İstanbul Üniv. Fen Fak. Mat. Der. **50** (1991), 67-77

ON THE NUMBER OF REPRESENTATIONS OF AN INTEGER BY A LINEAR FORM

S. SERTÖZ - A. ÖZLÜK

We investigate the number of representations $r_n(N)$ for an integer N given in the Diophantine form

$$N = a_1 X_1 + \ldots + a_n X_n$$

where $a_1, \ldots, a_n$ are mutually prime natural numbers and $X_1, \ldots, X_n$ are nonnegative integers. We obtain a formula for the leading coefficient of the polynomial part of r_n for any n. We also show that r_n satisfies a rather strong recursive relation through which we can analyze the $n = 3$ case more thoroughly than done before. We apply these results to Hilbert polynomials of finitely generated modules.

1. INTRODUCTION

The celebrated problem of Frobenius consists of determining the largest natural number g which cannot be expressed in the form

$$N = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n \tag{1}$$

where $a_1, a_2, \ldots, a_n$ are relatively prime natural numbers and $x_1, x_2, \ldots, x_n$ are nonnegative integers. It is well known that for $n = 2$,

$$g = a_1 a_2 - a_1 - a_2 . \tag{2}$$

The existence of such a formula for $n = 2$, first given in [10], provoked a large number of researchers to look for similar formulas for higher n. For an introduction to the vast literature on Frobenius's problem see, for example, [7], [8] and the references given there. Despite intense work on this problem no closed formula for $n > 2$, such as equation (2) is available. Algorithms for computing g however exist and we have given one such algorithm in [9].

In this note, in association with this problem, we investigate the number of different representations $r_n(N; a_1, \ldots, a_n) = r_n(N)$ of N in the form of (1). We obtain by elementary means a formula for $r_n(N)$ valid for sufficiently large N and for mutually prime a_i. For $n = 3$ we do not lose any generality by the latter restriction, see [4] and [7].

Before we state our results let us first set the notation to be used throughout this article. For a positive integer n define

$$P_n = \prod_{i=1}^{n} a_i \tag{3}$$

$$S_n = \sum_{i=1}^{n} a_i \tag{4}$$

and let N_0 and x be defined by

$$N = N_0 P_n + x, \quad 0 \leq x < P_n \tag{5}$$

i.e. N_0 is the largest integer in $\frac{N}{P_n}$ and x is the number remaining after dividing N by P_n. Also define $S(a_1, \ldots, a_n)$ as the semigroup generated by the a_i's over the natural numbers.

$$S(a_1, \ldots, a_n) = \{a_1 x_1 + \ldots + a_n x_n \mid x_1, \ldots, x_n \in \mathbf{N}\}. \tag{6}$$

2. RESULTS AND COMMENTS

We can now summarize our results in the following theorems and corollaries (We number our results with the same index for easy reference).

Theorem 1. As N increases $r_n(N)$ becomes asymptotically close to $N^{n-1} \Big/ \left(\prod_{i=1}^{n} a_i\right) (n-1)!$. That is

$$r_n(N) \sim \frac{N^{n-1}}{\left(\prod_{i=1}^{n} a_i\right) (n-1)!} \quad \text{as } N \to \infty. \tag{7}$$

For small values of n ($n = 2, 3, 4$), we know exactly what $r_n(N)$ is :

Corollary 2 (see [3]). When $N \geq P_n$ we have

$$r_2(N) = \frac{N}{P_2} - \frac{x}{P_2} + r_2(x) \tag{8}$$

$$r_3(N) = \frac{N(N+S_3)}{2P_3} - \frac{x(x+S_3)}{2P_3} + r_3(x) \tag{9}$$

$$r_4(N) = A - B \cdot r_4(P_4 - 2) + (B + N_0) \cdot r_4(P_4 - 1) + r_4(x) \tag{10}$$

where in the last equation the coefficients A and B are given by

$$A = \frac{1}{2} \sum_{k=1}^{N_0} (N - k P_4 + 1)(N - k P_4 + 2) \tag{11}$$

$$B = \frac{1}{2} N_0 (N + x - P_4 + 2). \tag{12}$$

Note that in the expression for A the leading coefficient is $N^3/6 P_4$ as expected. In general we observe that $r_n(N)$ satisfies the following recursive relation which is the key theorem behind our results:

Theorem 3. When $N > P_n - S_n + n - 2$ we have the following relation for $r_n(N)$

$$1 = \sum_{k=N-n+2}^{N} C_{N-k} \cdot [r_n(k) - r_n(k - P_n)] \tag{13}$$

where

$$C_m = \begin{cases} (-1)^m \binom{n-2}{m} & \text{for } 0 \leq m \leq n-2 \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

Moreover we have:

Corollary 4 (see [3]). For every n there exists a polynomial $L_n(X)$ of degree $n - 1$ whose leading coefficient is the asymptotic limit of $r_n(N)$, i. e. $N^{n-1} / [P_n (n-1)!]$, and if we define $\Delta_n(N)$ as

$$\Delta_n(N) = r_n(N) - L_n(N) \tag{15}$$

then $\Delta_n(N)$ is periodic with period P_n.

As a consequence of this periodicity it suffices to know only $L_n(N)$ and $\Delta_n(x)$ in order to understand the behaviour of $r_n(N)$, where x is N mod P_n as in equation (5). This combined with Corollary 2 leads to the following:

Corollary 5. For $n = 2, 3, 4$ we have

$$\Delta_2(x) = r_2(x) - \frac{x}{P_2} \tag{16}$$

$$\Delta_3(x) = r_3(x) - \frac{x(x + S_3)}{2 P_3} \tag{17}$$

$$\Delta_4(x) = r_4(x) + \frac{x^3}{6 P_4} + \left(\frac{3 - P_4 + 2 r_4(P_4 - 1) - 2 r_4(P_4 - 2)}{4 P_4} \right) x^2 +$$

$$+ \left(\frac{12 - 9 P_4 + P_4^2 + 6 [4 - P_4] r_4(P_4 - 1) - 6 [2 - P_4] r_4(P_4 - 2)}{12 P_4} \right) x. \tag{18}$$

We remark that the periodic function $\Delta(X)$ can be expresed as a trigonometrical sum using the a_i^{th} roots of unity, the analysis of which will be discussed elsewhere.

We give an interesting combinatorical proof for the following old but beautiful formula :

$$r_3(P_3) = \frac{P_3 + S_3}{2} + 1. \tag{19}$$

Finally combining this formula with our full understanding of what happens in the $n = 2$ case and with the aid of our recursion formula we have an almost total understanding of what happens in the $n = 3$ case. Note that $r_n(N)$ for $N \geq P_3$ is given by equation (9). The case for $P_3 - S_3 + 1 \leq N < P_3$ is covered by the following theorem. For N smaller than that no formula seems possible at present and we call it the erratic region.

Corollary 6.

$$r_3(P_3) = r_3(P_3 - 1) + 2 \tag{20}$$

$$r_3(P_3 - t) = r_3(P_3 - t - 1) + 1 \text{ for } 1 \leq t \leq S_3 - 2. \tag{21}$$

In particular we have

$$r_3(P_3 - S_3 + 1) = \frac{P_3 - S_3}{2} + 1. \tag{22}$$

In the last section we apply these results to the theory of Hilbert-Samuel polynomials.

COMMENTS. 1) This problem has been attacked by several authors. In particular Ehrhart has analyzed it in [2] and [3] where he has used what he calls Euler's recursion formula. He then obtains formulas (8), (9) and (19). He has also observed the periodicity property of r_n as in equation (15). But he has tried to express the polynomial $L_n(x)$ in terms of $n' = x + \frac{S_3}{2}$. This approach it seems prevented him from obtaining the leading coefficient of $L_n(x)$ for a general n as we did in Theorem 1.

2) Our basic claim is that once $r_n(N)$ is known for $0 \leq N \leq P_n$ then r_n for a general N can be obtained from that information by an appropriate polynomial. Our recursion formula (13) seems stronger than the ones used before hence making it possible to find the polynomial mentioned in Corollary 4.

PROOFS AND DISCUSSIONS

We find it convenient to begin with the proof of our recursion formula.

Proof of Theorem 3. First observe that $Q_n(x)$ which is defined as

$$Q_n(x) = \frac{(1-x^{P_n})(1-x)^{n-2}}{(1-x^{a_1})\ldots(1-x^{a_n})} - \frac{1}{1-x} \tag{23}$$

is a polynomial of degree $P_n - S_n + n - 2$, since every root of the denominator is a root of the numerator with the same multiplicity. Using the fact that we are using only mutually prime integers $a_1, \ldots, a_n$ we can show immediately that

$$\frac{1}{\prod_{i=1}^{n}(1-x^{a_i})} = \sum_{t=0}^{\infty} r_n(t)\, x^t . \tag{24}$$

Substituting this and the usual expansion of $1/(1-x)$ into equation (23) we obtain the following expression for Q_n:

$$Q_n(x) = \sum_{t=0}^{\infty} [(1-x^{P_n})(1-x)^{n-2} r_n(t) - 1]\, x^t . \tag{25}$$

Since $Q_n(x)$ is a polynomial the coefficient of x^N is zero beyond the degree of Q_n, and this is equivalent to the statement of Theorem 3.

We will now use this theorem to demonstrate a proof of Corollary 2.

See [3, Prop. 10.2, Thm. 10.5] for another proof of the $n = 2, 3$ cases.

Proof of Corollary 2. Putting $n = 2$ in equation (13) gives

$$r_2(N) = r_2(N - P_2) + 1.$$

By successively subtracting P_2 from N we obtain equation (8) of the theorem. Putting $n = 3$ in equation (13) gives

$$r_3(N) = r_3(N-1) + r_3(N-P_3) - r_3(N-P_3-1) + 1. \tag{26}$$

This equation is valid for $N > \deg Q_3 = P_3 - S_3 + 1$. By induction we find

$$r_3(N) = r_3(N-k) + r_3(N-P_3) - r_3(N-P_3-k-1) + k. \tag{27}$$

We may substitute $N - P_3$ for k in this equation. Noting that r_3 of a negative number is zero we obtain

$$r_3(N) = r_3(P_3) + r_3(N-P_3) + N - P_3 . \tag{28}$$

By successively subtracting P_3 from N we obtain

$$r_3(N) = \frac{N^2}{2P_3} + \left(\frac{2r_3(P_3) - P_3}{2P_3}\right) N + \left(\frac{xP_3 - 2xr_3(P_3) - x^3}{2P_3} + r_3(x)\right). \tag{29}$$

We now substitute equation (19) in the above equation to obtain equation (9).

The last equation of the corollary is obtained in a similar but more tedious way and we leave it to the reader.

We now give an interesting proof of equation (19) for completeness since we used it in the above proof.

Proof of (19). We apply a reduction trick

$$r_3(P_3) = \sum_{t=0}^{P_2} r_2(P_3 - t a_3). \tag{30}$$

Define f_t and k_t by

$$P_3 - t a_3 = f_t P_2 + k_t, \quad 0 \leq k_t < P_2. \tag{31}$$

Using equation (8) in (30) gives

$$r_3(P_3) = \sum_{t=0}^{P_2} [f_t + r_2(k_t)]. \tag{32}$$

It is well known that $r_2(m) = 0$ for exactly half of the numbers between 0 and $P_2 - S_2$ inclusively. On the other hand it can be shown that $r_2(m) = 1$ for $P_2 - S_2 + 1 \leq m \leq P_2$. These give

$$\sum_{t=0}^{P_2} r_2(k_t) = \frac{P_2 + S_2 + 1}{2}. \tag{33}$$

The other sum in (32) is the number of lattice points in and on the triangle, except the ones on the x—axis, defined by the line $P_2 y = P_3 - a_3 x$ in the first quadrant (compare with (31)). These lattice points can be counted by first counting the lattice points in and on the rectangle defined by the three corners of the above triangle. Since $(a_3, P_2) = 1$, there are no lattice points on the diagonal except the two corners $(0, a_3)$ and $(P_2, 0)$. Thus the triangle contains, in addition to these two points, half of all the other lattice points of the rectangle. Subtracting from this number the $P_2 + 1$ lattice points which lie on the x—axis we obtain

$$\sum_{t=0}^{P_2} f_t = \frac{P_3 - P_2 + a_3 + 1}{2}. \tag{34}$$

Finally adding equations (33) and (34) gives the desired formula for $r_3(P_3)$.

Proof of Theorem 1. We use induction on n. The assertion for $n = 2$ follows from the equation (8) of Theorem 2. We apply the reduction trick, which we used before, to $r_{n+1}(N)$,

$$r_{n+1}(N) = \sum_{t=0}^{\left[\frac{N}{a_{n+1}}\right]} r_n(N - a_{n+1} t). \tag{35}$$

Defining y as $y = N - a_{n+1}[N/a_{n+1}]$ and applying the induction hypothesis to the r_n of equation (35) we get

$$r_{n+1}(N) = \sum_{t=0}^{\frac{N-y}{a_{n+1}}} \left\{ \frac{(N - a_{n+1} t)^{n-1}}{P_n \cdot (n-1)!} + O(N^{n-1}) \right\} \tag{36}$$

where the $O(\cdot)$ notation is used in the sense that

$$\lim_{N \to \infty} \frac{O(N^{n-1})}{N^{n-1}} = 0 .$$

We can further simplify equation (36) by using the binomial theorem;

$$r_{n+1}(N) = \sum_{t=0}^{\frac{N-y}{a_{n+1}}} \frac{(N - a_{n+1} t)^{n-1}}{P_n \cdot (n-1)!} + O(N^n)$$

$$= \frac{1}{P_n \cdot (n-1)!} \sum_{t=0}^{\frac{N-y}{a_{n+1}}} (N^{n-1} - C_1^{n-1} N^{n-2} a_{n+1} t + \ldots + (-1)^{n-1} a_{n+1}^{n-1} t^{n-1}) + O(N^n)$$

$$= \frac{1}{P_n \cdot (n-1)!} \left\{ N^{n-1} \left(\frac{N}{a_{n+1}} - y + 1 \right) - C_1^{n-1} N^{n-2} a_{n+1} \left(\frac{N^2}{2 a_{n+1}} + \ldots \right) + \right.$$

$$+ \ldots + (-1)^{k-1} C_{k-1}^{n-1} N^{n-k} a_{n+1}^{k-1} \left(\frac{N^k}{k a_{n+1}} + \ldots \right) +$$

$$\left. + \ldots + (-1)^{n-1} a_{n+1}^{n-1} \left(\frac{N^n}{n a_{n+1}} + \ldots \right) \right\} + O(N^n) =$$

$$= \frac{N^n}{P_n \cdot a_{n+1} \cdot (n-1)!} \left(1 - C_1^{n-1} \frac{1}{2} + \ldots + \right.$$

$$\left. \ldots + (-1)^{k-1} C_{k-1}^{n-1} \frac{1}{k} + \ldots + (-1)^{n-1} \frac{1}{n} \right) + O(N^n) =$$

$$= \frac{N^n}{P_{n+1} \cdot (n-1)!} \cdot \frac{1}{n} + O(N^n) = \frac{N^n}{P_{n+1} \cdot n!} + O(N^n), \tag{37}$$

where $C_j^i = \binom{i}{j}$. This then completes the proof of Theorem 1

Proof of Corollary 4. We can apply induction for this proof; the case $n = 2$ being already done in Corollary 2 equation (8). For the general case we need the following interesting relation:

$$r_n(N) = \sum_{t=0}^{N} \varepsilon_{N-t}\, r_{n-1}(t\,;\, P_2\,,\ a_3\,,\ldots,\ a_n) \tag{38}$$

where

$$\varepsilon_{N-t} = \begin{cases} 1 & \text{if } N - t \in S(a_1\,,\, a_2) \\ 0 & \text{otherwise.} \end{cases} \tag{39}$$

We briefly indicate a proof of this: Recalling equations (8) and (24) we can write

$$\frac{1 - x^{P_2}}{(1 - x^{a_1})\,(1 - x^{a_2})} = \sum_{t=0}^{\infty} \varepsilon_t\, x^t. \tag{40}$$

Again in the same way we play with the right hand side of equation (24)

$$\frac{1}{(1 - x^{a_1}) \ldots (1 - x^{a_n})} = \frac{1 - x^{P_2}}{(1 - x^{a_1})\,(1 - x^{a_2})}\ \frac{1}{(1 - x^{P_2})(1 - x^{a_3}) \ldots (1 - x^{a_n}).} \tag{41}$$

Finally the following interesting fact

$$Q_2\ x) = -\sum_{n \notin S(a_1\,,\, a_2)} x^n \tag{42}$$

combined with the equations (40) and (41) yields the desired equation (38). Going back to the proof we need to observe that $r_{n-1}(t\,;\, P_2\,,\, a_3\,,\ldots,\, a_n)$ can be written as a polynomial plus a periodic part which has period equal to $P_2\, a_3 \ldots a_n = P_n$. The sum of these terms will again be a polynomial plus a periodic part with the right period. The degree of this polynomial is given by Theorem 1.

Corollary 5 follows upon inspection. We pass to the proof of Corollary 6.

Proof of Corollary 6. Returning to equation (27) note that we chose k such that $N - k$ was equal to P_3 and our calculations sailed off smoothly. However we are allowed to make $N - k$ as small as $P_n - S_n + 1$ and N as small as $P_3 - S_3 + 2$, not necessarily at the same time. First let $N = P_3$ and $k = 1$ in equation (27) and recall that r_3 of a negative number is zero. This will give

$$r_3(P_3) = r_3(P_3 - 1) + 2. \tag{43}$$

Next letting $N = P_3 - t$ and $k = 1$, where $1 \leq t \leq S_3 - 2$, we have

$$r_3(P_3 - t) = r_3(P_3 - t - 1) + 1 \text{ for } 1 \leq t \leq S_3 - 2. \tag{44}$$

This gives us the interesting fact that the number of representations of N increases by one as N increases from $P_3 - S_3 + 1$ to $P_3 - 1$. Combining this with equation (43) and with the formula of $r_3(P_3)$ given in equation (19) will finally give us

$$r_3(P_3 - S_3 + 1) = \frac{P_3 - S_3}{2} + 1. \tag{45}$$

Thus equations (9, 43, 44, 45) allow us to have a complete understanding of the $n = 3$ case except the erratic interval up to $P_3 - S_3$.

REMARK. Note that in equation (36) we treated $r_n(N - a_{n+1}t)$ as obeying the induction hypothesis even when $N - a_{n+1}t$ is small. This is justified by the following analysis for these small values: When $a_1, \ldots, a_{n+1}$ are fixed there are only finitely many values of t, say K of such t, for which $r_n(N - a_{n+1}t)$ is not of the required form. For each such term we can replace $r_n(X)$ by

$$\frac{X^{n-1}}{P_n(n-1)!} + \left(r_n(X) - \frac{X^{n-1}}{P_n(n-1)!}\right)$$

which is of the form $\frac{X^{n-1}}{P_n(n-1)!} + O(N^n)$. The $\frac{X^{n-1}}{P_n(n-1)!}$ term contributes to (36) as claimed in (37). Only K of the $O(N^n)$ terms are added for each such contribution. The number of m's for which $r_n(m)$ is not of the required form depends only on $a_1, \ldots, a_n$, hence there is a finite upper bound for K independent of N. Hence K terms of the form $O(N^n)$ still add up to a term of the same form as claimed in (37).

HILBERT-SAMUEL POLYNOMIALS

Basic reference for the definitions used here is [1]. Let $A = \bigoplus_{m=0}^{\infty} A_m$ be a graded Noetherian ring, generated as a A_0-algebra by $\xi_1, \ldots, \xi_n$ which are homogeneous elements of A of degrees $a_1, \ldots, a_n$. Let $M = \bigoplus_{m=0}^{\infty} M_m$ be a finitely generated graded A-module, and λ be an additive function on the class of finitely generated A_0-modules with values in $\mathbf{Z}$. An example of such λ is the dimension function. Then the Poincaré series of M with respect to λ is $P(M, x) = \sum_{m=0}^{\infty} \lambda(M_m) x^m$. Moreover it is known that

$$P(M, x) = \left[f(x) \Big/ \prod_{i=1}^{m} (1 - x^{a_i})\right]$$

for some polynomial $f(x)$ with integer coefficients (Hilbert-Serre). The research here concentrates on obtaining more information on $P(M, x)$ and interpreting this information geometrically.

Denote the order of the pole of $P(M, x)$ at $x = 1$ by d. Let

$$f(x) = g(x)(1 - x)^r,$$

where $g(1) \neq 0$ and $r = m - d$. Now we apply our results to conclude following theorem:

Theorem. If $(a_i, a_j) = 1$ for $i \neq j$, then for m sufficiently large

$$\lambda(M_m) = F(m) + \delta(m)$$

where $F(x)$ is a polynomial with rational coefficients of degree $d - 1$ and δ is a periodic function from integers to integers, its period dividing $P_n = a_1 \ldots a_n$. The leading term of $F(x)$ is

$$\frac{g(1)}{(d-1)!\,P_n} x^{d-1}, \quad \text{for } d \geq 2,$$

Corollary. Define $H_i(m) = \lambda(M_{i+mP_n})$ for $0 \leq i \leq P_n$. Then for m large enough each $H_i(x)$ is a polynomial with rational coefficients and they all have the same leading term given by the above theorem. In fact $H_i(x)$ and $H_j(x)$ differ by an additive constant.

Corollary (Hilbert-Serre, [1]). When all $a_i = 1$, then for m large enough $\lambda(M_m)$ is a polynomial ($P_n = 1$ so we have only $H_0(x)$ defined and $\lambda(M_m) = H_0(m)$ for large m).

We conclude by quoting a result of Morales which is related to ours.

Theorem of Morales (see [5]). When $a_1, \ldots, a_n$ are arbitrary let $k_n = l.c.m.(a_1, \ldots, a_n)$ and define $H_i(m) = \lambda(M_{i+mk_n})$ for $0 \leq i \leq k_n$. Then for sufficiently large m each $H_i(x)$ is a polynomial with rational coefficients.

In [6] Morales applies these results to examine the geometry of space curves in lower dimensional spaces.

REFERENCES

[1] ATIYAH, M.F. and MACDONALD, I.G. : Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass., 1969.

[2] EHRHART, E. : *Sur un problème de géometrie diophantienne linéaire* I, J. reine angew. Math., **226** (1965), 1-29.

[3] EHRHART, E. : *Sur un problème de géometrie diophantienne linéaire* II, J. reine angew. Math., **227** (1966), 30-54.

[4] JOHNSON, S.M. : *A linear Diophantine problem*, Canadian J. Math., **12** (1960), 390-398.

[5] MORALES, M. : *Fonctions de Hilbert, genre géometrique d'une singularité quasi homogène Cohen-Macaulay*, C. R. Acad. Sci. Paris, **301**, Série 1, no 14 (1985), 699-702.

[6] MORALES, M. : *Syzygies of monomial curves and a linear problem of Frobenius*, Preprint of Max-Planck Institut für Mathematik, Bonn (1987).

[7] RODSETH, O.J. : *On a linear Diophantine problem of Frobenius*, J. reine angew. Math., **301** (1978), 171-178.

[9] SELMER, E.S. : *On the linear Diophantine problem of Frobenius*, J. reine angew. Math., **293/294** (1977), 1-17.

[10] SERTÖZ, S. and ÖZLÜK, A. : *On a Diophantine problem of Frobenius*, Bulletin of the Technical University of Istanbul, **39** (1986), 41-51.

[10] SYLVESTER, J. J. : Educational Times, **41** (1884), 21.

SİNAN SERTÖZ
BİLKENT UNIVERSITY
DEPARTMENT OF MATHEMATICS
P.K. 8, 06572 MALTEPE
ANKARA, TURKEY

ALİ ÖZLÜK
UNIVERSITY OF MAINE
DEPARTMENT OF MATHEMATICS
NEVILLE HALL, ORONO, MAINE
04469 U.S.A.

Ö Z E T

Aralarında asal olan $a_1, \ldots, a_n$ gibi n tam sayının negatif olmayan tam katsayılarla oluşturulan lineer bileşenleri arasında N tam sayısının kaç değişik şekilde görüleceğini $r_n(N)$ ile gösterelim. Bu makalede $r_n(N)$ in polinom kısmının ilk terimini her n için veren bir formül buluyoruz. Ayrıca $r_n(N)$ fonksiyonunun N değişkeni üzerinde güçlü bir tekrar denklemi sağladığını gösteriyoruz. Bunu kullanarak $n = 3$ halini ayrıntılı olarak inceleyebiliyoruz. Bulduğumuz genel sonuçları Hilbert polinomları teorisine uyguluyoruz.