ACTA ARITHMETICA
XXVI (1975)

On the congruences $\sigma(n) \equiv a \pmod{n}$ and $n \equiv a \pmod{\varphi(n)}$

by

CARL POMERANCE (Athens, Ga.)

1. Introduction. In this paper we study the sets

$$\begin{aligned} S(a) &= \{n:\ \sigma(n) \equiv a \pmod{n}\}, \\ S_k(a) &= \{n:\ \sigma(n) = kn + a\}, \\ F(a) &= \{n:\ n \equiv a \pmod{\varphi(n)}\}, \\ F_k(a) &= \{n:\ n = k\cdot\varphi(n) + a\}, \end{aligned}$$

where a and k are integers, n is a natural number, $\sigma(n)$ is the sum of the divisors of n, and $\varphi(n)$ is Euler's function.

There are several famous problems in number theory connected with certain of these sets. For example, $S_2(0)$ is the set of perfect numbers and $S(0)$ is the set of multiply perfect numbers. No one knows any odd members of $S(0)$ other than 1, nor is it known if $S(0)$ is infinite.

Another famous question is to identify the composite members of $F(1)$, if there are any.

Other problems that have been raised along these lines are: Is $S_2(1) = \emptyset$? (Cattaneo [1] has called members of $S_2(1)$ quasi-perfect.) What are the members of $F(-1)$? (D. H. Lehmer [8] identified 8 members of this set.) What are the members of $S_2(2)$? (Mąkowski [9] identified 11 members.) What are the members of $F(0)$? (Sierpiński [11], p. 232, completely described this set.)

From Sierpiński's description of $F(0)$ it follows that this set has density 0. Although a complete description is lacking for $S(0)$, Kanold [7] showed that this set also has density 0. The main result obtained in this paper is that for any choice for a, the sets $S(a)$ and $F(a)$ have density 0. In fact we show that the number of members of $S(a)$ (or $F(a)$) which are $\leqslant n$ is $O(n/\log n)$ and that for some choices of a this result is best possible.

If r is a real number, then a natural number n will be called *r-abundant* if $\sigma(n)/n \geqslant r$, and n will be called *primitive r-abundant* if the only divisor of n which is r-abundant is n itself. The main result of Section 4 is that if $a \geqslant 0$, then there are only finitely many members of $S_k(a)$ which are not primitive k-abundant numbers, with certain explicit exceptions given.

Another result obtained is that for every a, $S(a)$ contains at least two elements and $F(a)$ contains at least four elements.

2. Elementary observations.

THEOREM 1. *If $k \leqslant 1$, then $S_k(a)$ and $F_k(a)$ are finite sets for any choice of a, except that $S_1(1) = F_1(1) =$ the set of primes.*

Proof. This result is obvious if $k \leqslant 0$ or if $a \leqslant 1$. Hence we assume $k = 1$ and $a \geqslant 2$. Then every member of $S_1(a)$ and $F_1(a)$ is composite. Let n be an arbitrary composite number $> a^2$. Then n has a divisor b with $a < b < n$. Hence $\sigma(n) \geqslant n+b > n+a$ and $\varphi(n) \leqslant n-b < n-a$, so that $n \notin S_1(a)$ and $n \notin F_1(a)$. Hence every member of $S_1(a)$ and $F_1(a)$ is $\leqslant a^2$.

We ask for which values of k and a is $S_k(a)$ or $F_k(a)$ finite or infinite. Theorem 1 settles this question if $k \leqslant 1$. The following theorem identifies some infinite $S_k(a)$ and $F_k(a)$ where $k \geqslant 1$.

THEOREM 2. *If $n \in S(0)$, then $pn \in S_{\sigma(n)/n}(\sigma(n))$ for all primes $p \nmid n$. If $m \in F(0)$, then $pm \in S_{m/\varphi(m)}(m)$ for all primes $p \nmid m$.*

Proof. Let $n \in S(0)$ and let p be a prime with $p \nmid n$. Then $\sigma(pn) = (p+1)\sigma(n) = (\sigma(n)/n)pn + \sigma(n)$. Also if $m \in F(0)$ and p is a prime with $p \nmid m$, then $\varphi(pm) = (p-1)\varphi(m) = (\varphi(m)/m)(pm-m)$, so that $pm = (m/\varphi(m))\varphi(pm) + m$.

We note that Theorem 2 generalizes the observation of Mąkowski [9] that if n is perfect and p is a prime with $p \nmid n$, then $pn \in S_2(2n)$. We further note that Theorem 2 does not necessarily describe every member of a $S_{\sigma(n)/n}(\sigma(n))$ or a $F_{m/\varphi(m)}(m)$. Indeed $24 \in S_2(12)$ (where $n = 6 \in S_2(0)$) and $1122 \in F_3(162)$ (where $m = 162 \in F_3(0)$).

Mąkowski [9] has noted that $S_2(-1)$ contains every power of 2, so that there are infinite $S_k(a)$ which are not in the form $S_{\sigma(n)/n}(\sigma(n))$. We know of no other example. Also $F_2(0)$ contains every power of 2 and $F_3(0)$ contains every power of 6, so there are infinite $F_k(a)$ which are not in the form $F_{m/\varphi(m)}(m)$. Again we know of no other examples.

Theorem 2 suggests that we partition each $S(a)$ and $F(a)$ into two disjoint subsets:

$$S(a) = S^0(a) \cup S'(a),$$
$$F(a) = F^0(a) \cup F'(a),$$

where

$$S^0(a) = \{pn\colon p \text{ prime},\ p \nmid n,\ n \in S(0),\ \sigma(n) = a\},$$
$$S'(a) = S(a) \setminus S^0(a),$$
$$F^0(a) = \{pm\colon p \text{ prime},\ p \nmid m,\ m \in F(0),\ m = a\},$$
$$F'(a) = F(a) \setminus F^0(a).$$

Hence, in particular, if $a \neq \sigma(n)$ for all $n \in S(0)$, then $S'(a) = S(a)$, and if $a \notin F(0)$, then $F'(a) = F(a)$.

3. The main result.

LEMMA 1. *There is a constant a such that*

$$\frac{\sigma(n)}{n} < \frac{n}{\varphi(n)} < a \log\log n$$

for every natural number $n \geqslant 3$.

Lemma 1 follows from Theorems 328 and 329 in Hardy and Wright [5], p. 267.

LEMMA 2. *Let a be an integer, let c be a natural number, and let p_1, p_2 be primes such that* (i) *$p_i \nmid c$,* (ii) *$p_i > 2a \log\log c$ when $c \geqslant 3$,* (iii) *$p_i c > 4|a|$, and* (iv) *$p_i c \in S'(a)$ for $i = 1, 2$. Then $p_1 = p_2$.*

Proof. Let k_i be the integer $(\sigma(p_i c) - a)/p_i c$ for $i = 1, 2$. Suppose first that $k_1 = k_2 = k$. Then

$$kp_i c + a = \sigma(p_i c) = (p_i+1)\sigma(c),$$

so that

$$p_i[\sigma(c) - kc] = a - \sigma(c) \quad \text{for} \quad i = 1, 2.$$

That is,

$$p_1[\sigma(c) - kc] = p_2[\sigma(c) - kc] = a - \sigma(c),$$

and our result, $p_1 = p_2$, will follow provided we show $\sigma(c) - kc \neq 0$. But if $\sigma(c) - kc = 0$, then $a - \sigma(c) = 0$ and $c \in S(0)$. This contradicts condition (iv).

Now suppose $k_1 \neq k_2$, so say $k_1 > k_2$. But

$$(p_i+1)\sigma(c) = k_i p_i c + a$$

implies

$$(1+1/p_i)(\sigma(c)/c) = k_i + a/p_i c \quad \text{for} \quad i = 1, 2.$$

Then, since $k_1 - k_2 \geqslant 1$ and $|a/p_i c| < 1/4$, we have

$$\frac{1}{2} < k_1 - k_2 + \frac{a}{p_1 c} - \frac{a}{p_2 c} = \left(\frac{1}{p_1} - \frac{1}{p_2}\right)\frac{\sigma(c)}{c} < \frac{1}{p_1}\cdot\frac{\sigma(c)}{c}$$

so that $\sigma(c)/c > p_1/2 > a\log\log c$ when $c \geqslant 3$, contradicting Lemma 1. If $c = 1$, then clearly $\sigma(c)/c \not> p_1/2$. Finally, if $c = 2$, then (i) implies $p_1 \geqslant 3$, so again $\sigma(c)/c \not> p_1/2$.

LEMMA 3. *Let a be an integer, let c be a natural number, and let p_1, p_2 be primes with* (i) $p_i \nmid c$, (ii) $p_i > 1+2a\log\log c$ *when* $c \geqslant 3$, (iii) $p_i c > 64a^2$, *and* (iv) $p_i c \in F'(a)$ *for* $i = 1, 2$. *Then* $p_1 = p_2$.

We omit the proof of Lemma 3 since it is almost identical with that of Lemma 2. We note that it is helpful to use the fact that $\varphi(n) > \sqrt{n}/2$ for every natural number n (cf. Sierpiński [11], p. 230).

LEMMA 4. *Let n be a natural number and let*

$$x = (\log n \log\log n)^{1/2}.$$

Then the number of natural numbers $m \leqslant n$ which do not satisfy both of the conditions:

(1) *the greatest prime factor of m is greater than $e^{x/\sqrt{2}}$;*

(2) *the square of the greatest prime factor of m does not divide m;*

is $O(n/e^{\beta x})$ where $\beta < 1/\sqrt{2}$ is an arbitrary constant.

If we let β be a constant $< 1/24$, then Lemma 4 is an immediate corollary of a lemma proved by Erdös [3], pp. 50–51. Actually, the truth of Lemma 4 for some positive constant β is the main thing, not how large we may take β, for all of the corollaries to Theorem 3 would remain true. For this reason, we omit the proof that any $\beta < 1/\sqrt{2}$ will do. This proof is easily obtained by sharpening the estimates made by Erdös in the cited lemma.

THEOREM 3. *Let a be an arbitrary integer. The number of members m of $S'(a)$ (or $F'(a)$) which are $\leqslant n$ is*

$$O\left(\frac{n}{e^{\beta(\log n \log\log n)^{1/2}}}\right)$$

where $\beta < 1/\sqrt{2}$ is arbitrary.

COROLLARY 1. *The number of members m of $S'(a)$ (or $F'(a)$) which are $\leqslant n$ is*

$$O\left(\frac{n}{(\log n)^j}\right)$$

for any j.

COROLLARY 2. *The sum of the reciprocals of the members of $S'(a)$ (or $F'(a)$) converges.*

COROLLARY 3. *The number of members m of $S(a)$ (or $F(a)$) which are $\leqslant n$ is*

$$O\left(\frac{n}{\log n}\right).$$

In particular, $S(a)$ and $F(a)$ have density 0.

Proof of Corollary 3. This is a combination of the Prime Number Theorem (or the weaker $\pi(n) = O(n/\log n)$), Theorem 3, and the partition of $S(a)$ and $F(a)$ mentioned at the end of Section 2.

Proof of Theorem 3. In the notation of Lemmas 1 and 4, let n be large enough so that $e^{x/\sqrt{2}} > 1+2a\log\log n$. In view of Lemma 4 we may ignore those numbers $m \leqslant n$ which do not satisfy conditions (1) and (2) of that lemma. Let the members of $S'(a)$ (resp. $F'(a)$) which are $\leqslant n$ and $\geqslant 64a^2$ and which satisfy conditions (1) and (2) of Lemma 4 be $m_1, m_2, \ldots, m_t$. Let p_i be the largest prime dividing m_i, and write $m_i = p_i c_i$, where $p_i \nmid c_i$. Then for $i = 1, 2, \ldots, t$ we have $c_i \leqslant n/e^{x/\sqrt{2}}$. Hence it will be sufficient to show that $c_1, c_2, \ldots, c_t$ are all distinct. But this follows from Lemma 2 (resp. Lemma 3). This completes the proof of the main theorem.

We remark that much better estimates are available for $S(0)$ and $F(0)$. Indeed, Hornfeck and Wirsing [6] (also see Wirsing [12]) proved that the number of members of $S(0)$ which are $\leqslant n$ is $O(n^\varepsilon)$ for every $\varepsilon > 0$. Sierpiński noted that

$$F(0) = \{1\} \cup \{2^i 3^j\colon i > 0, j \geqslant 0\}.$$

Hence the number of members of $F(0)$ which are $\leqslant n$ is $O\big((\log n)^2\big)$.

It might be true that for a general a, the sets $S'(a)$ and $F'(a)$ are just as sparse as $S(0)$ and $F(0)$. Indeed, we know of no counter-example. But we also know of no proof.

Had our only goal been to prove that $S(a)$ and $F(a)$ have density 0, there would have been a shorter route which would have by-passed the need for Lemmas 1–4. Indeed, making use of the continuous distribution functions of $\sigma(n)/n$ and $n/\varphi(n)$ (cf. Davenport [2], Erdös [4], and Schoenberg [10]), the result is almost immediate.

4. Other results.

THEOREM 4. *For every a, there are at least two members of $S(a)$ and four members of $F(a)$.*

Proof. First we note that $1 \in S(a)$ for every a. Suppose $a \neq 0$ or 2. Then there is a prime p with $p \mid a-1$, and hence $p \in S(a)$. In addition $6 \in S(0)$ and $20 \in S(2)$.

To prove the assertion about $F(a)$, we first note that 1 and $2 \in F(a)$ for every a. In addition 4 and $6 \in F(a)$ for every even a. Hence we may assume a is odd. Then $3 \in F(a)$. Now every odd a satisfies precisely one of the following congruences:

$$a \equiv 1\ (4), \quad a \equiv 7\ (8), \quad a \equiv 3\ (24), \quad a \equiv 11\ (24), \quad a \equiv 19\ (24).$$

But $5 \in F(a)$ if $a \equiv 1\ (4)$, $15 \in F(a)$ if $a \equiv 7\ (8)$, $9 \in F(a)$ if $a \equiv 3\ (24)$, $35 \in F(a)$ if $a \equiv 11\ (24)$, and $7 \in F(a)$ if $a \equiv 19\ (24)$.

With regards to possibly improving Theorem 4, we remark that we know of no members of $S(5)$ other than 1 and 2. However it might well be provable that every $F(a)$ contains at least 5 members, since we cannot find an a for which 5 members of $F(a)$ are not easily obtained.

We noted in the proof of Theorem 4 that $p \in S(a)$ for every prime p dividing $a-1$. But $a-1$ is "usually" divisible by $\log\log(a-1)$ distinct primes (cf. Theorem 431 in Hardy and Wright [5], p. 356). Hence given any N, the set of all a for which $S(a)$ has $\leqslant N$ elements has density 0 in $\mathbf{Z}$. We do not know if the same is true for $F(a)$. However it is easy to obtain a weaker result: namely, given N, the set of all a for which $F(a)$ has $\leqslant N$ elements has upper density < 1 in $\mathbf{Z}$. Indeed, if m is a natural number $\geqslant N$ and if $a \equiv 0 \pmod{2^m}$, then $2^i \in F(a)$ for $i = 0, 1, \ldots, m+1$, so that $F(a)$ has $\geqslant m+2 > N$ elements.

We recall now the definition of a primitive r-abundant number (cf. Section 1).

THEOREM 5. *Let $a \geqslant 0$, k be integers. Then there are at most finitely many members of $S_k(a) \cap S'(a)$ which are not primitive k-abundant numbers.*

To prove Theorem 5, we shall need the following lemma:

LEMMA 5. *If m is a proper divisor of n, then $\sigma(m)/m < \sigma(n)/n$. Further, if $\sigma(n)/n \geqslant k$, then*

$$\sigma(m) - km < \sigma(n) - kn.$$

Proof. The first assertion follows from the fact that $\sigma(x)/x$ is a multiplicative function of x, and if $x = p^a$, a prime power, we have $\sigma(p^a)/p^a = 1 + p^{-1} + \ldots + p^{-a}$. To prove the second assertion, we note that $\sigma(m)/m < \sigma(n)/n$ implies

$$\frac{\sigma(m) - km}{m} < \frac{\sigma(n) - kn}{n}.$$

Since $\sigma(n) - kn \geqslant 0$ and since $0 < m < n$, we have

$$\frac{\sigma(n) - kn}{n} \leqslant \frac{\sigma(n) - kn}{m}$$

and our conclusion follows.

Proof of Theorem 5. If $n \in S_k(a)$ is not a primitive k-abundant number, the first part of Lemma 5 implies we can write $n = mp$ where

$\sigma(m) \geqslant km$ and p is a prime. Hence if Theorem 5 fails, there is a sequence $m_1 p_1 < m_2 p_2 < \ldots$ such that $m_i p_i \in S_k(a) \cap S'(a)$, $\sigma(m_i) \geqslant km_i$, and p_i is prime. By passing to an infinite subsequence, we may assume either

1. $p_i \mid m_i$ for $i = 1, 2, \ldots$;
2. $p_i \nmid m_i$ for $i = 1, 2, \ldots$

Assume Case 1 holds. Let $x_i > 0$ be such that $p_i^{x_i} \| m_i$. If $\{m_i\}$ is a finite set, then $\{p_i\}$ is a finite set, and hence $\{m_i p_i\}$ is a finite set, a contradiction. Hence by passing to an infinite subsequence, we may assume $m_1, m_2, \ldots$ are mutually distinct.

Now for $i = 1, 2, \ldots$, we have

$$a = \sigma(m_i p_i) - km_i p_i = \frac{\sigma(p_i^{x_i+1})}{\sigma(p_i^{x_i})}\,\sigma(m_i) - km_i p_i \tag{1}$$

so that

$$a = p_i[\sigma(m_i) - km_i] + \frac{\sigma(m_i)}{\sigma(p_i^{x_i})}. \tag{2}$$

Hence

$$a \geqslant \frac{\sigma(m_i)}{\sigma(p_i^{x_i})} = \sigma\left(\frac{m_i}{p_i^{x_i}}\right) \geqslant \frac{m_i}{p_i^{x_i}}.$$

Hence by passing to an infinite subsequence, we may assume

$$\frac{m_1}{p_1^{x_1}} = \frac{m_2}{p_2^{x_2}} = \ldots \tag{3}$$

Hence there is a natural number μ such that for $i = 1, 2, \ldots$ we have

$$m_i = \mu p_i^{x_i}. \tag{4}$$

Suppose for some $i \neq j$ we had $p_i = p_j$. Then since $m_i \neq m_j$, (4) implies $x_i \neq x_j$, say $x_i < x_j$. Then $m_i p_i$ is a proper divisor of $m_j p_j$, so that (1) contradicts Lemma 5. Hence we have that $p_1, p_2, \ldots$ are mutually distinct. But (2) gives us

$$a = p_i[\sigma(m_i) - km_i] + \sigma(\mu), \tag{5}$$

and hence for $i = 1, 2, \ldots$, we have $p_i \mid a - \sigma(\mu)$. Since the p_i are mutually distinct, we must have $a = \sigma(\mu)$. Then (5) implies $\sigma(m_i) = km_i$ for $i = 1, 2, \ldots$ Hence

$$\sigma(\mu) = \frac{\sigma(m_i)}{\sigma(p_i^{x_i})} = \frac{km_i}{p_i^{x_i}} \cdot \frac{p_i^{x_i}}{\sigma(p_i^{x_i})},$$

so that (3) implies

$$\frac{p_1^{x_1}}{\sigma(p_1^{x_1})} = \frac{p_2^{x_2}}{\sigma(p_2^{x_2})} = \ldots$$

But the fractions $p_i^{x_i}/\sigma(p_i^{x_i})$ appear in reduced form, so $p_1^{x_1} = p_2^{x_2} = \ldots$, a conclusion we have already seen is impossible. Hence Case 1 does not occur.

Assuming Case 2 holds, we note that

$$a = \sigma(m_i p_i) - km_i p_i = (p_i+1)\sigma(m_i) - km_i p_i = p_i[\sigma(m_i) - km_i] + \sigma(m_i).$$

Then if $\sigma(m_i) = km_i$, we would have $a = \sigma(m_i)$ and hence $m_i p_i \notin S'(a)$, a contradiction. Hence we may assume $\sigma(m_i) > km_i$. Then for $i = 1, 2, \ldots$, we have

$$a \geqslant p_i + \sigma(m_i) \geqslant p_i + m_i.$$

But either $\{p_i\}$ or $\{m_i\}$ is unbounded, so we have a contradiction. This completes the proof of Theorem 5.

References

[1] P. Cattaneo, *Sui numeri quasiperfetti*, Boll. Un. Mat. Ital. (3) 6 (1951), pp. 59–62.
[2] H. Davenport, *Über Numeri Abundantes*, Sitzungsberichte der Preussichen Akademie, Phys. Math. Klasse (1933), pp. 830–837.
[3] P. Erdös, *On primitive abundant numbers*, J. London Math. Soc. 10 (1935), pp. 49–58.
[4] — *On the density of some sequences of numbers: III*, J. London Math. Soc. 13 (1938), pp. 119–127.
[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fourth edition, Oxford 1960.
[6] B. Hornfeck und E. Wirsing, *Über die Häufigkeit vollkommener Zahlen*, Math. Ann. 133 (1957), pp. 431–438.
[7] H.-J. Kanold, *Über die Verteilung der vollkommenen Zahlen und allgemeinerer Zahlenmengen*, Math. Ann. 132 (1956), pp. 442–450.
[8] D. H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc. 38 (1932), pp. 745–757.
[9] A. Mąkowski, *Remarques sur les fonctions $\theta(n)$, $\varphi(n)$ et $\sigma(n)$*, Mathesis 69 (1960), pp. 302–303.
[10] I. J. Schoenberg, *Über die asymptotische Verteilung reeler Zahlen* mod 1, Math. Zeitschr. 28 (1928), pp. 171–200.
[11] W. Sierpiński, *Elementary Theory of Numbers*, Warszawa 1964.
[12] E. Wirsing, *Bemerkung zu der Arbeit über vollkommene Zahlen*, Math. Ann. 137 (1959), pp. 316–318.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF GEORGIA
Athens, Georgia

Received on 29. 9. 1973 (465)

ACTA ARITHMETICA
XXVI (1975)

An "exact" formula for the $2n$-th Bernoulli number

by

HANS RIESEL (Stockholm)

Summary. In [1], Chowla and Hartung prove the following formula for the Bernoulli number B_{2n}: The integer

$$2(2^{2n}-1)(-1)^{n-1}B_{2n} = 1 + \left[\frac{2(2^{2n}-1)(2n)!}{2^{2n-1}\pi^{2n}} \sum_{k=1}^{3n} k^{-2n}\right], \tag{1}$$

where $[x]$ as usual denotes the greatest integer $\leqslant x$. The idea behind the above formula is to use the formula

$$\zeta(2n) = \sum_{k=1}^{\infty} k^{-2n} = \frac{2^{2n-1}\pi^{2n}(-1)^{n-1}B_{2n}}{(2n)!}, \tag{2}$$

and to sum the series for $\zeta(2n)$ far enough to get the rational number B_{2n} out sufficiently accurate in order to have its precise value determined. According to heavy overestimation of the denominator of B_{2n}, however, (1) sums the series in (2) unnecessarily far. The objective of the present paper is to show that a much smaller number of terms suffices in the series for $\zeta(2n)$. It turns out as is natural to suspect, that the B_{2n}'s with large denominators will need more terms than the others in a formula of the Chowla–Hartung type; to make a comparison, our formula (13) needs only 4 terms for B_{36}, which has a large denominator 1919190, where Chowla–Hartung's formula needs 54 terms. The number of terms needed to get B_{36} at all precisely by the used technique is in this case 3. We also deduce a corresponding formula with the denominators entirely removed by the use of the von Staudt–Clausen theorem. It needs still fewer terms from the series for $\zeta(2n)$.

An upper bound for the denominator Q_{2n} of $B_{2n} = P_{2n}/Q_{2n}$. As is well-known, the denominator of B_{2n} is

$$Q_{2n} = \prod_{(p-1)|2n} p, \tag{3}$$