma\beta_1 \geqq \alpha_1$, so that $q^\gamma(x_j - p_1^j)$ is divisible by n, that is,

$$x_j q^\gamma \equiv p_1^{j} q^\gamma \equiv p_1^{j+\gamma\beta_1} p_2^{\gamma\beta_2} \cdots p_h^{\gamma\beta_h} \pmod{n}.$$

Also $(x_j, n) = 1$ so that x_j and $x_j q^\gamma$ are in M. If M contained only a finite number of pseudo-primes of type (2), then

$$p_1^{j+\gamma\beta_1} p_2^{\gamma\beta_2} \cdots p_h^{\gamma\beta_h}$$

could not be factored into pseudo-primes for j very large, the exponents $\gamma\beta_2, \cdots, \gamma\beta_h$ being fixed. This completes the proof of Lemma 2, and in view of Lemma 1, we can now complete Case 4 by proving the following result.

LEMMA 3. *If M contains only a finite number of pseudo-primes of type* (2), *the number exceeds h.*

PROOF. By Lemma 2, M contains h pseudo-primes of the form $p_1^{\gamma_1}, p_2^{\gamma_2}, \cdots, p_h^{\gamma_h}$. We assume that these are all the pseudo-primes of type (2) in M, and obtain a contradiction.

First we establish that $\gamma_1=\gamma_2= \cdots =\gamma_h=1$. Choose the positive integer μ so that $\mu\gamma_1 \geqq \alpha_1$, and the positive integer x to satisfy simultaneously $x\equiv p_1 \pmod{n/p_1^{\alpha_1}}$ and $x\equiv 1 \pmod{p_1}$. Thus n is a divisor of $p_1^{\mu\gamma_1}(x-p_1)$, that is

$$xp_1^{\mu\gamma_1} \equiv p_1^{1+\mu\gamma_1} \pmod{n}.$$

Now $(x, n)=1$, so that x is in M, and so is $p_1^{\gamma_1}$, whence $xp_1^{\mu\gamma_1}$ is in M. Thus $p_1^{1+\mu\gamma_1}$ is in M. But by the opening remark of this proof the only powers of p_1 which are in M are also powers of $p_1^{\gamma_1}$. Hence $\gamma_1=1$. Similarly $\gamma_2=\gamma_3= \cdots =\gamma_h=1$.

We have established that the pseudo-primes of type (2) in M are $p_1, p_2, \cdots, p_h$. Thus the set M can be characterized as all positive integers relatively prime to $p_{h+1}, \cdots, p_r$, if such primes exist. So the set M can be described in terms of the modulus $p_{h+1}p_{h+2} \cdots p_r$, which is less than n since $h \geqq 1$. This contradicts our basic hypothesis that n is the smallest modulus available to define M. This completes the proof of Lemma 3 and Case 4.

REMARK ON THE PROOFS. The Dirichlet theorem on the infinitude of primes in an arithmetic progression is used in Cases 2 and 3, but is not essential in these proofs, as we now show.

In Case 2 it is not necessary that π_1, π_2, π_3 be primes, but merely that they have the following properties:

$$\pi_3 \equiv 1 \pmod{n},\ (\pi_1, n) = (\pi_2, n) = 1,$$

$$d_1\pi_1 \equiv d_1\pi_2 \equiv b_1 \pmod{n},\ \pi_1 \neq \pi_2.$$

It can be verified that these are all satisfied by the choices $\pi_3=1+n$, $\pi_1=q_1+uq_2$ where u is defined as the product of all primes dividing n but not dividing q_1, and $\pi_2=q_1+upq_2$ where p is any prime exceeding n.

To remove the Dirichlet theorem from the proof of Case 3 we proceed as follows. Let p be the smallest integer in A which is not in M. Our notation is justified since p is a prime in I, for if $p=qv$ it would follow that q and v were in A but not both in M, contradicting the minimal property of p. Define e as the least exponent such that $p^e \in M$, and so $1<e\leqq\phi(n)$. Define $b=n+p^{e-1}$, whence $b^e \equiv (p^e)^{e-1} \pmod{n}$ so that $b \notin M$ but $b^e \in M$ and $pb \in M$.

Now consider the factorization in M, not all factors being necessarily pseudo-primes,

$$(p^e)(b^e) = (pb)(pb) \cdots (pb).$$

However, p^e is a pseudo-prime, and p^e is not a divisor of pb, since $(p, n)=1$ implies $(p, b)=1$.

REFERENCES

1. C. C. MacDuffee, *Introduction to abstract algebra*, Wiley, 1940.
2. H. Davenport, *The higher arithmetic*, Hutchinson's University Library, 1952.

UNIVERSITY OF BRITISH COLUMBIA AND
UNIVERSITY OF OREGON

ON A PROBLEM OF ADDITIVE NUMBER THEORY

G. G. LORENTZ

Let $A, B, \cdots$ denote sets of natural numbers. *The counting function* $A(n)$ of A is the number of elements $a \in A$ which satisfy the inequality $a \leqq n$. We shall call two sets A, B *complementary* to each other if $A+B$ contains all sufficiently large natural numbers.

In a talk with the author P. Erdös conjectured that each infinite set A has a complementary set B of asymptotic density zero. Here we wish to establish a theorem which gives an upper estimate for $B(n)$ in terms of $A(n)$. As a particular case, the truth of Erdös' conjecture will follow. The estimate (1) below should be compared with the (trivial) lower estimate $B(n) \geqq (1-\epsilon)n/A(n)$, which holds for all large n.

THEOREM 1. *For each infinite set A there is a complementary set B such that*

$$B(n) \leqq C \sum_{k=1}^{n} \frac{\log A(k)}{A(k)}; \tag{1}$$

C is an absolute constant and the terms of the sum with $A(k)=0$ are to be replaced by one.

PROOF. Let A be given and let $m<n$ denote two natural numbers. We shall choose certain integers b in the interval $m \leqq b < 2n$ in such a way that the sums $a+b$, $a \in A$, fill the whole interval $n < a+b \leqq 2n$. Our concern will be to obtain the upper estimate (4) for the number K of the b's.

First we take a b_1 in $[m, 2n)$ in such a way that the portion of $A+b_1$ contained in $(n, 2n]$ has the maximal possible number S of elements and choose this b_1 as one of our b's. Then we take another

Received by the editors March 2, 1954.