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

by

CARL POMERANCE (Athens, Ga.)

I. Introduction. In this paper we study the sets

$$S(a) = \{ n : \sigma(n) = a \pmod{n} \},$$

$$S_k(a) = \{ n : \sigma(n) = kn + a \},$$

$$F(a) = \{ n : n = a \pmod{\varphi(n)} \},$$

$$F_k(a) = \{ n : n = k \varphi(n) + a \},$$

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 $S_2(2)$? (Makowski [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 $\leq n$ 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 $\sigma(n)/n > r$, 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 $a > 0$, 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 $k \leq 1$, then $S_k(a)$ and $F_k(a)$ are finite sets for any choice of $a$, except that $S_1(1) = F_1(1)$ is the set of primes.

**Proof.** This result is obvious if $k \leq 0$ or if $a < 1$. Hence we assume $k = 1$ and $a \geq 2$. 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 $a < b < c$. Hence $\sigma(n) > n = b > n + a$ and $\varphi(n) < n - b > n - a$, 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 $< a^2$.

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 $k \leq 1$. The following theorem identifies some infinite $S_k(a)$ and $F_k(a)$ where $k \geq 1$.

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

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

We note that Theorem 2 generalizes the observation of Mąkowski [9] that if $n$ is perfect and $p$ a prime with $p \mid n$, then $p \in S_1(2n)$. We further note that Theorem 2 does not necessarily describe every member of $S_{m/n}(\sigma(n))$ or a $F_{m/n}(m)$. Indeed $24 \notin S_{12}(12)$ (where $n = 6 \in S_1(0)$) and $122 \notin F_{162}(162)$ (where $m = 162 \in F_0(0)$).

Mąkowski [9] has noted that $S_1(-1)$ contains every power of 2, so that there are infinite $S_k(a)$ which are not in the form $S_{m/n}(\sigma(n))$. We know of no other example. Also $F_1(0)$ contains every power of 2, and $F_2(0)$ contains every power of 6, so there are infinite $F_3(a)$ which are not in the form $F_{m/n}(m)$. 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

$$S^*(a) = \{p \in S(a) \mid p \mid a, a \in S(0), \sigma(a) = a\},$$

$$F^*(a) = \{m \in F(a) \mid m \in F(0), m \mid a\},$$

$$F^0(a) = F(a) \setminus F^*(a).$$

Hence, in particular, if $a \notin S(0)$ for all $a \in S(0)$, 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 $\alpha$ such that

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

for every natural number $n \geq 3$.

Lemma 1 follows from Theorems 328 and 329 in Hardy and Wright [6, p. 267].

**Lemma 2.** Let $a$ be an integer, let $e$ be a natural number, and let $p_1, p_2$ be primes such that (i) $p_1 \mid e$, (ii) $p_1 > 2\log e$ when $e \geq 3$, (iii) $p_2 > 4|a|$, and (iv) $p_2 \mid S_i(a)$ for $i = 1, 2$. Then $p_1 \mid p_2$.

**Proof.** Let $k_1$ be the integer $|\sigma(p_1 e - a)|/p_1 e$ for $i = 1, 2$. Suppose first that $k_1 = k_2 = k$. Then

$$k_1 p_2 c - a = k_2 p_2 c = (p_1 + 1) \sigma(e),$$

so that

$$p_1 (\sigma(e) - k_2 e) = a - \sigma(e) \quad \text{for} \quad i = 1, 2.$$

That is,

$$p_1 (\sigma(e) - k_2 e) = p_2 (\sigma(e) - k_2 e) = a - \sigma(e),$$

and our result $p_1 = p_2$, will follow provided we show $\sigma(e) - k_2 e = 0$. But if $\sigma(e) - k_2 e = 0$, then $a - \sigma(e) = 0$ and $e \in S(0)$. This contradicts condition (iv).

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

$$(p_1 + 1) \sigma(e) = k_1 p_2 c - a$$

implies

$$(1 - 1/p_1) \sigma(e)/p_1 e = k_1 + a/p_1 e$$

for $i = 1, 2$.

Then, since $k_1 - k_2 > 0$ and $|a/p_1 e| < 1/4$, we have

$$\frac{1}{2} < k_1 - k_2 + \frac{a}{p_1 e} = \frac{1}{p_1} (1 - \frac{1}{p_2}) < \frac{1}{p_1} \sigma(e)$$
so that \( \sigma(x)/x > p_1/2 > \alpha \log \log x \) when \( c > 3 \), contradicting Lemma 1. If \( c = 1 \), then clearly \( \sigma(x)/x > p_1/2 \). Finally, if \( c = 2 \), then (i) implies \( p_1 > 3 \), so again \( \sigma(x)/x > p_1/2 \).

Lemma 3. Let \( n \) be an integer, let \( m \) be a natural number, and let \( p_1, p_2 \) be primes with (i) \( p_1 < m \), (ii) \( p_1 > 1 + 2 \alpha \log \log n \) when \( c > 3 \), (iii) \( p_1 > 64 \alpha^2 \), and (iv) \( p_1 \alpha \sigma(p_1) \) for \( 1 \leq i \leq 2 \). 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 \( \psi(n) > \sqrt{n}/2 \) for every natural number \( n \) (cf. Sierpiński [11], p. 230).

Lemma 4. Let \( n \) be a natural number and let

\[
\sigma = \left( \log n \log \log n \right)^{1/2}.
\]

Then the number of natural numbers \( m \leq n \) which do not satisfy both of the conditions:

1. The greatest prime factor of \( m \) is greater than \( \sigma \sqrt{\log \sigma} \);
2. The square of the greatest prime factor of \( m \) does not divide \( m \);

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

If we let \( \beta \) be a constant \( < 1/24 \), then Lemma 4 is an immediate corollary of a lemma proved by Erdős [3], pp. 50–51. Actually, the truth of Lemma 4 for some positive constant \( \beta \) is the main thing, not how large we may take \( \beta \), 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 Erdős 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 \( \leq n \) is

\[
O\left( \frac{n}{\sigma^{2/3} \left( \log n \right)^{2/3}} \right)
\]

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

Corollary 1. The number of members \( m \) of \( S'(a) \) (or \( F'(a) \)) which are \( \leq n \) is

\[
O\left( \frac{n}{\log n} \right)
\]

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 \( \leq n \) 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 partial sum 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 \( \sigma > 1 + 2 \alpha \log \log n \). In view of Lemma 4 we may ignore those numbers \( m \leq n \) which do not satisfy condition (1) and (2) of that lemma. Let the members of \( S'(a) \) (resp. \( F'(a) \)) which are \( \leq n \) and \( \geq 64 \alpha^2 \) and which satisfy conditions (1) and (2) of Lemma 4 be \( m_1, m_2, \ldots, m_\ell \). Let \( p_i \) be the largest prime dividing \( m_i \), and write \( m_i = p_i c_i \), where \( p_i = \sigma(a) \). Then for \( i = 1, 2, \ldots, \ell \) we have \( c_i \leq n/\sigma(a) \). Hence it will be sufficient to show that \( c_1, c_2, \ldots, c_\ell \) 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 \( \leq n \) is \( O(n^r) \) for every \( r > 0 \). Sierpiński noted that

\[
F(0) = \{1\} \cup \{2^j 3^j : j > 0, j \geq 0\}.
\]

Hence the number of members of \( F(0) \) which are \( \leq n \) is \( O(n^{3/2}) \).

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 \( n/\psi(n) \) (cf. Davenport [2], Erdős [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 \( p|a-1 \), and hence \( p \in S(a) \). In addition \( a \in S(0) \) and \( 2a \in S(2) \).

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

\[
\begin{align*}
3 \equiv 1 \pmod{4}, & \quad a = 7 \pmod{8}, & \quad a = 3 \pmod{24}, & \quad a = 11 \pmod{24}, & \quad a = 19 \pmod{24}.
\end{align*}
\]

But \( 5^a F(a) \) if \( a = 1 \pmod{4}, \; 15^a F(a) \) if \( a = 7 \pmod{8}, \; 9^a F(a) \) if \( a = 3 \pmod{24}, \; 36^a F(a) \) if \( a = 11 \pmod{24}, \) and \( 7^a F(a) \) if \( a = 19 \pmod{24}. \)

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 451 in Hardy and Wright [3], p. 356). Hence given any \( N \), the set of all \( a \) for which \( S(a) \) has \( < N \) elements has density 0 in \( \mathbb{Z} \). 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 \( < N \) elements has upper density \( < 1 \) in \( \mathbb{Z} \). Indeed, if \( m \) is a natural number \( < N \) and if \( a = 0 \pmod{2^m} \), then \( 2^m F(a) \) for \( i = 0, 1, \ldots, m + 1 \), so that \( F(a) \) has \( > m + 1 > N \) elements.

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

**Theorem 5.** Let \( a \geq 0 \), \( b \) be integers. Then there are at most finitely many members of \( S_b(a) \cap S_a(a) \) 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 \( \sigma(n)/n \geq k \), 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 \( a = p^n \), a prime power, we have \( \sigma(p^n)/p^n = 1 + p + \ldots + p^{n-1} \). 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 \( \sigma(n) - kn \geq 0 \) and since \( 0 < m < n \), we have

\[
\frac{\sigma(n) - kn}{n} \leq \frac{\sigma(n) - km}{m}
\]

and our conclusion follows.

**Proof of Theorem 5.** If \( n \in S_b(a) \) is not a primitive \( k \)-abundant number, the first part of Lemma 5 implies we can write \( n = mp \) where \( \sigma(m) \geq km \) and \( p \) is a prime. Hence if Theorem 5 fails, there is a sequence \( m_1, p_1, \ldots, m_2, p_2, \ldots \) such that \( m_i, p_i \in S_b(a) \cap S_a(a) \), \( \sigma(m_i) \geq km_i \), 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 \( p_i^{x_i} \mid m_i \). 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

\[
\begin{align*}
(1) & \quad a = \sigma(m_i, p_i) - km_i, p_i = \sigma(p_i^{x_i}) - \sigma(p_i^{x_i}) = \sigma(m_i) - km_i, p_i \\
(2) & \quad b = \sigma(m_i) - km_i, p_i = \sigma(p_i^{x_i}) - \sigma(p_i^{x_i}) = \sigma(m_i) - km_i, p_i.
\end{align*}
\]

so that

\[
\begin{align*}
(3) & \quad a \geq \sigma(m_i) - km_i, p_i = \sigma(p_i^{x_i}) - \sigma(p_i^{x_i}) = \sigma(m_i) - km_i, p_i.
\end{align*}
\]

Hence by passing to an infinite subsequence, we may assume

\[
\begin{align*}
\frac{m_1}{p_1^{x_1}} = \frac{m_2}{p_2^{x_2}} = \ldots
\end{align*}
\]

Hence there is a natural number \( \mu \) such that for \( i = 1, 2, \ldots \) we have

\[
\begin{align*}
(4) & \quad m_i = \mu p_i^{x_i}.
\end{align*}
\]

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

\[
\begin{align*}
(5) & \quad a = \sigma(p_i, \sigma(m_i) - km_i, p_i - \sigma(m_i)) - \sigma(\mu),
\end{align*}
\]

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

\[
\begin{align*}
(6) & \quad \sigma(m_i) = \frac{\sigma(m_i)}{\sigma(p_i^{x_i})} = \frac{km_i}{p_i^{x_i}} = \frac{p_i^{x_i}}{p_i^{x_i}} = \frac{p_i^{x_i}}{p_i^{x_i}}.
\end{align*}
\]

so that (3) implies

\[
\begin{align*}
(7) & \quad \frac{m_1}{p_1^{x_1}} = \frac{m_2}{p_2^{x_2}} = \ldots
\end{align*}
\]
But the fractions \( p_i^2 \sigma(p_i) / (p_i^2) \) appear in reduced form, so \( p_i^2 = p_i^2 = \ldots \), a conclusion we have already seen is impossible. Hence Case 1 does not occur.

Assuming Case 2 holds, we note that

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

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

\[
a > p_i + \sigma(m_i) > p_i + m_i.
\]

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

References

[9] A. Mąkowski, Remarques sur les fonctions \( \phi(n) \), \( \varphi(n) \) et \( \varphi(n) \), Mathesis 69 (1960), pp. 302–303.

Department of Mathematics
University of Georgia
Athens, Georgia

Received on 29. 9. 1973