Conspectus materiae tomi XXII, fasciculi 1



	ragina
T. W. Cusick, Simultaneous diophantine approximation of rational numbers	1
Nina Spears, A problem involving simultaneous binary compositions	11
R. C. Vaughan, On Goldbach's problem	21
D. Barsky, Sur les systèmes complets de restes modulo les idéaux d'un corps	
de nombres	48
M. Mignotte, Une généralisation d'un théorème de Cugiani-Mahler	57
J. H. Loxton, On the maximum modulus of cyclotomic integers	68
H. Davenport and D. J. Lewis, Gaps between values of positive definite	
quadratic forms	87
Y. Motohashi. On the distribution of the zeros of Dirichlet's L-functions	107
S. Chowla and P. Hartung, An "exact" formula for the m-th Bernoulli	
number	118

La revue est consacrée à la Théorie des Nombres The journal publishes papers on the Theory of Numbers Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange Address of the Editorial Board and of the exchange Die Adresse der Schriftleitung und des Austausches Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, Warszawa 1

Les volumes IV et suivants sont à obtenir chez	Volumes from IV on are available at	Die Bände IV und folgende sind zu beziehen durch	томы IV и следу ющие можно по лучить через
Ars Pol	ona-Ruch, Krakowski	ie Przedmieście 7, Wars	zawa 1
Prix d'un fascicule	Price of an issue	Preis für ein Heft	Цена номер
	. \$	4.35	
Les volumes I-III sont à obtenir chez	Volumes I-III are available at	Die Bände I–III sind zu beziehen durch	Томы I-III можи получить черев
Johnson 1	Reprint Corporation.	111 Fifth Ave., New Yo	rk, N. Y.

PRINTED IN POLAND

W R O C L A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA XXII (1972)

Simultaneous diophantine approximation of rational numbers

by

T. W. Cusick (Buffalo, N.Y.)

1. Introduction. For any real number x, let ||x|| denote the distance from x to the nearest integer; thus $\frac{1}{2} \ge ||x|| \ge 0$ for all x.

Let n be any positive integer and let $\sigma = (s_1, \ldots, s_n)$ denote an arbitrary point in the set S^n of n-dimensional points all of whose coordinates are rational noninteger numbers. Define the function $\omega(n)$ by

$$\omega(n) = \inf_{\sigma \in S^n} \sup_{q} \min_{1 \leqslant i \leqslant n} \|qs_i\|$$

where the supremum (or maximum) is taken over all integers q (in what follows, max will always be taken over all integers q).

If z > 1 is an integer with prime factorization $\prod_{i=1}^{k} p_i^{\alpha_i}$, define h(z) = k. Then for each positive integer n define the function w(n) by w(1) = 1/3, w(2) = 1/5 and

(2)
$$w(n) = \max\{z: h(z) + \frac{1}{2}\varphi(z) \le n\}$$

for $n \ge 3$ (here φ is Euler's function).

The main purpose of this paper is to propose the conjecture that $\omega(n) = 1/w(n)$ for every positive integer n, and to prove the conjecture for $n \leq 7$.

THEOREM 1. For $n \leq 7$, $\omega(n) = 1/w(n)$. Numerically,

$$\omega(1) = 1/3,$$

 $\omega(2) = 1/5,$
 $\omega(3) = 1/8,$
 $\omega(4) = 1/12,$
 $\omega(5) = 1/18,$
 $\omega(6) = 1/24,$
 $\omega(7) = 1/30.$

The problem of evaluating $\omega(n)$ originated in two papers of Wills ([6], [7]); he showed $\omega(1) = 1/3$ and $(2n^2)^{-1} \leq \omega(n) \leq 1/w(n)$ for $n \geq 2$. In a later paper, Wills [8] obtained the better lower bound $\omega(n)$

 $\geq e(n\log n)^{-1}$, and found an asymptotic formula for w(n) (see Lemma 7 below).

Actually, the function considered by Wills was defined by (1) with the infimum taken over all points in the set of n-dimensional points none of whose coordinates is an integer. The fact that Wills' function can also be defined by (1) (which simplifies the study of $\omega(n)$) was proved by Wills [7].

The results of this paper were announced in [3].

2. Preliminary results. I begin by giving a proof that $\omega(n) \leq 1/w(n)$ for every n; this proof uses the same idea as the one given by Wills ([7], pp. 376–377), but avoids his unnecessary use of certain auxiliary integer sequences in the argument.

LEMMA 1. For each positive integer n, $\omega(n) \leq 1/w(n)$.

Proof. The result is obvious for n=1, 2, so suppose $n \ge 3$ and w(n) has prime factorization $\prod_{i=1}^{n} p_i^{a_i}$. Define $s_i, 1 \le i \le h + \frac{1}{2}\varphi(w(n))$ by

$$s_i = egin{cases} p_i^{-1} & (1 \leqslant i \leqslant h), \ a_{i-h}/w(n) & (h+1 \leqslant i \leqslant h+rac{1}{2}arphi(w(n))), \end{cases}$$

where the numbers a_j $(1 \le j \le \frac{1}{2}\varphi(w(n)))$ are those positive integers less than $\frac{1}{2}w(n)$ which are relatively prime to w(n), taken in some order. Since $h + \frac{1}{2}\varphi(w(n)) \le n$ by the definition of w(n), there are no more than $n \ s_i$'s. If in fact $h + \frac{1}{2}\varphi(w(n)) < n$, define $s_i = p_1^{-1} \ (h + \frac{1}{2}\varphi(w(n)) + 1 \le i \le n)$, say. In order to prove the lemma, it suffices to show max $\min_{q} \|qs_i\| \le 1/w(n)$.

Clearly we need only consider integers q satisfying $1 \le q \le w(n)$. If q is not relatively prime to w(n), then $\min_{\substack{1 \le i \le h \\ h+1 \le i \le n}} \|qs_i\| \le 1/w(n)$: for each of the $\varphi(w(n))$ congruences $a_jx \equiv \pm 1 \mod w(n)$ $(1 \le j \le \frac{1}{2}\varphi(w(n)))$ has a unique solution x = q with $1 \le q \le w(n)$ and q prime to w(n), and no two of these solutions are the same because the a_j are distinct and satisfy $1 \le a_j < \frac{1}{2}w(n)$. This proves the lemma.

Thus in order to prove Theorem 1, it is only necessary to show that $\omega(n) \ge 1/w(n)$ for $1 \le n \le 7$. The following lemma will play an important role:

LEMMA 2. Let n, k and m be any positive integers, and suppose m has prime factorization $\prod_{i=1}^{h} p_i^{a_i}$. If there exist rational noninteger numbers s_1, \ldots, s_n such that $\max \min_{a_i = 1 \le i \le n} ||qs_i|| \le k/m$, then we may assume without loss of generality that $h \le n$, $s_i = b_i/p_i$ $(1 \le i \le h)$ where the b_i are integers satisfying

 $0 < b_i < p_i$, and $s_i = a_i/m$ (h+1 $\leq i \leq n$) where the a_i are integers satisfying $0 < a_i < m$.

Proof. This is a lemma of Wills ([7], Lemma 3, p. 372) expressed in a different form. I give a simplified proof, as follows:

We may obviously assume that $\max_{q} \min_{1 \leqslant i \leqslant n} \|qs_i\| = k/m$ and $s_i = a_i/m$ $(1 \leqslant i \leqslant n)$ where the a_i are integers satisfying $0 < a_i < m$. Let p be any prime dividing m and suppose that ps_i is not an integer for $1 \leqslant i \leqslant n$. Then if we define $s_i' = ps_i$ $(1 \leqslant i \leqslant n)$ the s_i' are rational noninteger numbers and clearly $\max_{q} \min_{1 \leqslant i \leqslant n} \|qs_i'\| \leqslant k/m$. Hence we need only consider

the case where for each p dividing m, ps_i is an integer for some subscript i = i(p). The subscripts i(p) must be different for different p, and this proves the lemma.

The arguments used below to establish $\omega(n) \ge 1/w(n)$ for $3 \le n \le 7$ do not seem to apply for n = 1, 2, so I give special proofs for these cases.

LEMMA 3. The equality $\omega(n) = 1/w(n)$ holds for n = 1, 2.

Proof. The case n=1 is trivial. For n=2, we have w(2)=5, so it suffices to show that for any two rational noninteger numbers a/b and o/d which satisfy

(3)
$$\max_{a} \min(\|qa/b\|, \|qe/d\|) \le 1/5,$$

equality must hold in (3).

We assume without loss of generality that a/b and c/d are in lowest terms. There are clearly $\leqslant d(2 \lceil b/5 \rceil + 1)$ integers q in the range $1 \leqslant q \leqslant bd$ which satisfy $\|qa/b\| \leqslant 1/5$, with a similar result for the inequality $\|qc/d\| \leqslant 1/5$. It follows that (3) implies

$$2\left(b\left[\frac{d}{5}\right]+d\left[\frac{b}{5}\right]\right)+b+d\geqslant bd.$$

Using the trivial estimate for the greatest integer function in (4), we obtain $b^{-1}+d^{-1} \ge 1/5$, so at least one of b, d is ≤ 10 . We assume without loss of generality that $2 \le b \le 10$, $b \le d$. Then a little arithmetic shows that for $b \ne 5$, the only pairs (b,d) which satisfy (4) are (2,5), (2,6), (2,10), (6,6), (6,10) and (10,10). It is a simple matter to verify that (3) cannot hold for any fractions a/b, c/d in lowest terms if (b,d) is one of these pairs.

Hence b = 5, and it is easily seen that strict inequality cannot hold in (3) for any choice of a, c and d.

3. The cases $3 \le n \le 7$ of Theorem 1. Assume that for some n, there exist positive integers k and m such that

(5)
$$\omega(n) \leqslant \frac{k}{m} < \frac{1}{w(n)}.$$

I prove Theorem 1 by showing that for $3 \le n \le 7$, the assumption (5) leads to a contradiction.

By Lemma 2, we can suppose without loss of generality that there exist distinct primes r_i $(1 \le i \le h, r_1 < r_2 < \ldots < r_h)$ and rational numbers $s_i = a_i/m$ $(1 \le i \le n)$ such that

(6)
$$m = \prod_{i=1}^{h} r_i^{\beta_i}, \quad h \leqslant n;$$

(7)
$$\max_{q} \min_{1 \le i \le n} ||qs_i|| \le k/m;$$

and

(8)
$$0 < a_i < m \ (1 \le i \le n), \quad a_i = mb_i/r_i \text{ for integers } b_i,$$
 $0 < b_i < r_i \ (1 \le i \le h).$

Define

 $v_n(m)$ = the number of distinct primes p such that p divides m and p < w(n).

LEMMA 4. If (5), (6), (7) and (8) hold, then

$$\frac{m}{\varphi(m)} > \begin{cases} \frac{w(n)}{2n - h(m) - v_n(m)}, & m \text{ even,} \\ \frac{w(n)}{2(n - v_n(m))}, & m \text{ odd.} \end{cases}$$

Proof. Let (a, b) denote the greatest common divisor of the integers a and b. There are at most 2k different values of x, $1 \le x \le m$, which satisfy at least one of the 2k congruences

$$a_i x \equiv \pm i \bmod m \quad (1 \leqslant i \leqslant k).$$

This is clear if $(a_i, m) = 1$, for then each of the congruences in (9) has a unique solution $\operatorname{mod} m$. If $(a_i, m) > 1$, the congruence $a_i x = j \operatorname{mod} m$ is solvable if and only if (a_i, m) divides j, in which case there are (a_i, m) solutions $x, 1 \leq x \leq m$. The number of j such that $1 \leq |j| \leq k$ and (a_i, m) divides j is $2 \left[k/(a_i, m) \right]$, so the total number of different x, $1 \leq x \leq m$, which satisfy at least one of the congruences in (9) is $\leq 2(a_i, m) \left[k/(a_i, m) \right] \leq 2k$.

Since $0 < a_i < m$ by (8), any integer q such that (q, m) = 1 and $\min_{1 \le i \le n} ||qs_i|| \le k/m$ must be a solution of at least one of the congruences in (9) for some $i, v_n(m) + 1 \le i \le n$. The range $1 \le i \le v_n(m)$ need not be considered, because for these i we have

$$(a_i, m) = \frac{m}{r_i} > \frac{m}{w(n)} > k$$

by (8), the definition of $v_n(m)$ and (5); thus none of the congruences in (9) has solutions if $1 \le i \le v_n(m)$. There are $\varphi(m)$ values of q such that (q, m) = 1 and $1 \le q \le m$, so (7) implies that there are at least $\varphi(m)/2k$ different values of a_i $(v_n(m)+1 \le i \le n)$. Hence, using (5),

$$\varphi(m) \leqslant 2k \big(n - v_n(m)\big) < \frac{2m \big(n - v_n(m)\big)}{w(n)},$$

which gives the lemma if m is odd.

For m even, we shall show that if $v_n(m)+1 \le i \le h(m)$, then there are at most k different values of x such that (x,m)=1, $1 \le x \le m$ and x satisfies at least one of the congruences in (9). Then the argument which led to (10) will give

$$\varphi(m) \leqslant 2k(n-h(m)) + k(h(m) - v_n(m)) < \frac{m(2n-h(m) - v_n(m))}{w(n)},$$

which is the desired result.

The (a_i, m) solutions of any solvable congruence $a_i x \equiv j \mod m$ are given by

$$(11) x = x_0 + t \frac{m}{(a_i, m)} (1 \leqslant t \leqslant (a_i, m))$$

where

$$\frac{a_i}{(a_i, m)} x_0 \equiv \frac{j}{(a_i, m)} \mod \frac{m}{(a_i, m)}.$$

If m is even and $v_n(m)+1 \le i \le h(m)$, then by (8) $(a_i, m) = m/r_i$ is even and $m/(a_i, m) = r_i$ is odd. Hence exactly half of the solutions (11) are even, namely those for which t has the same parity as x_0 .

We saw previously that at most 2k different values of $x, 1 \le x \le m$, satisfy at least one of the congruences in (9). The above remarks show that at most k of these values of x also satisfy (x, m) = 1. This completes the proof of the lemma.

Define for each positive integer n

$$P_n = \prod_{i=1}^n \frac{p_i}{p_i - 1}$$

where $p_1 = 2, ..., p_i$ = the *i*th prime. Values of P_n for various n < 20 occur frequently in the calculations necessary in the proofs of the next two lemmas. For this work a table of P_n (or P_n^{-1}) is very convenient; such tables are given in [1], [4], [5].

LEMMA 5. If (5), (6), (7) and (8) hold and n satisfies $3 \le n \le 7$, then m is even.

6

Proof. If m is not even, it follows from (6) that

(12)
$$\frac{m}{\varphi(m)} = \prod_{i=1}^{h} \frac{r_i}{r_i - 1} \leqslant \frac{1}{2} P_{n+1}.$$

For each n in the range $3 \le n \le 7$, it is a simple calculation to verify that for any odd m the inequality (12) contradicts the inequality of Lemma 4. For example, if n=4 and both inequalities hold, then $v_4(m) < 4 - (w(4)/P_5) = 1.50 \dots$ This implies either $v_4(m) = 0$, so that $m/\varphi(m) \le P_9 P_5^{-1} = 1.27 \dots$, or $v_4(m) = 1$, so that $m/\varphi(m) \le 1.5 P_9 P_5^{-1} = 1.82 \dots$; in both cases the inequality of Lemma 4 is contradicted.

The range of n for which Lemma 5 is valid could be greatly extended, by the same type of calculation. It is the next lemma which leads to the restriction $n \leq 7$ in Theorem 1.

LEMMA 6. If n satisfies $3 \le n \le 7$, then there is no even integer m for which (5), (6), (7) and (8) are valid.

Proof. We show that for $3 \le n \le 7$, the assumption of the existence of an even m such that (5), (6), (7) and (8) hold contradicts Lemma 4. For each n, the first step is to deduce an upper bound for $h(m) + v_n(m)$ from the inequalities

(13)
$$P_n \geqslant \frac{m}{\varphi(m)} > \frac{w(n)}{2n - h(m) - v_n(m)},$$

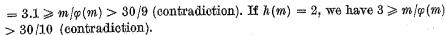
which follow from (6) and Lemma 4. Then calculations similar to those in the proof of Lemma 5 show that the conditions imposed on m cannot all be satisfied. I illustrate the calculations with the cases n=3 and n=7; the other cases are much the same. Notice that the trivial inequality $h(m) \ge v_n(m)$ is frequently used.

The case n=3. Here (13) implies $h(m)+v_3(m) \le 3$, so the only possibilities are $v_3(m)=1$, h(m)=2 or 1. If h(m)=2, then $m/\varphi(m) \le 2(11/10)=2.2$; if h(m)=1, then $m/\varphi(m) \le 2$. In both cases the inequality of Lemma 4 is contradicted.

The case n=7. Here (13) implies $h(m)+v_7(m) \le 8$, so $v_7(m) \le 4$. If $v_7(m)=4$, then also h(m)=4, so $m/\varphi(m) \le P_4=4.375$. This contradicts the inequality of Lemma 4.

If $v_7(m) = 3$, then $3 \le h(m) \le 5$. If h(m) = 5, we have $P_5 = 4.8125 \ge m/\varphi(m) > 30/6$ (contradiction). If h(m) = 4, we have $P_4 = 4.375 \ge m/\varphi(m) > 30/7$ (contradiction). If h(m) = 3, $P_3 = 3.75 \ge m/\varphi(m) > 30/8$ (contradiction).

If $v_7(m) = 2$, then $2 \le h(m) \le 6$, so $m/\varphi(m) \le 3P_{14}P_{10}^{-1} = 3.34...$ However, by Lemma 4, $m/\varphi(m) > 30/(12-h(m)) \ge 3.75$ for $h(m) \ge 4$; this eliminates the cases $4 \le h(m) \le 6$. If h(m) = 3, we have 3(31/30)



If $v_7(m)=1$, then $1\leqslant h(m)\leqslant 7$, so $m/\varphi(m)\leqslant 2P_{16}P_{10}^{-1}=2.32\ldots$ However, by Lemma 4, $m/\varphi(m)>30/(13-h(m))\geqslant 2.5$ for $h(m)\geqslant 1$, which gives a contradiction for any possible value of h(m).

Lemma 6 completes the proof of Theorem 1. The method used to prove Lemma 6 breaks down for $n \ge 8$ by failing to exclude all possible even values of m. For example, in the case n = 8 (w(8) = 36), the method excludes all even integers m except m of the form (6) with m = 3, m = 1, m = 1, that is, the assumption that m exists leads to a contradiction except when m = 1 and 30 divides m. Thus the technique of Lemma 6 is insufficient to evaluate m = 1 although the calculations will give the estimates m = 1.

4. A theorem about w(n). The function w(n) is of some interest in its own right. (See table of w(n) below. This table was easily constructed by using Tables I and II of [2]. Table I gives n, the factorization of n, and $\varphi(n)$; Table II gives the values of n for which $\varphi(n)$ takes on a given value.)

Theorem 2 below states one of the more striking properties of w(n). The proof makes use of the fact that w(n)/n tends to infinity, which is an immediate consequence of the following known result:

LEMMA 7. If γ denotes Euler's constant, then

$$\lim_{n\to\infty}\frac{w(n)}{n\log\log n}=2e^{\nu}.$$

Proof. This was proved by Wills ([8], Lemma 1, p. 167).

THEOREM 2. Given any prime q, q divides w(n) for all sufficiently large n.

Proof. We first obtain the weaker result that $h(w(n)) \to \infty$ as $n \to \infty$. First, we have

$$\varphi(w(n)) = w(n) \prod_{p} \left(1 - \frac{1}{p}\right) \geqslant \frac{w(n)}{h(w(n)) + 1},$$

where the product is over the h(w(n)) primes p which divide w(n) and the inequality is trivial. Second, we have $w(n)/\varphi(w(n)) \to \infty$ as $n \to \infty$: for if $w(n)/\varphi(w(n)) \leqslant B$ for infinitely many n, then the inequality $n > \frac{1}{2}\varphi(w(n))$ implies $w(n)/n \leqslant 2B$ for infinitely many n, in contradiction to Lemma 7. It follows at once that $h(w(n)) \to \infty$ as $n \to \infty$.

Suppose now that $w(n) = z_0$ and the prime q does not divide z_0 ; we shall deduce a contradiction if n is sufficiently large. Suppose the prime

factorization of
$$z_0$$
 is $\prod_{i=1}^k p_i^{a_i}$, $p_1 < p_2 < \dots < p_k$.

Let N(r) be a function with the property that x > N(r) implies the existence of a prime p satisfying x <math>(0 < r < 1). The existence of such a function of course follows from the prime number theorem.

Since $h(w(n)) \to \infty$ as $n \to \infty$, we may suppose that n is so large that $k \ge 3$ and p_{k-1}, p_k satisfy

$$\frac{q}{q-1} \left(\frac{p_{k-1}-1}{p_{k-1}} \right) \left(\frac{p_k-1}{p_k} \right) \ge 1 + \frac{1}{2q},$$

$$\frac{p_{k-1}p_k}{q} > N\left(\frac{1}{2q}\right)$$

and

$$(16) p_{k-1} > q.$$

Then (15) and (16) imply that there exists a prime p such that

$$(17) p_k < p_{k-1}^{a_{k-1}} p_k^{a_k} q^{-1} < p < \left(1 + \frac{1}{2q}\right) p_{k-1}^{a_{k-1}} p_k^{a_k} q^{-1}.$$

Now define $z_1 = pq \prod_{i=1}^{n-1} p_i^{a_i}$; neither p nor q is one of the p_i 's because $p_{k-2} < p_k < p$ by (17) and q does not divide z_0 by hypothesis. We have $z_1 > z_0$ by (17), $h(z_1) = h(z_0)$ and $\varphi(z_1) < \varphi(z_0)$ (because

$$\varphi(pq) = (p-1) (q-1) < \varphi(p_{k-1}^{a_{k-1}} p_{k}^{a_{k}}) = (p_{k-1}-1) (p_{k}-1) p_{k-1}^{a_{k-1}} p_{k}^{a_{k-1}}$$

follows from (14) and the third inequality in (17)). This contradicts the hypothesis $w(n) = z_0$, and so proves the theorem.

Table of w(n), $1 \le n \le 50$

n	w(n)	·n	w (n)	n	w (n)	n	w (ň)	n	w(n)
1	3	11	60	21	126	31	210	4.1	270
2	5	12	60	22	126	32	210	42	270
3	8	13	66	23	150	33	210	43	300
4	12	14	72	24	150	34	210	44	330
5	.18	15	90	25	150	35	240	45	330
6	24	16	90	26	150	36	240	46	330
7	30	17	90	27	180	37	240	47	330
8	36	18	96	28	210	38	240	48	390
9	42	19	120	29	210	39	270	49	330
10	4.8	20	120	30	210	40	270	50	330

References

[1] Kenneth I. Appel and J. Barkley Rosser, Table for estimating functions of primes (Communications Research Division Technical Report no. 4, Institute for Defense Analyses), Princeton, New Jersey 1961.



- [2] British Association Mathematical Tables, vol. VIII: Number-Divisor Tables, Cambridge 1940.
- [3] T. W. Cusick, Simultaneous Diophantine approximation of rational numbers, Notices Amer. Math. Soc. 17 (1970), p. 801.
- [4] J. W. L. Glaisher, Table of the values of (1/2) (2/3) (4/5) ... ((x-1)/x), the denominators being the series of prime numbers, Messenger of Math. 28 (1898), pp. 1-17.
- [5] A. M. Legendre, Théorie des Nombres (4th. ed., 1830, reprinted by Libraire Scientifique et Technique, A. Blanchard, Paris, 1955).
- [6] J. M. Wills, Zur simultanen homogenen diophantischen Approximation I, Monatsh. Math. 72 (1968), pp. 254-263.
- Zur simultanen homogenen diophantischen Approximation II, Monatsh. Math.
 (1968), pp. 368-381.
- [8] Zur simultanen homogenen diophantischen Approximation III, Monatsh. Math. 74 (1970), pp. 166-171.

Received on 15.8.1970 (219)