ACTA ARITHMETICA
VI (1960)

On congruence classes of denominators of convergents

by

S. Hartman (Wrocław) and P. Szüsz (Budapest)

Denote by p_n/q_n the convergents of the continued fraction representing a given real a. Let $a > 0$ and b be integers. It will be shown that for almost every a one has $q_n \equiv b \pmod a$ for arbitrarily many n. Then, obviously, for almost every a, numbers from an arbitrary arithmetical progression occur among the q_n's. Actually we are going to prove a stronger theorem:

Theorem 1. *Given a decreasing sequence* $\{c_k\}$ *with* $\sum_{k=1}^{\infty} c_k = \infty$ *and the sequence* $\{c'_k\}$ *being defined by*

$$c'_k = \begin{cases} c_k & \text{for} \quad k \equiv b \pmod a, \\ 0 & \text{otherwise}, \end{cases} \tag{1}$$

the inequality

$$|ak - p| < c'_k \tag{2}$$

is fulfilled for almost every a *by infinitely many* k *with suitable* p *and* $(k, p) = 1$.

The preceding statement follows from Theorem 1 by putting $c_k = 1/2k$ and observing that if $|ak - p| < 1/2k$ and $(k, p) = 1$ then p/k is a convergent of a, this being a well-known result.

The proof is based on the following theorem of Duffin and Schaeffer [1]:

If for non-negative numbers c'_k $(k = 1, 2, \ldots)$ *with* $\sum_k c'_k = \infty$ *there is a constant* K *such that*

$$\sum_{k=1}^{n} \frac{\varphi(k)}{k} c'_k > K \sum_{k=1}^{n} c'_k$$

for infinitely many n, φ *being the Euler function, then* (2) *has for almost every* a *arbitrarily many solutions with* $(k, p) = 1$.

The numbers c'_k being defined by (1) it suffices to show

$$\sum_{k=1}^{n} \frac{c_k \varphi'(k)}{k} > K \sum_{k=1}^{n} c'_k \tag{3}$$

where $\varphi'(k) = \varphi(k)$ or 0 according as $k \equiv b \pmod a$ or not. Since the sequence $\{c_k\}$ is monotonous, (3) will follow by partial summation from the inequality

$$\sum_{k=1}^{n} \frac{\varphi'(k)}{k} > Kn, \tag{4}$$

which we are now going to prove.

Assume first $(a, b) = 1$ and let χ be characters mod a. It is known that

$$\sum_{\chi} \frac{\chi(k)}{\chi(b)} = \begin{cases} \varphi(a) & \text{if} \quad k \equiv b \pmod a, \\ 0 & \text{if} \quad k \not\equiv b \pmod a. \end{cases} \tag{5}$$

We have also

$$\frac{\varphi(k)}{k} = \sum_{d|k} \frac{\mu(d)}{d},$$

where μ denotes the Möbius function. Therefore

$$\sum_{k=1}^{n} \frac{\varphi'(k)}{k} = \sum_{\substack{1 \leqslant k \leqslant n \\ k \equiv b (\mathrm{mod}\, a)}} \frac{\varphi(k)}{k} = \frac{1}{\varphi(a)} \sum_{k=1}^{n} \sum_{\chi} \frac{\chi(k)}{\chi(b)} \cdot \frac{\varphi(k)}{k}$$

$$= \frac{1}{\varphi(a)} \sum_{k=1}^{n} \sum_{\chi} \frac{\chi(k)}{\chi(b)} \sum_{d|k} \frac{\mu(d)}{d} = \frac{1}{\varphi(a)} \sum_{d=1}^{n} \frac{\mu(d)}{d} \sum_{\substack{d|k \\ 1 \leqslant k \leqslant n}} \sum_{\chi} \frac{\chi(k)}{\chi(b)}$$

$$= \frac{1}{\varphi(a)} \sum_{d=1}^{n} \frac{\mu(d)}{d} \sum_{l=1}^{[n/d]} \sum_{\chi} \frac{\chi(ld)}{\chi(b)}.$$

If $(d, a) > 1$ then since $(a, b) = 1$, one has $ld \not\equiv b \pmod a$ and in virtue of (5)

$$\sum_{l=1}^{[n/d]} \sum_{\chi} \frac{\chi(ld)}{\chi(b)} = 0.$$

If $(d, a) = 1$ then this double sum equals the number of l's for which $ld \equiv b \pmod a$ and $l \leqslant [n/d]$. This number being $n/ad + O(1)$, one has

$$\sum_{k=1}^{n} \frac{\varphi'(k)}{k} = \frac{1}{\varphi(a)} \sum_{\substack{1 \leqslant d \leqslant n \\ (a,d)=1}} \frac{\mu(d)}{d} \left(\frac{n}{ad} + O(1) \right)$$

$$= \frac{n}{a\varphi(a)} \sum_{\substack{1 \leqslant d \leqslant n \\ (a,d)=1}} \frac{\mu(d)}{d^2} + O(\log n)$$

$$= n \frac{1}{a\varphi(a)} \frac{6}{\pi^2} \prod_{p|a} \left(1 - \frac{1}{p^2}\right)^{-1} + O(\log n),$$

where the last equality can be deduced from

$$\sum_{\substack{1 \leqslant d \leqslant n \\ (a,d)=1}} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} \prod_{p|a} \left(1 - \frac{1}{p^2}\right)^{-1} + O\left(\frac{1}{n}\right).$$

Thus, (4) is proved for the case $(a, b) = 1$. In the case $(a, b) = d > 1$ the estimation (4), and consequently (3), remain valid; this can be deduced by applying it to the numbers $a' = a/d$, $b' = b/d$ and observing that $\varphi(ld) \geqslant \varphi(l)\varphi(d)$. Thus, Theorem 1 is completely proved.

Let us observe that omitting the condition $(k, p) = 1$ in this Theorem we obtain a special case of a stronger result proved by de Vries ([3], p. 46, Stelling 13).

Putting $c_k = 1/2k\log k$ we deduce at once from Theorem 1 the following

THEOREM 2. *For almost every a and every positive integer l the sequence $\{q_n\}$ contains a subsequence $\{q_{\nu_n}\}$ which consists of multiples of l and is such that*

$$\lim_n \frac{q_{\nu_n+1}}{q_{\nu_n}} = \infty.$$

For this result, in spite of its being a consequence of the preceding one, we will now supply a direct and more elementary proof. This seems justified, since Theorem 2 may have some independent significance and can be applied to a problem treated formerly by one of us [2].

Evidently it will be sufficient to prove that a number l being prescribed, the desired subsequence exists for almost every a. We proceed by induction with respect to the number m of distinct prime factors of l. For $m = 0$, i. e. $l = 1$, the statement is trivial. Assume that it is true

for a given m; then fix arbitrarily a positive integer a having m distinct prime factors and choose a prime s not entering into a. One has to prove that for $k = 1, 2, \ldots$ and $l = as^k$ a sequence $\{q_{\nu_n}\}$ with required properties can be found for almost every α.

Let us suppose that $0 \leqslant \alpha < 1$. Writing $\alpha_1 + \alpha_2$ we mean addition mod1. Denote by E_k the set of those α for which our statement is satisfied for $l = a$ by the numbers $\alpha + r/s^k$ $(r = 1, 2, \ldots, s^k - 1)$. The inductive hypothesis obviously implies

$$|E_k| = 1. \tag{6}$$

Thus, for an $\alpha \in E_k$ and arbitrarily fixed r $(1 \leqslant r < s^k)$ we can find a sequence $\{P_n/Q_n\}$ of convergents of $\alpha + r/s^k$ for which

$$a/Q_n, \tag{7}$$

$$\left|\alpha + \frac{r}{s^k} - \frac{P_n}{Q_n}\right| < \frac{c_n}{Q_n^2}, \tag{8}$$

$$c_n \to 0, \quad c_n \leqslant \frac{1}{2s^{2k}}. \tag{9}$$

From (8) we obtain

$$\left|\alpha - \frac{P_n s^k - rQ_n}{Q_n s^k}\right| < \frac{c_n s^{2k}}{Q_n^2 s^{2k}}. \tag{10}$$

Since $c_n s^{2k} \leqslant \frac{1}{2}$, the fraction on the left of (10) equals a convergent p_{ν_n}/q_{ν_n} of α; moreover, on account of (9) one has

$$\lim_n \frac{q_{\nu_n+1}}{q_{\nu_n}} = \infty.$$

From (7) and $(P_n, Q_n) = 1$ follows $(a, P_n) = 1$, and since $(a, s) = 1$, we have

$$a/q_{\nu_n}.$$

Let the integer λ $(0 \leqslant \lambda < k)$ be defined by conditions

$$r = s^\lambda u, \quad (u, s) = 1.$$

LEMMA 1. *For every n at least one of the following two cases occurs*

(a) $$s^{k-\lambda}/q_{\nu_n},$$

(b) $$s^{k-\lambda}/Q_n.$$

Let

$$Q_n = s^\mu t \quad (\mu \geqslant 0;\ (s, t) = 1). \tag{11}$$

Then

$$\frac{p_{\nu_n}}{q_{\nu_n}} = \frac{P_n s^k - rQ_n}{Q_n s^k} = \frac{P_n s^{k-\mu} - s^\lambda ut}{ts^k}.$$

If $0 \leqslant k - \mu < \lambda$, then

$$\frac{p_{\nu_n}}{q_{\nu_n}} = \frac{P_n - s^{\lambda+\mu-k} ut}{ts^\mu}.$$

Since in this case $\mu > 0$, we have $(P_n, s) = 1$; hence s^μ/q_{ν_n} and this implies (a). If $k - \mu > \lambda$, then

$$\frac{p_{\nu_n}}{q_{\nu_n}} = \frac{P_n s^{k-\mu-\lambda} - ut}{ts^{k-\lambda}}.$$

Since $(u, s) = 1$, we have $s^{k-\lambda}/q_{\nu_n}$ and (a) holds again. It $\mu > k$ or $k - \mu = \lambda$, then (b) holds by (11).

Now let M_i^k $(i = 0, 1, \ldots, k-1)$ denote the set of those α's for which the sequence $\{q_n\}$ contains infinitely many terms q_{ν_n} divisible by as^{k-i} and fulfilling the condition $q_{\nu_n+1}/q_{\nu_n} \to \infty$. Put

$$N_i^k = E_k \setminus M_i^k.$$

LEMMA 2. *If $\alpha \in N_i^k$, then $\alpha + r/s^k \in M_i^k$ for every $r = 1, 2, \ldots, s^i - 1$.*

In fact, for such r's we have $\lambda \leqslant i - 1$. For a fixed r and a fixed sequence $\{P_n/Q_n\}$ satisfying (7)-(9) the case (a) can occur at most finitely often; otherwise we should have s^{k-i}/q_{ν_n} for infinitely many n, and hence $\alpha \in M_i^k$, against the assumption. Thus, by Lemma 1, it is the case (b) which occurs for infinitely many n. This case implies s^{k-i}/Q_n, and therefore $\alpha + r/s^k \in M_i^k$. The sets

$$\left\{\alpha:\ \alpha - \frac{r}{s^k} \in N_i^k\right\} \tag{12}$$

are disjoint for $r = 0, 1, \ldots, s^i - 1$. In fact, otherwise there would exist two integers r_1 and r_2 $(0 \leqslant r_1 < r_2 \leqslant s^i - 1)$ and two numbers $\beta_1, \beta_2 \in N_i^k$ such that $\beta_1 + r_1/s_k = \beta_2 + r_2/s^k$. However, the equality $\beta_1 - \beta_2 = (r_1 - r_2)/s^k$ implies together with Lemma 2 that β_1 and β_2 cannot both belong to N_i^k. The sets (12) are evidently L-measurable and congruent to N_i^k. Since they are disjoint, their Lebesgue measure fulfils the inequality

$$|N_i^k| \leqslant \frac{1}{s^i}.$$

Hence, by (1), we have

$$|M_i^k| > 1 - \frac{1}{s^i} \quad (i = 0, 1, \ldots, k-1). \tag{13}$$

Now let k run over all even integers and put $i = k/2$. Then (13) yields $|M^k_{k/2}| \to 1$, and since $M_1^2 \supset M_2^4 \supset M_3^6 \supset \ldots$, it follows that

$$|M^k_{k/2}| = 1$$

for every k. This means that for $l = as^{k/2}$ $(k = 2, 4, 6, \ldots)$ and for almost every α a required sequence $\{q_{n_\nu}\}$ does exist.

Application. In [2] it was proved that for almost every α the inequalities $|q\alpha - p| < 1/t$, $|q| < ct$ $(p, q$ integers) cannot be solved simultaneously for every $t > 1$ with an *odd* q, however large constant c is chosen. For this proof it is essential that for almost every α the sequence $\{q_n\}$ should contain a subsequence $\{q_{\nu_n}\}$ consisting of even numbers and such that $\lim_n (q_{\nu_n+1}/q_{\nu_n}) = \infty$. Replacing this proposition by Theorem 2 we can obtain without further modification of arguments the following generalization of the result in [2]:

For almost every α, every $c > 0$ and every integer l the inequalities $|q\alpha - p| < 1/t$ and $|q| < ct$ are not simultaneously solvable for arbitrary $t > 1$ if it is required that q should not be divisible by l.

It may be observed that the theorem of Duffin and Schaeffer and the estimation of the number of primes in arithmetical progressions enable us to prove that for almost every α the sequence $\{q_n\}$ contains primes belonging to any progression $b + na$ $(n = 1, 2, \ldots)$ with $(a, b) = 1$.

References

[1] R. J. Duffin and A. C. Schaeffer, *Khintchine's problem in metric diophantine approximation*, Duke Math. J. 8 (1941), p. 243-255.

[2] S. Hartman, *A feature of Dirichlet's approximation theorem*, Acta Arithmetica 5 (1959), p. 261-263.

[3] O. de Vries, *Metrische onderzoekingen van diophantische benaderings-problemen in het niet-lacunaire geval* (thesis), Amsterdam 1955.

MATHEMATICAL INSTITUTE OF THE POLISH ACADEMY OF SCIENCE
INSTITUTE OF MATHEMATICAL RESEARCH OF THE HUNGARIAN ACADEMY OF SCIENCE

Reçu par la Rédaction le 14. 1. 1960

ACTA ARITHMETICA
VI (1960)

On a generalization of Wilson's theorem

by

B. Gyires (Debrecen, Hungary)

1. In the present paper we denote by printed Latin capitals quadratic matrices of order n, and by written Latin capitals quadratic matrices of order nr. In particular, E and O will denote the unit matrix and the zero matrix of order n, respectively, whereas $\mathcal{C}$ will be the unit matrix of order nr. $\langle A_1, \ldots, A_r \rangle$ stands for a hypermatrix of order nr, built from matrices of order n, in which all elements outside the matrices in the main diagonal are zero matrices, and the hth element of the main diagonal is A_h. We shall call this matrix a diagonal-matrix, whereas the (evidently regular) matrix

$$(1) \qquad \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \ldots & \lambda_r \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_1^{r-1} & \lambda_2^{r-1} & \ldots & \lambda_r^{r-1} \end{bmatrix}.$$

built from the pairwise different numbers

$$(2) \qquad \lambda_1, \lambda_2, \ldots, \lambda_r$$

will be called the Vandermonde-matrix generated by the elements (2). The direct product of the matrix E with the matrix (1) is also regular, since by the well-known theorem on determinants of Kronecker the determinant of the direct product is the nth power of the determinant of the matrix (2).

A quadratic matrix whose elements are rational integers will be called *regular with respect to the module p* (p a prime), if its determinant is not divisible by p. By Cramer's rule for linear systems of congruences any matrix regular mod$p$ has an inverse in the sense that there exists a matrix, such that the product of multiplying by it the original martix will be congruent mod$p$ with the unit matrix. If the elements (2) are rational integers incongruent mod$p$, then it follows from the product