S. SRINIVASAN

Two results in number theory

Astérisque, tome 209 (1992), p. 307-310

<http://www.numdam.org/item?id=AST_1992__209__307_0>

TWO RESULTS IN NUMBER THEORY

S. Srinivasan

In memory of my friend
Mr. Ellis Martin Richstone

§1. **Introduction.** Let $N \geq 1$ be an integer and, for a reduced fraction a/N, let $K(a/N)$ denote the largest partial quotient in the continued fraction expansion of a/N. Set $K_0(N) = \min K(a/N)$ for $1 \leq a \leq N, (a, N) = 1$. Let, for a sequence B of integers, $B(x)$ denote the number of b in B, but not exceeding x. With this notation, a conjecture of S.K. Zaremba can be stated as $K_0(N) \leq 5$, for all N (cf., p.76 of [4]). There has also been some numerical evidence for this conjecture (cf., p.989 of [2]).

Now considering for given integer $\ell \geq 2$, the sequence A_ℓ consisting of N with $K_0(N) \leq \ell$, it has been shown in [3] that

$$A_\ell(x) > \frac{1}{\sqrt{2\ell}} x^{\frac{1}{2}(1-\ell^{-2})}, \text{ for } x \geq 1. \tag{1}$$

In this context, we observe the following proposition, which also leads to a qualitative result of type (1). For a given collection of a.p.s (i.e., arithmetic progressions) of (positive) integers, let $\alpha(m)$ denote the number of a.p.s containing m (but not as the smallest) and, $\delta(m)$ denote the number of a.p.s with common difference m.

Proposition 1. *Let $k (\geq 2)$ be an integer, β and β' some positive constants. Suppose A is the union of a collection of a.p.s, each consisting of k integers, satisfying (i) $\alpha(m) \leq \beta\delta(m)$ for all m and (ii) the smallest member of each a.p. is $\leq \beta'$ times its common difference. Then, for any b such that $\alpha(b) > 0$ and for all sufficiently large x, we have*

$$A(x) \geq \frac{\sqrt{\beta}}{k-1}\left(\frac{x}{b}\right)^\theta, \quad \textit{for some } \theta = \theta(\beta, \beta', k) > 0, \tag{2}$$

provided $(k-1)$ exceeds β. (An expression for θ is given in (4) below.)

Our second observation gives the following

Proposition 2. *Any solution in integers of the equation*

$$(\xi^2+\eta^2-1)=t(\xi u+\eta v)(\xi v-\eta u) \tag{3}$$

satisfies $tuv=0$.

In § 3, we shall give an example from R.Tijdeman in connection with Proposition 1. And in § 4, we have some remarks about these results.

§2. Proofs. We start with the proof of Proposition 1. Consider

$$T(x):=\sum_{m\le x}\alpha(m)\le\beta\sum_{m\le x}\delta(m).$$

Since every a.p. counted by the last sum, in view of the assumption (ii), consists of members not exceeding $(k-1+\beta')x$, we see that it occurs $(k-1)$ times in $T((k-1+\beta')x)$ and so,

$$(k-1)T(x)\le\beta T((k-1+\beta')x).$$

On letting $x_r=(k-1+\beta')^r b$, we obtain

$$T(x_r)\ge(\frac{k-1}{\beta})^r,\quad r=1,2,3,\cdots.$$

From here, after a short calculation, (2) is obtained on noting that $T(x)\le(k-1)(A(x))^2$. To see the last inequality observe that every a.p. counted in $\alpha(m)$ determines the pair (a,m), a being its smallest member and, each such pair arises from at most $(k-1)$ of the a.p.s. Also, we may take

$$\theta=\frac{1}{2}\{\log(\frac{k-1}{\beta})/\log(k-1+\beta')\}. \tag{4}$$

Now we give a proof of Proposition 2. Let $tuv\ne0$. First, observe that, after changing notations if necessary, we can assume that

$$(u,v)=1,\quad\min(\xi,\eta,t,x,y)>0, \tag{5}$$

where $x:=\xi u+\eta v, y:=\xi v-\eta u$. Now, since $(x,y)\nmid(\xi^2+\eta^2)$, we can conclude, by (5), that $(x,y)=1$. Then (3) can be rewritten as

$$(x^2+y^2)=d(1+txy),\quad d:=u^2+v^2>1.$$

Next we obtain from this

$$w\ge\varphi(x,y):=(x^2+y^2-wxy)=d>1,\quad w:=dt. \tag{6}$$

We have here

$$\varphi(x,y) = y^2 - xz = \varphi(y,z); \quad z := wy - x.$$

Thus starting with a solution (x,y) of (6), we obtain another solution (y,z) through $z = wy - x$. Now we observe that if $x \geq y > 1$ and $\gcd(x,y) = 1$, then $y > z > 0$, and obviously $\gcd(y,z) = 1$ so that, on iteration, we finally get a solution of (6) with $y = 1$, whereas (6) has no such solution and therefore $tuv = 0$, which proves Proposition 2.

§**3. About β.** The following example illuminates the significance of β occurring in Proposition 1: Let $k > 2$, and let r be a positive integer such that $r+1, \ldots, r+k-2$ are all composite. (We can take $r < k!$) Consider the sequence A of positive integers composed of primes at most r. Take any element $m > 1$ of A. Then m is divisible by a prime p which is at most r. The numbers $p-1, p, \ldots, p+k-2$ are all smaller than $r+k-1$ and therefore composed of primes at most r. Thus m is the second element of the following a.p. of length k with entries from A: $(p-1)m/p, m, (p+1)m/p, \ldots, (p+k-2)m/p$. Now it is easily seen that

$$A(x) < 2(\log x)^t,$$

where t is the number of primes at most r. Hence t is a constant depending only on k.

This example satisfies all conditions of Proposition 1, except the last one. For, we have $\delta(m) = t$ and $\alpha(m) \leq t(k-1)$ and further, $\alpha(m) = t(k-1)$ for all m belonging to A and which are multiples of K, defined as the product of $(p+j)$, as p runs through all of the t primes not exceeding r, and j takes values $0, 1, \ldots, (k-2)$. So, $\beta = k-1$.

§**4. Some remarks.** It can easily be seen that the conjecture of Zaremba (in §1) may also be stated as follows: Let $V_q := \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}$ and Z_ℓ denote the semigroup of matrices generated by $V_1, \cdots, V_\ell$. Then every $N \geq 1$ occurs as an entry of some element in Z_5. It is this formulation involving substitutions like $x_{j+1} = qx_j + x_{j-1}$ which links Propositions 1 and 2 with the conjecture; in fact, in Proposition 1 this connection comes by considering members of an a.p., with least element a and common difference m, as values of $qm + a$ $(0 \leq q < k)$, whereas in Proposition 2 this is more explicit through the substitution $z = wy - x$.

For obtaining a result of the form (1), from (2), we need only observe that A_ℓ can be considered as a sequence A of Proposition 1, with $k = \ell + 1$,

$\beta = 1 = \beta'$. (Here, with regard to $N \in A_\ell$, $N \geq 2$ and a/N with $K(a/N) \leq \ell$ we consider the a.p.s (of length $\ell+1$): (i) with smallest member b and common difference a, where $N = aj + b$ $(0 \leq b < a, 1 \leq j \leq \ell)$, and (ii) with smallest member a and common difference N.)

Also, it is apparent from the proof that for an estimate like (2) it suffices to have (i), in Proposition 1, for all sufficiently large values of m.

Incidentally, it may be noted that the argument subsequent to (6) would lead to all solutions of the simultaneous congruences

$$\xi^2 \equiv 1 \pmod{\eta}, \quad \eta^2 \equiv 1 \pmod{\xi}. \tag{7}$$

This is because (7) implies that $\xi^2 + \eta^2 - 1 = w\xi\eta$ for some positive integer w and so we obtain (6), but instead with $d = 1$. Now starting with any solution (ξ, η) of (7) we can iterate the passage from (ξ, η) to $(\eta, w\eta - \xi)$ from the proof following (6) until, after only finitely many steps, we reach $(w, 1)$. It is obvious that $(w, 1)$ is a solution of (7) for every positive integer w. Hence we obtain a complete parametrization of the set of solutions of (7). Congruences of the type (7) were earlier considered in [1].

§5. Acknowledgement. The author thanks Professor R.Tijdeman, for his kind permission to include his construction in this paper and for suggesting the parameter β' (instead of the earlier 1) in Proposition 1. Also the author would like to thank the referee for helpful suggestions.

References

[1] Gupta, H. and Srinivasan, S.: *Cycles of Quadratic Congruences*, Res. Bull. (N.S.) of the Panjab University, **22** (1971),401–404.

[2] Niederreiter, H.: *Quasi Monte-Carlo methods and pseudo-random numbers*, Bull. of A.M.S., **84** (1978), 957–1041.

[3] Sander, J.W.: *On a Conjecture of Zaremba,* Mh. Math., **104** (1987), 133–137.

[4] Zaremba, S.K.: *La méthode des »bons treillis« pour le calcul des intégrales multiples*, Application of Number Theory to Numerical Analysis (S.K. Zaremba, ed.), pp.39–119, New York; Academic Press (1972).

Seshadri SRINIVASAN
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Bombay 400 005, India