Publ. Math. Debrecen
79/3-4 (2011), 461–468
DOI: 10.5486/PMD.2011.5132

Representing integers as linear combinations of powers

By LAJOS HAJDU (Debrecen) and ROBERT TIJDEMAN (Leiden)

Dedicated to Professors K. Győry and A. Sárközy on their 70th birthdays and Professors A. Pethő and J. Pintz on their 60th birthdays

Abstract. At a conference in Debrecen in October 2010 Nathanson announced some results concerning the arithmetic diameters of certain sets. (See his paper in the present volume.) He proposed some related problems on the representation of integers by sums or differences of powers of 2 and of 3. In this note we prove some results on this problem and the more general problem about the representation by linear combinations of powers of some fixed integers.

1. Introduction

Let P be a nonempty finite set of prime numbers, and let T be the set of positive integers that are products of powers of primes in P. Put $T_P = T \cup (-T)$. Then there does not exist an integer k such that every positive integer can be represented as a sum of at most k elements of T_P. This follows e.g. from Theorem 1 of Jarden and Narkiewicz [6], cf. [5], [1]. At a conference in Debrecen in October 2010 Nathanson announced the following stronger result (see also [7]):

Mathematics Subject Classification: 11D85.
Key words and phrases: representation of integers, linear combinations, powers.
Research supported in part by the OTKA grants K67580 and K75566, and by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, cofinanced by the European Social Fund and the European Regional Development Fund.

For every positive integer k there exist infinitely many integers n such that k is the smallest value of l for which n can be written as

$$n = a_1 + a_2 + \cdots + a_l \qquad (a_1, a_2, \ldots, a_l \in T_P).$$

Let $f(k)$ be the smallest positive integer which cannot be represented as sum of less than k terms from T_P. In Problem 2 of [7] NATHANSON asked to give estimates for $f(k)$. (The notation in [7] is somewhat different from ours.) Problem 1 asks the same question in case T consists of the pure powers of 2 and of 3. Observe that in both cases $f(k)$ can be represented as a sum of k terms from T_P, since less than T_P terms suffice for $f(k) - 1$ and $1 \in T_P$.

In this note we consider Problem 1. More generally, let $B = \{b_1, \ldots, b_t\}$ be any finite set of positive integers. Put $A = \{b_i^j, -b_i^j : i = 1, \ldots, t;\ j = 0, 1, 2, \ldots\}$. Note that on writing $P = \{p \text{ prime} : p \mid b_1 \cdots b_t\}$ we have $A \subseteq T_P$. So there is no k for which every positive integer can be represented as a sum of at most k elements of A. Let $f(k)$ be the smallest positive integer which cannot be represented as sum of less than k terms of A. Similarly as above, we get that $f(k)$ can be represented as a sum of k terms of A.

In this paper we show that there exists a number c depending only on B and an absolute constant C such that $\exp(ck) < f(k) < \exp((k \log t)^C)$. Moreover, we show that there are infinitely many k's for which $f(k) < \exp(c^* k \log(2kt) \log\log k)$ where c^* is some constant.

For the upper bound we apply a method of ÁDÁM, HAJDU and LUCA [1] in which a result of ERDŐS, POMERANCE and SCHMUTZ [4] plays an important part. We refine the result of Erdős, Pomerance and Schmutz in Section 2 and that of Ádám, Hajdu and Luca in Section 3. In Section 4 we derive lower and upper bounds for $f(k)$ in a somewhat more general setting. We conclude with some remarks in Section 5.

2. An extension of a theorem of Erdős, Pomerance and Schmutz

Let $\lambda(m)$ be the Carmichael function of the positive integer m, that is the least positive integer for which

$$b^{\lambda(m)} \equiv 1 \pmod{m}$$

for all $b \in \mathbb{Z}$ with $\gcd(b, m) = 1$. Theorem 1 of [4] gives the following information on small values of the Carmichael function.

For any increasing sequence $(n_i)_{i=1}^{\infty}$ of positive integers, and any positive constant $c_0 < 1/\log 2$, one has

$$\lambda(n_i) > (\log n_i)^{c_0 \log\log\log n_i}$$

for i sufficiently large. On the other hand, there exist a strictly increasing sequence $(n_i)_{i=1}^{\infty}$ of positive integers and a positive constant c_1, such that, for every i,

$$\lambda(n_i) < (\log n_i)^{c_1 \log\log\log n_i}.$$

This nice theorem does not give any information on the size of n_i. Since we need such information in this paper, we prove the following refinement of the second part. The proof is an extension of the proof in [4].

Theorem 1. *There exist positive constants c_2, c_3 such that for every large integer i there is an integer m with $\log m \in [\log i, (\log i)^{c_2}]$ and*

$$\lambda(m) < (\log m)^{c_3 \log\log\log m}.$$

Proof. In [2] it is shown that there is a computable constant $c_4 > 0$ with the property that, for any $x > 10$, there is a squarefree number $h_x < x^2$ for which

$$\sum_{p-1|h_x} 1 > e^{c_4 \log x/\log\log x}.$$

Put $x = (\log i)^{(2/c_4)\log\log\log i}$, $y = h_x$, and $m = \prod_{p-1|y} p$. Note that, for i sufficiently large, we have

$$m \geq \prod_{p-1|y} 2 > \exp\left((\log\ 2)\exp\left(\frac{c_4 \log x}{\log\log x}\right)\right) > i.$$

But then, for i sufficiently large and $c_3 = 4/c_4$,

$$\lambda(m) \leq y < x^2 = (\log i)^{(4/c_4)\log\log\log i} < (\log m)^{c_3 \log\log\log m}.$$

It remains to estimate m from above. Let s be the number of prime factors of the squarefree number y and $0 < \varepsilon < 0.1$. Then y is at least $s^{(1-\varepsilon)s}$ if i is sufficiently large. Hence $s < (1+2\varepsilon)\log y/\log\log y$. It follows that

$$\sum_{p-1|y} 1 \leq 2^s < \frac{y^{1/\log\log y}}{\log(y+1)}$$

when i is large. Thus

$$\log m = \log\left(\prod_{p-1|y} p\right) < \sum_{p-1|y} \log(y+1) < y^{1/\log\log y} < x^{2/\log\log x} < (\log i)^{c_2}$$

for some constant c_2. □

3. An extension of a theorem of Ádám, Hajdu and Luca

Let $B = \{b_1, \dots, b_t\}$ be any finite set of positive integers. Let $A = \{b_i^j : i = 1, \dots, t;\ j = 0, 1, 2, \dots\}$. Let k be a positive integer and R a finite set of integers of cardinality ρ. Put

$$H_{B,R,k} = \left\{ n \in \mathbb{Z} : n = \sum_{i=1}^{k} r_i a_i \right\}$$

where $r_i \in R$, $a_i \in A$ $(i = 1, 2, \dots, k)$. For $H \subseteq \mathbb{Z}$ and $m \in \mathbb{Z}, m \geq 2$, we write $\sharp H$ for the cardinality of the set H and

$$H(\mathrm{mod}\ m) = \{i : 0 \leq i < m, h \equiv i\ (\mathrm{mod}\ m) \text{ for some } h \in H\}.$$

Observe that the definition of A differs from that in the introduction and that we get the situation described there by choosing $R = \{-1, 1\}$.

Theorem 2. *Let B, R and k be given as above. For every sufficiently large integer i there exists a number m with $\log m \in [\log i, (\log i)^{c_2}]$ such that*

$$\sharp H_{B,R,k}\ (\mathrm{mod}\ m) < (\rho t)^k (\log m)^{c_5 k \log\log\log m}$$

where c_5 is a constant.

In the proof of Theorem 1 the following lemma is used.

Lemma 1 ([1], Lemma 1)**.** *Let $m = q_1^{\alpha_1} \cdots q_z^{\alpha_z}$ where $q_1, \dots, q_z$ are distinct primes and $\alpha_1, \dots, \alpha_z$ are positive integers, and let $b \in \mathbb{Z}$. Then*

$$\sharp\{b^u\ (\mathrm{mod}\ m) : u \geq 0\} \leq \lambda(m) + \max_{1 \leq j \leq z} \alpha_j.$$

The proof of Theorem 2 is similar to that of Theorem 3 of [1]. In that paper there is the restriction that of each element of B only one power occurs in $H_{B,R,K}$, hence $k = t$.

Proof of Theorem 2. Let i be an integer so large that Theorem 1 applies. Choose m as in Theorem 1. Write m as in Lemma 1 as a product of powers of distinct primes. Lemma 1 implies that for all $b \in B$,

$$\sharp\{r \cdot b^u\ (\mathrm{mod}\ m) : b \in B, r \in R, u \geq 0\} \leq \rho t \Big(\lambda(m) + \max_{1 \leq j \leq z} \alpha_j \Big).$$

On the other hand, with the constant c_3 from Theorem 1,

$$\lambda(m) + \max_{1 \leq j \leq z} \alpha_j \leq (\log m)^{c_3 \log\log\log m} + \frac{\log m}{\log 2}.$$

The combination of both inequalities yields the theorem. □

4. Representing integers as linear combinations of powers

We use the notation of Section 3. Suppose we want to express the positive integer n as a finite sum of powers of b_1. For this we apply the greedy algorithm. If we subtract the largest power of b_1 not exceeding n from n, we obtain a number which is less than $n(1-1/b_1)$. We can iterate subtracting the highest power of b_1 not exceeding the rest from the rest and so reduce the rest each time by a factor at most $1-1/b_1$. Hence we can represent n as the sum of at most $\log n/\log(1/(1-1/b_1))$ powers of b_1. Thus we find that the sum of $k \le c_6 \log n$ powers of b_1 suffices to represent n, where c_6 depends only on b_1. This implies the lower bound $\exp(ck)$ for $f(k)$ claimed in the introduction. More generally, let $f_R(k)$ be the smallest positive integer n which cannot be represented as a sum $\sum_{j=1}^{l} r_j a_j$ with $l < k$, $r_j \in R, a_j \in A$. Then the above argument shows that $1 \in R$ implies $f_R(k) > e^{k/c_6}$.

For an upper bound for $f_R(k)$ suppose first that all the elements of R are positive. We study the representation of positive integers up to n as $\sum_{j=1}^{k-1} r_j b_j^{k_j}$ with $r_j \in R$, $b_j \in B$, $k_j \in \mathbb{Z}$, $k_j \ge 0$. Then $k_j \le \log n/\log b_j \le \log n/\log 2$. Hence the number of represented integers is at most $(\rho t \log n/\log 2)^{k-1}$. If this number is less than n, then we are sure that some positive integer $\le n$ is not represented. This is the case if

$$k-1 < \frac{\log n}{\log(\rho t) + \log\log n - \log\log 2}.$$

Hence it suffices that $n \ge (1.5\rho k t \log(\rho k t))^{k-1}$ and for this special case we find that

$$f_R(k) \le (1.5\rho k t \log(\rho k t))^{k-1}.$$

We now turn to the general case. Choose the smallest positive integer $i > 10$ such that $i > (\rho t)^k (\log i)^{c_5 k \log\log\log i}$. Then $i < 2(\rho t)^k (\log i)^{c_5 k \log\log\log i}$. It follows that

$$\log i < k(\log \rho t) + c_7 k (\log\log i)(\log\log\log i)$$

for some constant c_7, thus $\log i < 2k\log(\rho t)$ or $\log i < 2c_7 k(\log\log i)(\log\log\log i)$. In the latter case $\log i < c_8 k(\log k)(\log\log k)$ for some suitable constant c_8. According to Theorem 2 there exists an m with $\log i \le \log m \le (\log i)^{c_2}$ such that all representations are covered by at most $(\rho t)^k (\log m)^{c_5 k \log\log\log m}$ residue classes modulo m. By the definition of i and the inequality $i \le m$, we see that this number of residue classes is less than m, therefore at least one positive integer $n \le m$ has no representation of the form $\sum_{j=1}^{k} r_j a_j$ with $r_j \in R$, $a_j \in A$ for all j.

Since $\log m \le (\log i)^{c_2}$, we obtain

$$\log n \le \log m \le (\log i)^{c_2} < (\max(2k \log \rho t, c_8 k (\log k)(\log\log k)))^{c_2} < (k \log \rho t)^{c_9}$$

for some constant c_9.

There are infinitely many k's for which a considerably better bound for $f_R(k)$ can be derived by a variant of the above argument. According to Theorem 1 there are infinitely many integers m for which

$$\lambda(m) < (\log m)^{c_3 \log\log\log m}. \tag{1}$$

Let B, hence A, ρ and t be given. Choose k as the largest integer such that

$$(\rho t)^k (\log m)^{c_5 k \log\log\log m} < m$$

for an m satisfying (1). It follows from Theorem 1 that there are infinitely many such k's. Theorem 2 and its proof imply that there is a positive integer $n \le m$ which is not representable as a linear combination of k elements of A with coefficients from R. Moreover,

$$\log m \le (k+1)(\log(\rho t) + c_5 \log\log m \log\log\log m).$$

Hence $\log m \le 2(k+1)\log(\rho t)$ or $\log m \le 2c_5(k+1)\log\log m \log\log\log m$. In the latter case $\log m \le c_{10} k \log k \log\log k$ where c_{10} is some constant. Combining both inequalities we obtain, for some constant c_{11},

$$\log n \le \log m \le c_{11} k \log(\rho k t) \log\log k.$$

So we have proved the following result.

Theorem 3. *Let $B = \{b_1, \dots, b_t\}$ be any finite set of positive integers. Put $A = \{b_i^j : i = 1, \dots, t; j = 0, 1, 2, \dots\}$. Let R be a finite set of integers of cardinality ρ and k a positive integer. Denote by $f_R(k)$ the smallest positive integer which cannot be represented in the form $\sum_{i=1}^{k-1} r_i a_i$ with $r_i \in R$, $a_i \in A$ for all i. Then*

(i) *if $1 \in R$, then $\log f_R(k) > k/c_6$ for some number $c_6 > 0$ depending only on b_1,*

(ii) *if all elements of R are positive, then $f_R(k) \le (1.5\rho k t \log(\rho k t))^{k-1}$,*

(iii) *there exists a constant c_9 such that $\log f_R(k) < (k \log(\rho t))^{c_9}$,*

(iv) *there exist a constant c_{11} and infinitely many positive integers k such that $\log f_R(k) \le c_{11} k \log(\rho k t) \log\log k$.*

In Nathanson's Problem 1 mentioned in the introduction we have $R = \{-1, 1\}$, and hence $\rho = 2$. Thus we have the following consequences for the function f.

Corollary 1. *There is a positive number c depending only on b_1 such that* $\log f(k) > ck$.
On the other hand, $\log f(k) < (k \log(2t))^C$ *where C is a constant.*
Moreover, $\log f(k) < c^* k \log(2kt) \log\log k$ *for infinitely many integers k where c^* is a constant.*

5. Some remarks

Remark 1. To prove that $f_R(k) > e^{ck}$ we assumed $1 \in R$. Here we check what happens if this condition is not fulfilled. Obviously, we may assume that $0 \notin R$ and that not all the elements of R are negative. Further, if the elements of R are not coprime, then there is a full residue class not represented as $\sum_{i=1}^{k} r_i a_i$. Therefore we may assume that the elements of R are coprime. (In particular, since $R = \{1\}$ is now excluded, that $\rho > 1$.)

Assume first that R contains a negative element. There exist integers d_j ($j = 1, \dots, \rho$) such that $\sum_{j=1}^{\rho} d_j r_j = 1$. Let $P = \prod_{j=1}^{\rho} |r_j|$. So P is a multiple of r_j for every j. Consider the sum $\sum_{j=1}^{\rho} \big(d_j + e_j \frac{P}{r_j}\big) r_j$ where the e_j's are integers such that $d_j + e_j \frac{P}{r_j} \geq 0$ and $e_j r_j \geq 0$ for all j. Let $v = \sum_{j=1}^{t} e_j$. If $v > 0$ then we replace e_j by $e_j - v$ for some j with $r_j < 0$, and if $v < 0$ then we do so for some j with $r_j > 0$. Afterwards $\sum_{j=1}^{t} e_j = 0$, hence $\sum_{j=1}^{\rho} \big(d_j + e_j \frac{P}{r_j}\big) r_j = 1$, and further $d_j + e_j \frac{P}{r_j} \geq 0$ for $j = 1, \dots, \rho$. Thus 1 admits a representation $\sum_{j=1}^{k} r_j a_j$ where $a_j = b_1^0 = 1$ for all j, and k is bounded by $\sum_{j=1}^{\rho} \big(d_j + e_j \frac{P}{r_j}\big)$, that is by a constant c_{12} which only depends on R.

If the elements of R are coprime and all positive, then we have to do with the so-called coin problem or Frobenius problem. Let $0 < r_1 \leq r_2 \leq \dots \leq r_\rho$. Schur [3] proved in 1935 that every number larger than $c_{13} := r_1 r_\rho + r_2 + \dots + r_{\rho-1}$ can be represented as a linear combination of $r_1, r_2, \dots, r_\rho$ with nonnegative integer coefficients. Note that c_{13} depends only on R. Therefore each of the integers in the interval $(c_{13}, 2c_{13}]$ can be represented as $\sum_{j=1}^{c_{14}} r_j a_j$ where the number c_{14} depends only on R. We can now use the greedy algorithm as in the first block of Section 4, iterating until we reach this interval, to obtain a representation of $n > c_{13}$ with at most $(c_6 + c_{14}) \log n$ terms $r_j a_j$.

We conclude that if the elements of R are coprime, every positive integer $n > c_{13}$ can be represented as $\sum_{i=1}^{k-1} r_i a_i$ with $r_i \in R$, $a_i \in A$ for all i and with $k < c_{15} \log n$, where c_{15} is a number depending only on R. Thus $f_R(k) > e^{ck}$ where c is a number depending only on R.

Remark 2. The upper bound for $f(k)$ can possibly be improved by deriving a version of Theorem 1 where the interval for m is essentially smaller at the cost of a larger bound for $\lambda(m)$. We expect that the given upper bound for infinitely many values of k may be close to an upper bound for all k.

Acknowledgements. The authors are grateful to the referees for their helpful remarks.

References

[1] Zs. Ádám, L. Hajdu and F. Luca, Representing integers as linear combinations of S-units, *Acta Arith.* **138** (2009), 101–107.

[2] L. M. Adleman, C. Pomerance and R. S. Rumley, On distinguishing prime numbers from composite numbers, *Ann. Math.* **117** (1983), 173–206.

[3] A. Brauer, On a problem of partitions, *Amer. J. Math.* **64** (1942), 299–312.

[4] P. Erdős, C. Pomerance and E. Schmutz, Carmichael's lambda function, *Acta Arith.* **58** (1991), 365–385.

[5] L. Hajdu, Arithmetic progressions in linear combinations of S-units, *Period. Math. Hungar.* **54** (2007), 175–181.

[6] M. Jarden and W. Narkiewicz, On sums of units, *Monatsh. Math.* **150** (2007), 327–332.

[7] M. B. Nathanson, Geometric group theory and arithmetic diameter, *Publ. Math. Debrecen* **79** (2011), xxx-xxx.

LAJOS HAJDU
INSTITUTE OF MATHEMATICS
UNIVERSITY OF DEBRECEN
AND THE NUMBER THEORY RESEARCH GROUP
OF THE HUNGARIAN ACADEMY OF SCIENCES
H-4010 DEBRECEN, P.O. BOX 12
HUNGARY

E-mail: hajdul@science.unideb.hu

ROBERT TIJDEMAN
MATHEMATICAL INSTITUTE
LEIDEN UNIVERSITY
2300 RA LEIDEN, P.O. BOX 9512
THE NETHERLANDS

E-mail: tijdeman@math.leidenuniv.nl

(Received February 7, 2011; revised August 16, 2011)