ACTA ARITHMETICA
XXXI (1976)

On a linear diophantine equation[*]

by

EUGENE L. GOLDBERG (New York, N.Y.)

Given a finite set of positive integers $S = \{s_1, \ldots, s_k\}$, let

$$\mathrm{sp}(S) = \Big\{\sum_{i=1}^{k} a_i s_i\colon\ a_i \text{ are non-negative integers}\Big\}.$$

Thus, $\mathrm{sp}(S)$ is the subsemigroup generated by S considered as a subset of the semigroup of non-negative integers under addition. It is known that $\mathrm{sp}(S)$ contains all sufficiently large multiples of $\mathrm{GCD}(s_1, \ldots, s_k)$. In particular if this GCD is 1, $\mathrm{sp}(S)$ contains all sufficiently large integers, and we let

$$\theta(S) = \text{the largest integer not in } \mathrm{sp}(S).$$

The object of this paper is to calculate $\theta(S)$ for two special types of sets. The principal results are:

1. Given positive integers a, b with $1 < a < b$ and $\mathrm{GCD}(a, b) = d$, for all sufficiently large n such that $\mathrm{GCD}(n, d) = 1$;

$$\theta(\{n, n+a, n+b\}) = \begin{cases} \Big(\dfrac{a}{d}+x_0+y_0+d-3)n+b\Big(\dfrac{a}{d}-1\Big)-a, & \text{if } dx_0 \geqslant b-a, \\ \Big(\dfrac{b}{d}+y_0+d-3\Big)n+b\Big(\dfrac{a}{d}-1\Big)-a(x_0+1), & \text{if not,} \end{cases}$$

where $dn = ax_0+by_0$ with $0 \leqslant x_0 < b/d$ and $0 \leqslant y_0$.

2. Given $1 < a_1 < a_2 < \ldots < a_k$ such that $a_i | a_{i+1}$ for $i = 1, \ldots, k-1$, let $S = \{n, n+1, n+a_1, \ldots, n+a_k\}$. If n is large enough,

$$\theta(S) = \left(\left[\frac{n}{a_k}\right]+a_1+\frac{a_2}{a_1}+\ldots+\frac{a_k}{a_{k-1}}-k-2\right)n+\left[\frac{n}{a_k}\right]a_k+a_k-a_{j_0}-1,$$

where a_{j_0} is the smallest a_j with $a_k-a_j \leqslant n-\left[\dfrac{n}{a_k}\right]a_k$.

[*] Research supported in part by the National Science Foundation.

The basic idea in the proof of the first result is to reduce the problem to a problem involving only two numbers. For two numbers $\operatorname{sp}(S)$ is known completely. The following lemmas and corollary express the situation.

LEMMA 1. *If* $\mathrm{GCD}(a,b)=1$, *then for any integer* n, *the equation* $n=ax+by$ *is solvable in integers. Furthermore, if* (x_0,y_0) *is one solution, all other solutions are given by*

$$x=x_0-bt,\qquad y=y_0+at \qquad \textit{as } t \textit{ varies over the integers.}$$

Proof ([2], p. 21).

From Lemma 1, we immediately deduce

LEMMA 2. *If* $\mathrm{GCD}(a,b)=1$, *then the equation* $n=ax+by$ *does not have a solution in non-negative integers if and only if*

$$n=ax_0-by_0 \qquad \textit{with} \qquad 0\leqslant x_0<b \ \textit{ and } \ 1\leqslant y_0.$$

Letting $x_0=b-1$ and $y_0=1$, we obtain

COROLLARY. *If* $\mathrm{GCD}(a,b)=1$, *then* $\theta(\{a,b\})=ab-a-b$.

All of the work in the proof of the first result is in the case of $\mathrm{GCD}(a,b)=1$. Thus, in the interest of clarity, we first assume the GCD is 1. Note, that the assumption that $n=ax_0+by_0$ can be solved in non-negative integers is, after the corollary, true for $n\geqslant(a-1)(b-1)$.

THEOREM 1. *Given* a,b *such that* $1<a<b$ *and* $\mathrm{GCD}(a,b)=1$, *if* $n>b(b-a-2)$ *and* $n=ax_0+by_0$ *with* $0\leqslant x_0<b$ *and* $0\leqslant y_0$, *then*

$$\theta(\{n,n+a,n+b\})=\begin{cases}(a+x_0+y_0-2)n+b(a-1)-a, & \textit{if } x_0\geqslant b-a,\\ (b+y_0-2)n+b(a-1)-a(x_0+1), & \textit{if not.}\end{cases}$$

Proof. Observe that if the equation $X=a(n+a)+\beta(n+b)+\gamma n$ has a solution with non-negative a,β,γ, so does the equation with X replaced by $X+mn$ with $m\geqslant 0$. Hence, for each congruence class modulo n, there is a dividing line, before which all numbers cannot be represented while after they can. The first part of the proof studies this line. It will be shown to be a simple function of the first number in the congruence class that can be represented by a, b. The second part of the proof maximizes over congruence classes and produces θ.

Part 1. For each r, $0\leqslant r<n$, let

$X(r)=$ the smallest integer X congruent to r modulo n such that $X=a(n+a)+\beta(n+b)+\gamma n$ has a solution with a,β,γ non-negative integers.

It is clear that in the representation of $X(r)$, $\gamma=0$. Thus if $aa+\beta b=r+\delta n$ then $X(r)=(a+\beta+\delta)n+r$. For r, δ such that $ax+by=r+\delta n$ has a non-negative solution let

(1) $\quad X(r,\delta)=\min\big((a+\beta+\delta)n+r\big)$ over all solutions to $aa+\beta b=r+\delta n$ with $a,\beta\geqslant 0$.

Then

$$X(r)=\min_{\delta} X(r,\delta).$$

From the corollary $X(r,\delta)$ is defined for all sufficiently large δ. However, since $X+cn=X+c(ax_0+by_0)$ we see that for a fixed r, if $X(r,\delta)$ is defined for some δ, then it is defined for all larger δ.

Claim: $X(r,\delta)$ is a non-decreasing function on its domain of definition. Among all solutions to $r+\delta n=ax+by$ with $x,y\geqslant 0$, $x+y$ is smallest for the solution with $0\leqslant x<b$. Thus $X(r,\delta)=(a+\beta+\delta)n+r$ where $0\leqslant a<b$, $0\leqslant\beta$, and $aa+\beta b=r+\delta n$. Now we calculate $X(r,\delta)$ explicitly as a function of δ. Choose $a',b'\geqslant 0$ such that $aa'-bb'=1$. Then

$$r+\delta n=a\big(a'(r+\delta n)\big)+b\big(-b'(r+\delta n)\big).$$

By Lemma 1

$$a=a'(r+\delta n)-b\left[\frac{a'(r+\delta n)}{b}\right],\qquad \beta=-b'(r+\delta n)+a\left[\frac{a'(r+\delta n)}{b}\right].$$

Hence

$$\frac{1}{n}\big(X(r,\delta+1)-X(r,\delta)\big)$$
$$=1+n(a'-b')+(b-a)\left\{\left[\frac{a'(r+\delta n)}{b}\right]-\left[\frac{a'\big(r+(\delta+1)n\big)}{b}\right]\right\}.$$

Using the fact that the expression in braces is $\geqslant\big((a'n/b)+1\big)$ and the bound on n, we obtain

$$1/n\big(X(r,\delta+1)-X(r,\delta)\big)>-1.$$

Since the left-hand side is an integer, the claim is proved.

Therefore

(2) $\quad X(r)=X(r,\delta_0)$ where δ_0 is minimal such that $r+\delta_0 n=ax+by$ has a non-negative solution.

Part 2. Clearly,

$$\theta\big(\{n,n+a,n+b\}\big)=\max_r\big(X(r)-n\big).$$

The numbers $r+\delta_0 n$ that appeared in Part 1, are precisely those numbers R such that $R=ax+by$ has a non-negative solution but $R-n$ does not.

Thus by (1), (2),

$$\theta(\{n, n+a, n+b\}) = \max\big((\alpha+\beta)n+R-n\big) \text{ over } R \text{ such that } R = a\alpha+b\beta,\ 0 \leqslant \alpha < b,\ 0 \leqslant \beta \text{ and } R-n \text{ does not have a non-negative solution.}$$

By Lemma 2, $R-n = by-ax$, $0 \leqslant y < a-1$, $1 \leqslant x$.

The argument now splits into three cases according to the size of x. We compute the maximum for each case and θ is the maximum of the three.

Case (i). $x \geqslant b$. Thus $R-n \leqslant -b$. Hence

$$n-b \geqslant R = au+bv \quad \text{with} \quad 0 \leqslant u < b,\ 0 \leqslant v.$$

Therefore, $u+v \leqslant u+\left[\dfrac{n-b-au}{b}\right]$.

The function of u on the right-hand side is clearly non-decreasing, so

$$u+v \leqslant (b-1)+\left[\frac{n-b-a(b-1)}{b}\right] \leqslant (b-1)+\left[\frac{n-b-ax_0}{b}\right] = b-2+y_0.$$

Finally $X(r) \leqslant (b-2+y_0)n-b$ in this case.

Case (ii). $1 \leqslant x \leqslant x_0$. Then

$$R = a(x_0-x)+b(y_0+y)$$

is the appropriate representation of R, and

$$X(r) \leqslant (x_0+y_0+a-1)+b(a-1)-b-n$$

with equality for

$$r \equiv R_1 = ab-a-b \bmod n \quad \text{if} \quad x_0 \geqslant 1.$$

Case (iii). $x_0 < x \leqslant b-1$. Then

$$R = a(x_0-x+b)+b(y_0+y-a)$$

is the appropriate representation and

$$X(r) \leqslant (b+y_0-1)n+b(a-1)-a(x_0+1)-n$$

with equality for

$$r \equiv R_2 = ab-a-b-ax_0 \bmod n \quad \text{if} \quad x_0 < b-1.$$

In Cases (ii) and (iii), the choice of x, y made maximizes both the sum $\alpha+\beta$ and R. As δ is obviously a monotone function of R this choice maximizes X. Notice that the maximum in (iii) majorizes the bound in (i). Finally since $0 \leqslant ax_0 \leqslant n$

$$R_1 \geqslant R_2 \geqslant R_1-n.$$

The statement about which case leads to the maximum follows easily.

If $\mathrm{GCD}(a, b) = d > 1$, then we must assume $\mathrm{GCD}(n, d) = 1$ in order to have $\mathrm{GCD}(n, n+a, n+b) = 1$. Also, since $ax+by$ now only represents multiples of d, we change the assumption to nd can be represented. The proof will show that we may cancel all the d's.

THEOREM 2. *Given a, b with $1 < a < b$ and $\mathrm{GCD}(a, b) = d > 1$ i, $(n, d) = 1$, $nd^2 > b(b-a-2d)$, and $dn = ax_0+by_0$ with $0 \leqslant x_0 < b/df$ $0 \leqslant y_0$, then*

$$\theta(\{n, n+a, n+b\}) = \begin{cases} \left(\dfrac{a}{d}+x_0+y_0+d-3\right)n+b\left(\dfrac{a}{d}-1\right)-a, & \text{if } dx_0 \geqslant b-a, \\ \left(\dfrac{b}{d}+y_0+d-3\right)n+b\left(\dfrac{a}{d}-1\right)-a(x_0+1), & \text{if not.} \end{cases}$$

Proof. With only minor alteration of the proof as in Theorem 1 we obtain equation (2) again

$$X(r) = X(r, \delta_0) \text{ where } \delta_0 \text{ is minimal such that } ax+by = r+\delta_0 n \text{ has a non-negative solution.}$$

Let $R = r+\delta_0 n$.

The representations of R tell us that $R \equiv 0 \bmod d$ and $R \equiv r \bmod n$. Hence there is a unique congruence class r_1 modulo nd such that

$$R \equiv r_1 \bmod nd.$$

Since $r_1 \equiv 0 \bmod d$ we have

$$r_1 \equiv dr_2 \bmod nd$$

for a unique $r_2 \bmod n$. Thus

$$R = dr_2+\delta_1 dn$$

and

$$R = ax = by \quad \text{if and only} \quad \text{if } r_2+\delta_1 n = \frac{a}{d}x+\frac{b}{d}y.$$

Therefore if R leads to $\theta(\{n, n+a/d, n+b/d\})$ then dR will lead to $\theta(\{n, n+a, n+b\})$

$$dR_1 = b(a/d-1)-a+dn,$$
$$dR_2 = b(a/b-1)-a(x_0+1)+dn.$$

Finally since $\theta(\{n, n+a, n+b\}) = \max\big(X(r)-n\big)$ the theorem follows.

The case where $a = 1$ has been excluded so far because in that case $r = ax+by$ is automatically satisfied. Thus the second and third cases, which are primarily concerned with r such that $\delta_0 > 0$ do not arise. However this case is contained in the following

THEOREM 3. *Given integers* $1 = a_0 < a_1 < \ldots < a_k$ *such that* $a_i | a_{i+1}$ *for* $i = 1, \ldots, k-1$, *if* $n > a_k(a_k-2)$ *then*.

$$\theta(\{n, n+1, n+a_1, \ldots, n+a_k\})$$
$$= \left(\left[\frac{n}{a_k}\right] + a_1 + \frac{a_2}{a_1} + \ldots + \frac{a_k}{a_{k-1}} - k - 2\right)n + \left[\frac{n}{a_k}\right]a_k + a_k - a_{j_0} - 1,$$

where a_{j_0} *is the smallest* a_j *such that* $a_k - a_j \leqslant n - a_k[n/a_k]$.

Proof. The proof follows the lines of the proof of Theorem 1, except now R will be represented by $1, a_1, a_2, \ldots, a_k$.

Part 1. For $0 \leqslant r < n$ let

$$X(r) = (b_0 + b_1 + \ldots + b_k)n + b_0 + b_1 a_1 + \ldots + b_k a_k$$

be the smallest $X \equiv r \bmod n$ such that

$$X \equiv b_0(n+1) + b_1(n+a_1) + \ldots + b_k(n+a_k) \quad \text{with} \quad b_i \geqslant 0.$$

Claim: among all solutions to $R = b_0 + b_1 a_1 + \ldots + b_k a_k$ with $b_i \geqslant 0$, $b_0 + \ldots + b_k$ is smallest for the solution that has $b_k = [R/a_k]$ and $0 \leqslant b_j < a_{j+1}/a_j$ for $j = 0, \ldots, k-1$.

The claim will be proved by induction on k. It is clear for $k = 0$. Suppose it for $k = j-1$.

Let $R = b_0 + b_1 a_1 + \ldots + b_j a_j$ be the recommended solution and let $R = c_0 + c_1 a_1 + \ldots + c_j a_j$ be any other. Finally suppose

(3) $$c_j = b_j - \delta, \qquad \delta \geqslant 0.$$

By induction hypothesis

(4) $$c_0 + c_1 + \ldots + c_{j-1} \geqslant d_0 + d_1 + \ldots + d_{j-1}$$

where

$$d_{j-1} = \left[\frac{R - b_j a_j + \delta a_j}{a_{j-1}}\right], \quad 0 \leqslant d_i < \frac{a_{i+1}}{a_i}, \quad d_0 + d_1 a_1 + \ldots + d_j a_j = R - c_j a_j.$$

Since a_j/a_{j-1} is an integer

(5) $$d_{j-1} = \left[\frac{R - b_j a_j}{a_{j-1}}\right] + \delta(a_j/a_{j-1}) = b_{j-1} + \delta(a_j/a_{j-1}).$$

Then $R - c_j a_j - d_{j-1} a_{j-1} = r - b_j a_j - b_{j-1} a_{j-1}$ and therefore

(6) $$b_i = d_i \quad \text{for} \quad i = 0, \ldots, j-2.$$

It follows from (3)–(6) that

$$c_0 + c_1 + \ldots + c_j > b_0 + b_1 + \ldots + b_j$$

and the claim is proved.

As in the proof of Theorem 1, we define $X(r, \delta)$ and as before the assumption on n insures $X(r, \delta)$ is non-decreasing. Thus $\delta = 0$.

Part 2. We are reduced to considering r with $0 \leqslant r < n$ and we must maximize $b_0 + \ldots + b_k$ and then choose the largest r in case of a tie. Clearly we have

$$b_k = \left[\frac{n-1}{a_k}\right] \quad \text{or} \quad \left[\frac{n-1}{a_k}\right] - 1$$

since in any other case we could replace b_k by $b_k + 1$, leave all other b_i the same and remain less than n.

$(b_0 + \ldots + b_{k-1})$ is maximum for $a_k - 1$ and is within 1 of the maximum only for $a_k - a_j - 1$, $j = 0, \ldots, k-1$. Hence the maximum value of

$$b_0 + \ldots + b_k = \left[\frac{n}{a_k}\right] + (a_1 - 1) + \left(\frac{a_2}{a_1}\right) + \ldots + \left(\frac{a_k}{a_{k-1}} - 1\right) - 1.$$

Note. Only in the case where $n \equiv 0 \bmod a_k$ can we realize both the maximum possible values of b_k and $b_0 + \ldots + b_{k-1}$. The change from $n-1$ to n in the greatest integer function is to include this case.

From the characterization of which numbers have maximal sums

$$r = \left[\frac{n}{a_k}\right]a_k + a_k - a_{j_0} - 1,$$

where a_{j_0} is minimal such that $r < n$.

Subtracting n as before the theorem follows.

In conclusion there are a few points to make about the hypotheses of the theorems. In all cases the lower bound for n can be lowered by better estimates. However in no case can it be eliminated by this method of proof.

If n is sufficiently small, the functions that were shown to be non-decreasing are not. It then appears complicated to chose the proper δ.

In the first two theorems, the assumption that n can be represented allows us to only look at R such that $R - n$ cannot be represented. If n is not representable then it is possible for $R - n$ to be unrepresentable while $R - 2n$ is. For example if $R - n = ab - a - b$ and n cannot be represented then $R - 2n$ can be.

Finally, the divisibility conditions of Theorem 3 are only used to show the form of the solution with minimum sum. However with no condition the answer is wrong. For example $a_0 = 1$, $a_1 = 3$, $a_2 = 4$ and $R = 6$.

For the interested reader, I have listed a few of the many related papers. As an historical note, the questions raised were first posed in a lecture by Frobenius.

Bibliography

[1] P. Erdös and R. L. Graham, *On a linear diophantine problem of Frobenius*, Acta Arith. 21 (1972), pp. 399–408.

[2] G. H. Hardy and E. M. Wright, *The Theory of Numbers*, 4th ed., Oxford University Press, 1960.

[3] B. R. Heap and M. S. Lynn, *A graph theoretic algorithm for the solution of a linear diophantine equation*, Numerische Math. 6 (1964), pp. 346–354.

[4] S. M. Johnson, *A linear diophantine problem*, Canad. J. Math. 12 (1960), pp. 390–398.

[5] N. S. Mendelsohn, *A linear diophantine equation with applications to nonnegative matrices*, Ann. N. Y. Acad. Sci. 175. art. 1 (1970), pp. 287–294.

Received on 23. 1. 1975 (666)

ACTA ARITHMETICA
XXXI (1976)

On c-semigroups

by

LADISLAV SKULA (Brno)

A semigroup with a divisor theory in which all factorizations into irreducibles of a given element have the same length is called a *c-semigroup*.

In his paper [1] L. Carlitz has proved that *the multiplicative semigroup of the ring of all algebraic integers of a number field is a c-semigroup if and only if that ring has class number* $\leqslant 2$.

In Narkiewicz's book [3] the following problem (no. 29) is posed: *Characterize Dedekind domains in which all factorizations into irreducibles of a given element have the same length.*

In this paper it is shown that the property *to be a c-semigroup* depends on the so-called *c-characteristic* of a semigroup (with a divisor theory) that is equal to the pair consisting of its divisor class group and of the image of the canonical mapping of all prime divisors into that group (Proposition 2.3).

From Claborn's Realization Theorem ([2], Theorem 15.18) it follows that *for every pair consisting of a commutative group and its any strong systems of generators there exists a Dedekind domain for which that pair is its c-characteristic* (Theorem 2.4).

For a subset of a commutative group the notion of *c-set* is introduced by means of the properties of that group only. It is shown (Proposition 2.3, Theorems 2.6, 2.7) that *the c-characteristics of c-semigroups are just the commutative groups and their strong systems of generators which are c-sets of those groups.*

In Section 3 the c-sets of elements of finite orders of a commutative group are characterized by Theorem 3.1, from which the characterization of all c-sets of the cyclic group of order p^n (p a prime, n a positive integer) is derived (Proposition 3.4). An analogous characterization of all c-sets of a finite cyclic group remains an open question.

1. Fundamental concepts

1.1. In this paper all groups considered are commutative and additive notation is employed. For semigroups multiplicative notation is employed. (If a semigroup is a group, then we use additive and multi-