MATH. SCAND. 67 (1990), 190–192.

ON FORMULAS FOR THE FROBENIUS NUMBER OF A NUMERICAL SEMIGROUP

FRANK CURTIS

Let $S = \langle s_1, \ldots, s_n \rangle$ be the numerical semigroup generated by relatively prime positive integers $s_1, \ldots, s_n$, that is, $S = \left\{ \sum_{i=1}^{n} a_i s_i \mid a_i \in \mathbf{N} \right\}$, where $\mathbf{N} = \{0, 1, \ldots\}$. The Frobenius number of S, $g(S)$, is the largest integer not in S. If $n = 2$, then $g(S) = s_1 s_2 - s_1 - s_2$ [3]. In the case $n = 3$, algorithms for computing $g(S)$ have been given gy Selmer and Beyer [2] and by Rödseth [4]. The purpose of this note is to prove that in the case $n = 3$, and consequently in all cases $n \geqq 3$, $g(S)$ cannot be given by closed formulas of a certain type. The main result is the following theorem.

THEOREM. *Let $A = \{(s_1, s_2, s_3) \in \mathbf{N}^3 \mid s_1 < s_2 < s_3,\ s_1$ and s_2 are prime, and $s_i \nmid s_3$ for $i = 1, 2\}$. Then there is no nonzero polynomial $F \in \mathbf{C}[X_1, X_2, X_3, Y]$ such that $F(s_1, s_2, s_3, g(\langle s_1, s_2, s_3 \rangle)) = 0$ for all $(s_1, s_2, s_3) \in A$.*

The corollary below shows that $g(\langle s_1, s_2, s_3 \rangle)$ cannot be determined by any set of closed formulas which could be reduced to a finite set of polynomials when restricted to A.

COROLLARY. *There is no finite set of polynomials $\{f_1, \ldots, f_n\}$ such that for each choice of s_1, s_2, s_3, there is some i such that $f_i(s_1, s_2, s_3) = g(\langle s_1, s_2, s_3 \rangle)$.*

PROOF. $F = \prod_{i=1}^{n} (f_i(X_1, X_2, X_3) - Y)$ would vanish on A.

The proof of the theorem depends on the construction of certain infinite classes of semigroups, which is carried out in the next two lemmas.

LEMMA 1. *Let $\alpha \in \mathbf{R}^+$, and let $\varepsilon > 0$ be given. Let p be a prime, and $i, j \in \mathbf{N}$ with $(p, i) = (p, j) = 1$. Then there exist $x, y \in \mathbf{N}$ such that x is prime, $x \equiv i \pmod p$, $y \equiv j \pmod p$, $(x, y) = 1$, and $|\alpha - y/x| < \varepsilon$.*

Received November 28, 1989

PROOF. We may assume $\varepsilon < \alpha$. Choose $n > 1/\varepsilon$ and let $q/r, s/t \in (\alpha - \varepsilon, \alpha + \varepsilon)$ be adjacent elements in the Farey sequence F_n. As $|rs - qt| = 1$, the following system of equations has a solution in $\mathbf{Z}/p\mathbf{Z}$:

$$\bar{r}U + \bar{t}V = \bar{i}$$
$$\bar{q}U + \bar{s}V = \bar{j}$$

Let $U = \bar{u}$, $V = \bar{v}$, for some u, v > 0, be the solution. If necessary, we can relabel q/r and s/t, so that we may assume $p \not| u$. Then, by Dirichlet's theorem, we can choose $a \geqq 0$ so that $u' = ap + u$ is prime, $(u', v) = 1$, and $u' > t$. Then $ru' + tv \equiv i \pmod p$, so $(p, ru' + tv) = 1$. From $(t, r) = (t, u') = (u', v) = 1$, we also have $(t, ru' + tv) = (u', ru' + tv) = 1$. So $(ptu', ru' + tv) = 1$, and we can choose $b \geqq 0$ so that $ru' + tv + bptu'$ is prime. Let $v' = v + bpu'$. Then $(u', v') = 1$, and $x = ru' + tv'$, $y = qu' + sv'$ satisfy the lemma.

If $s \in S$ and $s \neq 0$, let $S(s)$ denote the set of all $t \in S$ such that t is the smallest element in S in some residue class modulo s. Then $g(S) = t - s$, where t is the largest element in $S(s)$ [1].

LEMMA 2. *Let* $S = \langle s_1, s_2, s_3 \rangle$, *where* $2 < s_1 < s_2 < s_3$. *Let* $2 \leqq k \leqq (s_1 - 1)/2 + 1$, *and suppose* $s_1 - k < s_3/s_2 < s_1 - k + 1$, $s_2 \equiv 1 \pmod{s_1}$, $s_3 \equiv s_1 - k + 1 \pmod{s_1}$. *Then* $g(\langle s_1, s_2, s_3 \rangle) = (k-2)s_2 + s_3 - s_1$.

PROOF. We first show that $(k-2)s_2 + s_3 \in S(s_1)$. Suppose not. Then, as $(k-2)s_2 + s_3 \equiv s_1 - 1 \pmod{s_1}$, we have $as_2 + bs_3 < (k-2)s_2 + s_3$ for some $a, b \geqq 0$, with $as_2 + bs_3 \equiv s_1 - 1 \pmod{s_1}$. If $b = 0$, then $s_2 \equiv 1 \pmod{s_1}$ implies $a \geqq s_1 - 1$. Thus $(s_1 - 1)s_2 < (k-2)s_2 + s_3$, which would imply $s_1 - k + 1 < s_3/s_2$, a contradiction. If $b = 1$, then $a \equiv k - 2 \pmod{s_1}$, so $a \geqq k - 2$, and $as_2 + bs_3 \geqq (k-2)s_2 + s_3$, contrary to assumption. So $b \geqq 2$, and $2s_3 < (k-2)s_2 + s_3$. Then $s_3/s_2 < k - 2$, which implies $s_1 - k < k - 2$, i.e. $s_1/2 + 1 < k$, contrary to the choice of k. So $(k-2)s_2 + s_3 \in S(s_1)$.

For $m = 0, 1, \ldots, s_1 - k$, we have $ms_2 \equiv m \pmod{s_1}$, and $s_3/s_2 > s_1 - k \geqq m$, so $s_3 > ms_2$ and $(k-2)s_2 + s_3 > ms_2$. Foe $m = s_1 - k + 1, \ldots, s_1 - 2$, we have $(m - (s_1 - k + 1))s_2 + s_3 \equiv m \pmod{s_1}$, and $(m - (s_1 - k + 1))s_2 + s_3 < (k-2)s_2 + s_3$. So $(k-2)s_2 + s_3$ is the largest element in $S(s_1)$, and $g(S) = (k-2)s_2 + s_3 - s_1$.

PROOF OF THE THEOREM. Assume such a polynomial F exists. Fix a prime $p \neq 2$ and let $2 \leqq k \leqq (p-1)/2 + 1$. Let $G(X_2, X_3) = F(p, X_2, X_3, (k-2)X_2 + X_3 - p)$. Let $\alpha \in (p - k, p - k + 1)$ be irrational. For $n = 1, 2, 3, \ldots$, choose, by lemma 1, $x_n \equiv 1 \pmod p$, $y_n \equiv p - k + 1 \pmod p$, with x_n prime, $(x_n, y_n) = 1$ and $|\alpha - y_n/x_n| < 1/n$. Then $(p, x_n, y_n) \in A$, and by lemma 2, $G(x_n, y_n) = 0$. Let $G^*(X_2, X_3, Z)$ be the homogenization of G with respect to Z in $\mathbf{C}[X_2, X_3, Z]$. Then $G^*(x_n, y_n, 1) = 0$, which implies $G^*(1, y_n/x_n, 1/x_n) = 0$, and thus

$G^*(1, \alpha, 0) = 0$, by continuity, for any irrational $\alpha \in (p-k, p-k+1)$. So the projective curve $\mathscr{V}(G^*)$ contains infinitely many points $(1:\alpha:0)$, and thus $\mathscr{V}G^*)$ contains $\mathscr{V}(Z)$. It follows that $Z|G^*$, thus $G(X_2, X_3) = 0$.

Fix a prime $p > 2$, let $H(X_2, X_3, Y) = F(p, X_2, X_3, Y)$, and let $H^*(X_2, X_3, Y, Z)$ be the homogenization of H with respect to Z in $\mathbf{C}[X_2, X_3, Y, Z]$. Then H^* vanishes on the hyperplanes $\mathscr{V}((k-2)X_2 + X_3 - Y - pZ)$ for $k = 2, \ldots, (p-1)/2 + 1$, so $\deg H = \deg H^* \geqq (p-1)/2$. Thus $\deg F \geqq (p-1)/2$ for every prime $p > 2$, and there is no such F.

REFERENCES

1. A. Brauer and J. E. Shockley, *On a problem of Frobenius*, J. Reine Angew. Math. 211 (1962), 215-220.
2. B. E. S. Selmer and Ö. Beyer, *On a linear diophantine problem of Frobenius in three variables*, J. Reine Angew. Math. 301 (1978), 161-170.
3. J. J. Sylvester, *Mathematical questions with their solutions*, Educational Times 41 (1884), 21.
4. Ö. J. Rödseth, *On a linear diophantine problem of Frobenius*, J. Reine Angew. Math. 301 (1978), 171-178.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF MAINE
336 NEVILLE HALL
ORONO, ME 04469
U.S.A.