

# Pacific Journal of Mathematics

**PARTITIONING INTEGERS USING A FINITELY GENERATED  
SEMIGROUP**

DANIEL REICH

## PARTITIONING INTEGERS USING A FINITELY GENERATED SEMIGROUP

DANIEL REICH

**Denoting by  $\Gamma$  the semigroup of positive integers generated by two fixed primes, let  $r_k(N)$  be the number of partitions of  $N$  as a sum of  $k$  elements of  $\Gamma$ . Our main result is that  $r_2(N)$  is a bounded function of  $N$ . Incidentally, we obtain an estimate of the number of distinct prime divisors of numbers of the form  $1+q^n$ . Boundedness of  $r_k(N)$  would resolve an approximation theoretic conjecture of D. J. Newman.**

Let  $\Gamma$  be a finitely generated semigroup of positive integers. For a positive integer  $N$ , let  $r_k(N)$  be the number of partitions of  $N$  into  $k$  parts from  $\Gamma$ . Donald J. Newman has asked the following question:

Is  $r_k(N)$  a bounded function of  $N$ , for all  $k$ ?

This question arose in the context of a general problem of approximation theory; that is, the determination of when, for a given function  $f(x)$ , the functions  $\{f(kx)\}_{k=-\infty}^{\infty}$  generate a dense subspace  $E_f$  of some function space. This problem has been considered by Neuwirth, Ginsberg and Newman in [3] for  $f(x)$  a trigonometric polynomial. In his report to the Canterbury conference on complex analysis ([4], 1973), Newman stated a conjecture: Let  $f(z) = z + a_2z^2 + \dots + a_nz^n$  (here  $z = e^{i\theta}$ ). To  $f(z)$  we associate a "Dirichlet polynomial"

$$D(s) = 1 + a_2/2^s + \dots + a_n/n^s.$$

Then  $E_f$  is dense in  $L^p(1 \leq p < \infty)$  if and only if  $D(s)$  has no zeros in  $\text{Re } s > 0$ , and  $E_f$  is dense in  $L^\infty$  if and only if  $D(s)$  is bounded away from zero in  $\text{Re } s > 0$ . Newman asserts that the settling of this conjecture for  $p < \infty$  depends on making a connection between norms in the  $z$  and  $s$  variables, and that this connection can be made according to a classical result of Szidon, if the above number theoretic question has an affirmative answer.

In this paper we shall consider the simplest case of the question, when  $\Gamma$  is generated by two primes, and  $k = 2$ . A complete proof of Newman's conjecture for the corresponding  $f(z)$  would require a proof for this  $\Gamma$ , for all  $k$ .

Let  $p, q$  be distinct primes; we shall denote by  $\Gamma$  the multiplicative semigroup of nonnegative integers generated by  $\{0, p, q\}$ . For any integer  $N$ , let  $r_2(N)$  denote the number of representations

$$N = \alpha + \beta \quad (\alpha, \beta \in \Gamma).$$

Our purpose is to prove:

**THEOREM 1.**  $r_2(N)$  is bounded.

We shall show in fact that  $r_2(N) \leq 5$ . This is merely the estimate that falls readily out of the proof, not necessarily the best possible one.

We begin with two simple observations, whose proofs are included for the convenience of the reader. In what follows,  $\mathbb{Z}$  denotes the integers, and  $\text{ord}_p$  denotes the standard valuation, order of divisibility by  $p$ .

**LEMMA 1.**  $(1 + q^n) \mid (1 + q^m)$  if and only if  $m = \lambda n$ , with  $\lambda$  odd.

*Proof.* Let  $m = \lambda n + r$ , with  $0 \leq r < n$ . For an indeterminate  $y$ , we may write

$$(1 + y^m)/(1 + y) = \begin{cases} P(y), & \text{if } \lambda \text{ is odd} \\ Q(y) + 2/(y + 1), & \text{if } \lambda \text{ is even} \end{cases}$$

with  $P(y), Q(y) \in \mathbb{Z}[y]$ .

Set  $f(x) = (x^m + 1)/(x^n + 1)$ . Then

$$f(x) = x^r(x^{2n} + 1)/(x^n + 1) + (1 - x^r)/(x^n + 1).$$

If  $\lambda$  is odd,

$$f(x) = x^r P(x^n) - (x^r - 1)/(x^n + 1);$$

thus

$$f(q) = \text{integer} - (q^r - 1)/(q^n + 1)$$

and so  $f(q)$  is an integer if and only if  $r = 0$ .

If  $\lambda$  is even,

$$\begin{aligned} f(x) &= x^r(Q(x^n) + 2/(x^n + 1)) + (1 - x^r)/(x^n + 1) \\ &= x^r Q(x^n) + (1 + x^r)/(1 + x^n). \end{aligned}$$

Thus

$$f(q) = \text{integer} + (1 + q^r)/(1 + q^n)$$

and so cannot be an integer.

**LEMMA 2.** Let  $p$  be an odd prime. Suppose for integers  $q, \lambda > 1$ , and  $r, s \geq 1$ , we have

$$(1) \quad \begin{aligned} r &= \text{ord}_p(1 + q) \\ r + s &= \text{ord}_p(1 + q^2). \end{aligned}$$

Then  $\text{ord}_p \lambda = s$ .

*Proof.* Write  $1 + q = p^r K$ , with  $(p, K) = 1$ . Then

$$\begin{aligned} q^2 &= (-1 + p^r K)^2 \\ &= -1 + 2p^r K - \sum_{\nu=2}^{\lambda} (-1)^\nu \binom{\lambda}{\nu} p^{\nu r} K^\nu. \end{aligned}$$

Thus

$$1 + q^2 = p^r K(\lambda + \lambda'),$$

where

$$(2) \quad \lambda' = - \sum_{\nu=2}^{\lambda} (-1)^\nu \binom{\lambda}{\nu} p^{(\nu-1)r} K^{\nu-1}.$$

It now follows from equation (1) that  $\text{ord}_p(\lambda + \lambda') = s$ . From equation (2) we obtain

$$\text{ord}_p \lambda' \geq \min_{\nu \geq 2} \left\{ r(\nu - 1) + \text{ord}_p \binom{\lambda}{\nu} \right\}.$$

We now show that for each  $\nu \geq 2$ ,

$$\text{ord}_p \lambda < r(\nu - 1) + \text{ord}_p \binom{\lambda}{\nu}.$$

First, write

$$\binom{\lambda}{\nu} = (\lambda/\nu) \cdot \binom{\lambda - 1}{\nu - 1}$$

and we obtain

$$\text{ord}_p \lambda - \text{ord}_p \nu \leq \text{ord}_p \binom{\lambda}{\nu}.$$

But for  $\nu \geq 2$ ,  $\text{ord}_p \nu < \nu - 1$  (since  $p > 2$ , so  $p^x > x + 1$  for  $x \geq 1$ ), and this does it.

It now follows that

$$\text{ord}_p \lambda < \text{ord}_p \lambda',$$

and thus

$$\text{ord}_p \lambda = \text{ord}_p(\lambda + \lambda') = s.$$

An immediate consequence of Lemma 2 provides the key step in our proof of Theorem 1:

LEMMA 3. *Let  $p, q$  be positive integers, with  $p$  a prime and either  $p \neq 3$  or  $q \neq 2$ . For  $\underline{N} \in \mathbb{Z}$ , with  $(p, N) = 1$ , the simultaneous equations*

$$(3) \quad \begin{aligned} p^r N &= 1 + q^n \\ p^{r+s} N &= 1 + q^m \end{aligned}$$

*have no solutions in integers  $r, s, n, m \geq 1$ .*

*Proof.* Suppose we are given a solution  $(r, s, n, m)$  to (3). According to Lemma 1, we may write

$$m = \lambda n, \quad \lambda \text{ odd}.$$

Consider first the case  $p > 2$ . According to Lemma 2,  $\text{ord}_p \lambda = s$ ; set

$$\begin{aligned} \lambda &= p^s l \\ m &= p^s l n, \end{aligned}$$

where  $l$  is odd. From equation (3) we obtain

$$(*) \quad \begin{aligned} p^s &= (1 + q^{p^s l n}) / (1 + q^n) \\ &= q^{(p^s l - 1)n} - q^{(p^s l - 2)n} + \dots + 1 \\ &> q^{p^s - 2} \\ &> p^s. \end{aligned}$$

This last step follows from the inequality

$$q^{x-2} > x,$$

which is valid under either of the following circumstances:

$$\begin{aligned} q > 3 \quad \text{and} \quad x &\geq 3 \\ q \geq 2 \quad \text{and} \quad x &\geq 5. \end{aligned}$$

This covers all present cases, and the contradiction completes the proof for  $p > 2$ .

To dispose of  $p = 2$ , we observe that from equation (3),

$$\begin{aligned} 2^s &= (1 + q^{n\lambda}) / (1 + q^n) \\ &= \lambda + \lambda' \end{aligned}$$

with  $\lambda'$  defined as in equation (2) of Lemma 2. Here  $\lambda'$  is clearly even, and  $\lambda$  is odd; thus  $s = 0$ .

As an interesting consequence of Lemma 3 we obtain an estimate of the number of primes dividing numbers of the form  $1 + q^n$ . We

denote by  $\omega(N)$  the number of distinct prime divisors of  $N$ , and by  $\Omega(N)$  the total number of prime divisors.

**COROLLARY.** *Given integers  $q, n$  such that  $n$  is odd, and either  $q \neq 2$  or  $(3, n) = 1$ , we have*

$$\omega(1 + q^n) \geq \Omega(n) + \omega(1 + q) .^1$$

*Proof.* Write  $n = \prod_{i=1}^r p_i$ , with  $\{p_i\}$  odd primes, not necessarily distinct, and  $r = \Omega(n)$ . Let  $q_0 = q$ , and for  $1 \leq j \leq r$ ,

$$q_j = (q_{j-1})^{p_j} .$$

The result will follow once we prove

$$\omega(1 + q_j) \geq \omega(1 + q_{j-1}) + 1, \quad (1 \leq j \leq r) .$$

Dropping the subscripts, we must show that for  $p$  an odd prime,  $\omega(1 + q^p) \geq \omega(1 + q) + 1$ . Let  $\{\pi_1, \dots, \pi_s\}$  be the distinct primes dividing  $1 + q$ . Since  $p$  is odd we may write

$$1 + q^p = M(1 + q) ,$$

with  $M$  an integer. Suppose for some  $\nu, \pi_\nu | M$ ; then, according to Lemma 2, we have  $\pi_\nu | p$  and thus  $\pi_\nu = p$ . Now write  $M = p^\alpha M'$  with  $(M', 1 + q) = 1$ . Lemma 3 assures us that  $M' \neq 1$ , and thus  $1 + q^p$  is divisible by at least one prime not dividing  $1 + q$ .

Note that for  $q = 2$  and  $n = 3k$  we now obtain

$$\omega(1 + 2^{3k}) = \omega(1 + 8^k) \geq \Omega(k) + 1 ;$$

similarly, if  $n$  is even we can obtain a bound by setting  $n = 2^t n'$ , with  $n'$  odd, and replacing  $n$  by  $n'$  and  $q$  by  $q^{2^t}$ .

C. Gurwood has proven a result very closely related to Lemma 3 [2]:

**LEMMA (Gurwood).** *The equation*

$$(m^a + 1)n^b = m^c + 1$$

*has no solutions in integers  $a, c > 0$  and  $b, m, n > 1$ .*

This result is better than Lemma 3, but does not include it because of the restriction  $b > 1$ .

We now proceed to the main result:

---

<sup>1</sup> I would like to thank the referee for pointing out that E. Artin derived similar results about numbers of the form  $q^n - 1$  in his discussion of coincidences among orders of the finite linear groups (see [1]).

THEOREM 1.  $r_2(N) \leq 5$ .

*Proof.* Assume to begin with that  $p \neq 2, q \neq 2$ .

Case (i).  $(p, N) = (q, N) = 1$ .

Suppose we are given a representation

$$(4) \quad N = \alpha + \beta$$

with  $\alpha, \beta \in \Gamma$ . Then  $\alpha$  and  $\beta$  cannot both be divisible by  $p$  or by  $q$ . Say  $p \nmid \alpha$ :

(a) Suppose  $q \nmid \alpha$ . Then  $\alpha = 1$ , and (4) reads:

$$N = 1 + \beta.$$

But then  $\beta$  is determined by  $N$ ; i.e., there is at most one such representation.

(b) Suppose  $q \nmid \beta$ . Then (4) reads:

$$N = q^a + p^b.$$

Here one of the two conditions

$$N/2 < q^a < N$$

$$N/2 < p^b < N$$

must be satisfied. Thus  $(a, b)$  have at most two possible values. Combining (a) and (b), we have

$$r_2(N) \leq 3.$$

Case (ii).  $p \mid N, (q, N) = 1$ .

Suppose first  $N \notin \Gamma$ . Then in all representations (4),  $\alpha\beta \neq 0$ .

Write  $N = p^r N'$ , with  $(p, N') = 1, \alpha = p^s$ , and  $\beta = q^a p^t$ . Equation (4) now takes the form

$$(5) \quad p^r N' = p^s + q^a p^t.$$

We now note that multiplication by  $p^r$  provides a one-to-one correspondence between the set of such representations of  $N$  with  $s \geq r, t \geq r$ , and the set of all representations of  $N'$ ; that is,

$$(6) \quad \#\{\text{representations of } N \text{ with } s, t \geq r\} = r_2(N').$$

It follows from (5) that  $r \geq \min\{s, t\}$ , and  $r = \min\{s, t\}$  if  $s \neq t$ . Thus the left side of (6) includes all representations of  $N$  with  $s \neq t$ ; and we have

$$(7) \quad \#\{\text{representations of } N \text{ with } s \neq t \text{ or } s = t = r\} = r_2(N').$$

Now suppose we have a representation (5) with  $s = t < r$ . Then we have

$$(8) \quad p^{r-s}N' = 1 + q^a.$$

Since  $p \neq 2$ , we can conclude  $a \geq 1$ . According to Lemma 3,  $s$  and  $a$  are then determined by  $N$ ; i.e., there is at most one such representation. Thus equation (7) yields

$$r_2(N) \leq r_2(N') + 1 \leq 4.$$

Now suppose  $N \in \Gamma$ ; then  $N = p^r$ , and since  $p$  is odd,  $r_2(N) = 1$ . Thus in case (ii),

$$r_2(N) \leq 4.$$

Case (iii):  $q \mid N, (p, N) = 1$ .

As for case (ii),  $r_2(N) \leq 4$ .

Case (iv):  $pq \mid N$ .

Let  $N = p^r N'$ , with  $p \nmid N'$  and  $q \mid N'$ . Given a representation (4), write

$$\begin{aligned} \alpha &= p^s q^a \\ \beta &= p^t q^b. \end{aligned}$$

As before, we may use (7) to count representations with  $s \neq t$ , or  $s = t = r$ . Now suppose  $s = t < r$ . Then since  $p \neq 2$ , we know  $a \neq b$ ; say  $b > a \geq 0$ . Setting  $N'' = q^a + q^b$ , we have

$$N = p^s N'' = p^r N'.$$

Writing  $u = r - s, c = b - a$ , then  $u > 0, c > 0$  and

$$N'' = p^u N' = q^a(1 + q^c).$$

Now, setting  $N''' = N'/q^a$ ,

$$(**) \quad p^u N''' = 1 + q^c.$$

Here  $a = \text{ord}_q N, r = \text{ord}_p N$ , and  $N''' = N/p^r q^a$  are all determined by  $N$ , and so applying Lemma 3 to (\*\*),  $u$  is also determined. That is, there is at most one such representation of  $N$ . Combining this with (7) and the result of case (iii), we obtain:

$$r_2(N) \leq r_2(N') + 1 \leq 5.$$

This completes the proof of the theorem for  $p, q$  odd.

The same reasoning goes through for  $p = 2, q \geq 5$ , or vice versa, with one minor modification. In case (ii), we cannot exclude  $a = 0$  in equation (8). But if there is such a representation of  $N$  with



$a = 0$ , it is unique; and since  $r > s$ ,  $N = 2^r$ . Consequently  $N' = 1$ ,  $r_2(N') = 1$  and  $r_2(N) \leq 3$ . Case (iv) requires no change, since if  $p = 2$  we can interchange the roles of  $p$  and  $q$ .

For  $\{q, p\} = \{2, 3\}$ , we must modify Lemma 3 as follows:

LEMMA 3'. *The equations*

$$(9) \quad \begin{aligned} 3^r N &= 1 + 2^n \\ 3^{r+s} N &= 1 + 2^m \end{aligned}$$

have exactly one solution with  $r > 0$ ,  $s > 0$ ; namely  $r = s = N = n = 1$ ,  $m = 3$ .

*Proof.* The argument given for Lemma 3 is applicable up to (\*). Thus, given a solution to (9), we have

$$3^s > 2^{3^s-2}$$

and so  $s = 1$ . Applying this to (9), we have

$$(1 + 2^m)/(1 + 2^n) = 3,$$

from which it easily follows that  $n = 1$ ,  $m = 3$ , and thus  $N = 1$ ,  $r = 1$ .

We now indicate the changes that have to be made in the proof of Theorem 1 when  $q = 2$ ,  $p = 3$ :

*Case (ii).* According to Lemma 3', equation (8) will have at most one solution unless  $N' = 1$ ,  $N = 3^r$ , in which case it can have at most two. But then  $r_2(N') = 1$  and so

$$r_2(N) \leq r_2(N') + 2 \leq 3.$$

*Case (iv).* The argument is the same up to (\*\*). This equation can have two solutions only when  $N''' = 1$  (by Lemma 3'). But then  $N' = 2^n$ , and we have seen that in this case  $r_2(N') \leq 3$ . Thus  $r_2(N) \leq 5$ . This completes the proof of Theorem 1.

#### REFERENCES

1. E. Artin, *The orders of the linear groups*, Comm. Pure Appl. Math., **8** No. 3 (1955), 355-365.
2. C. Gurwood, unpublished note.
3. J. H. Neuwirth, J. Ginsberg, and D. J. Newman, *Approximation by  $\{f(kx)\}$* , J. Functional Anal., **5** (1970), 194-203.
4. D. J. Newman, *Completeness questions and related Dirichlet polynomials*, Proc. Symposium on Complex Analysis, Canterbury, (1973), 111-112.

Received November 4, 1977.

TEMPLE UNIVERSITY

PHILADELPHIA, PA. 19122

# PACIFIC JOURNAL OF MATHEMATICS

## EDITORS

RICHARD ARENS (Managing Editor)

University of California  
Los Angeles, California 90024

C. W. CURTIS

University of Oregon  
Eugene, OR 97403

C. C. MOORE

University of California  
Berkeley, CA 94720

J. DUGUNDJI

Department of Mathematics  
University of Southern California  
Los Angeles, California 90007

R. FINN AND J. MILGRAM

Stanford University  
Stanford, California 94305

## ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSHIDA

## SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA  
CALIFORNIA INSTITUTE OF TECHNOLOGY  
UNIVERSITY OF CALIFORNIA  
MONTANA STATE UNIVERSITY  
UNIVERSITY OF NEVADA, RENO  
NEW MEXICO STATE UNIVERSITY  
OREGON STATE UNIVERSITY  
UNIVERSITY OF OREGON

UNIVERSITY OF SOUTHERN CALIFORNIA  
STANFORD UNIVERSITY  
UNIVERSITY OF HAWAII  
UNIVERSITY OF TOKYO  
UNIVERSITY OF UTAH  
WASHINGTON STATE UNIVERSITY  
UNIVERSITY OF WASHINGTON

Simeon M. Berman, <i>A class of isotropic distributions in <math>\mathbf{R}^n</math> and their characteristic functions</i> .....	1
Ezra Brown and Charles John Parry, <i>The 2-class group of biquadratic fields. II</i> .....	11
Thomas E. Cecil and Patrick J. Ryan, <i>Focal sets of submanifolds</i> .....	27
Joseph A. Cima and James Warren Roberts, <i>Denting points in <math>B^p</math></i> .....	41
Thomas W. Cusick, <i>Integer multiples of periodic continued fractions</i> .....	47
Robert D. Davis, <i>The factors of the ramification sequence of a class of wildly ramified <math>v</math>-rings</i> .....	61
Robert Martin Ephraim, <i>Multiplicative linear functionals of Stein algebras</i> .....	89
Philip Joel Feinsilver, <i>Operator calculus</i> .....	95
David Andrew Gay and William Yslas Vélez, <i>On the degree of the splitting field of an irreducible binomial</i> .....	117
Robert William Gilmer, Jr. and William James Heinzer, <i>On the divisors of monic polynomials over a commutative ring</i> .....	121
Robert E. Hartwig, <i>Schur's theorem and the Drazin inverse</i> .....	133
Hugh M. Hilden, <i>Embeddings and branched covering spaces for three and four dimensional manifolds</i> .....	139
Carlos Moreno, <i>The Petersson inner product and the residue of an Euler product</i> .....	149
Christopher Lloyd Morgan, <i>On relations for representations of finite groups</i> .....	157
Ira J. Papick, <i>Finite type extensions and coherence</i> .....	161
R. Michael Range, <i>The Carathéodory metric and holomorphic maps on a class of weakly pseudoconvex domains</i> .....	173
Donald Michael Redmond, <i>Mean value theorems for a class of Dirichlet series</i> .....	191
Daniel Reich, <i>Partitioning integers using a finitely generated semigroup</i> .....	233
Georg Johann Rieger, <i>Remark on a paper of Stux concerning squarefree numbers in non-linear sequences</i> .....	241
Gerhard Rosenberger, <i>Alternierende Produkte in freien Gruppen</i> .....	243
Ryōtarō Satō, <i>Contraction semigroups in Lebesgue space</i> .....	251
Tord Sjödin, <i>Capacities of compact sets in linear subspaces of <math>\mathbf{R}^n</math></i> .....	261
Robert Jeffrey Zimmer, <i>Uniform subgroups and ergodic actions of exponential Lie groups</i> .....	267