MATHEMATICS OF COMPUTATION
Volume 67, Number 222, April 1998, Pages 843–861
S 0025-5718(98)00951-X

WILSON QUOTIENTS FOR COMPOSITE MODULI

TAKASHI AGOH, KARL DILCHER, AND LADISLAV SKULA

Abstract. An analogue for composite moduli $m \geq 2$ of the Wilson quotient is studied. Various congruences are derived, and the question of when these quotients are divisible by m is investigated; such an m will be called a "Wilson number". It is shown that numbers in certain infinite classes cannot be Wilson numbers. Eight new Wilson numbers up to 500 million were found.

1. Introduction

One of the most classical and celebrated theorems in number theory is Wilson's Theorem (see, e.g. [5] or [11]):

Theorem 1.1 (Wilson's Theorem). *If p is a prime, then*

$$(p-1)! \equiv -1 \pmod{p}.$$

It is particularly attractive since, together with its converse due to Lagrange, it characterizes the primes. Also, it allows us to introduce special quotients which are integers.

Definition 1.1. Let p be a prime. The quotient

$$w_p := \frac{(p-1)!+1}{p}$$

is called the *Wilson quotient of p*. The prime p is called a *Wilson prime* if

$$w_p \equiv 0 \pmod{p}.$$

These objects have been extensively studied (see, e.g., [5], [9], [10], or [11]). The first two Wilson primes are 5 and 13. Goldberg (1953) discovered the third Wilson prime 563, and subsequent searches by various authors showed that there are no other such primes below 5×10^8 (see [4], [6], [7], [11], and [12]).

It is the aim of this paper to investigate analogs of the quotients w_p for composite moduli. Our generalization is based on the following classical theorem.

Received by the editor January 23, 1995 and, in revised form, May 22, 1996.

1991 *Mathematics Subject Classification.* Primary 11A07; Secondary 11B68.

The first author was supported in part by a grant of the Ministry of Education, Science and Culture of Japan.

The second author's research was supported by NSERC of Canada.

Research of the third author was supported by the Grant Agency of the Czech Republic, "Number Theory, its Algebraic Aspects and its Relationship to Computer Science", No. 201/93/2/22.

Theorem 1.2 (Wilson's Theorem for composite moduli). *Let $m \geq 2$ be an integer, and set $\epsilon_m = -1$ when $m = 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime and α a positive integer, and $\epsilon_m = 1$ otherwise. Then*

$$\prod_{\substack{j=1\\(j,m)=1}}^{m} j \equiv \epsilon_m \pmod{m}.$$

This theorem was first stated by Gauss who gave an outline of a proof (see [5], p. 65). Note that $\epsilon_m = -1$ if and only if m has a primitive root.

The theorem enables us to introduce generalized Wilson quotients for arbitrary integers $m \geq 2$. Although they have occurred in the literature, they have so far not been studied in any great detail.

In Section 2 we investigate these quotients and mention some extensions of results of E. Lehmer [10]. Section 3 is devoted to the composite Wilson numbers. Some congruences concerning generalized Wilson quotients are derived; they are useful in the search for Wilson numbers.

In Section 4 we study the values of generalized Wilson quotients mod 3 for integers $3m$ and $9m$, where m is a squarefree integer ≥ 2 with all prime divisors congruent to 2 mod 3. Finally, Sections 5 and 6 deal with the actual search for Wilson numbers.

2. Wilson quotients for composite moduli

On the basis of Theorem 1.2 (Wilson's Theorem for composite moduli) we will define the Wilson quotient for arbitrary integers $m \geq 2$.

Definition 2.1. Let $m \geq 2$ be an integer, and ϵ_m be as defined in Theorem 1.2. Denote

$$P(m) = \prod_{\substack{j=1\\(j,m)=1}}^{m} j.$$

Then the integer

$$W(m) = \frac{P(m) - \epsilon_m}{m}$$

is called the *generalized Wilson quotient* of m.

We will now derive some basic congruences, analogous to the known congruences for Wilson quotients with prime moduli. First we need another definition.

Definition 2.2. Let a and $m \geq 2$ be relatively prime integers. The quotient

$$q(a, m) = \frac{a^{\phi(m)} - 1}{m}$$

will be called the *Euler quotient of m with base a*.

Note that by Euler's Theorem, this quotient is an integer. It was first studied by Lerch [9]; for further properties, see [2]. The two quotients just defined are related by the following fundamental congruence.

Proposition 2.1. *For integers $m \geq 3$ we have*

$$\epsilon_m \phi(m) W(m) \equiv \sum_{\substack{a=1\\(a,m)=1}}^{m} q(a,m) \pmod{m}.$$

For $m = p$ (an odd prime) this congruence is due to Lerch [9, (4)].

Proof. Using the definitions of $P(m)$ and the Euler quotients, we have

$$\begin{aligned} P(m)^{\phi(m)} &= \prod_{\substack{a=1\\(a,m)=1}}^{m} a^{\phi(m)} = \prod_{\substack{a=1\\(a,m)=1}}^{m} (1 + mq(a,m)) \\ &\equiv 1 + m \sum_{\substack{a=1\\(a,m)=1}}^{m} q(a,m) \pmod{m^2}. \end{aligned}$$

On the other hand, we get

$$\begin{aligned} P(m)^{\phi(m)} &= (\epsilon_m + mW(m))^{\phi(m)} \\ &\equiv \epsilon_m^{\phi(m)} + \phi(m)\epsilon_m^{\phi(m)-1} mW(m) \pmod{m^2} \\ &= 1 + \epsilon_m \phi(m) mW(m) \pmod{m^2}, \end{aligned}$$

and the result follows. □

Proposition 2.2. *For integers $m \geq 3$ and $t \geq 1$ we have*

$$\sum_{\substack{a=1\\(a,m)=1}}^{m} a^{t\phi(m)} \equiv \phi(m) + \epsilon_m tm\phi(m) W(m) \pmod{m^2}.$$

Proof. We use the definition of $q(a,m)$,

$$a^{t\phi(m)} = (a^{\phi(m)})^t = (1 + mq(a,m))^t \equiv 1 + tmq(a,m) \pmod{m^2}$$

and sum over the a's to get

$$\begin{aligned} \sum_{\substack{a=1\\(a,m)=1}}^{m} a^{t\phi(m)} &\equiv \sum_{\substack{a=1\\(a,m)=1}}^{m} (1 + tmq(a,m)) \pmod{m^2} \\ &= \phi(m) + tm \sum_{\substack{a=1\\(a,m)=1}}^{m} q(a,m) \\ &\equiv \phi(m) + \epsilon_m tm\phi(m) W(m) \pmod{m^2} \end{aligned}$$

by Proposition 2.1. □

For another expression of the right-hand side in Proposition 2.2 we need the following result due to Agoh [1, 3.1]. Here and in what follows, B_i denotes the ith Bernoulli number (in even-index notation).

Proposition 2.3 (Agoh). *For positive integers m and n we have*

$$\sum_{i=1}^{n+1} \binom{n+1}{i} H_{n+1-i}(m) m^i = (n+1) \sum_{\substack{a=1\\(a,m)=1}}^{m} a^n,$$

where

$$H_i(m) = \prod_{p \mid m} (1 - p^{i-1}) B_i$$

(with the product taken over all prime divisors p of m).

Notation. Let t and m be integers, $t \geq 1$, $m \geq 3$. For $1 \leq i \leq t\phi(m) + 1$ set

$$M_i = \frac{1}{i} \binom{t\phi(m)}{i-1} H_{t\phi(m)+1-i}(m) m^i.$$

Note that for i even we have $M_i = 0$ and since

$$\frac{1}{n+1} \binom{n+1}{i} = \frac{1}{i} \binom{n}{i-1}$$

for positive integers i, n with $i \leq n+1$, we get from Proposition 2.3

$$\sum_{\substack{a=1 \\ (a,m)=1}}^{m} a^{t\phi(m)} = \sum_{\substack{i=1 \\ i \text{ odd}}}^{t\phi(m)+1} M_i. \tag{2.1}$$

Proposition 2.4. *For integers $m \geq 3$ and $t \geq 1$ we have*

$$\begin{aligned} \epsilon_m t m \phi(m) W(m) &\equiv -\phi(m) + M_1 + M_3 \pmod{m^2} \\ &= -\phi(m) + m \prod_{p \mid m} (1 - p^{t\phi(m)-1}) B_{t\phi(m)} \\ &\quad + \frac{1}{3} \binom{t\phi(m)}{2} m^3 \prod_{p \mid m} (1 - p^{t\phi(m)-3}) B_{t\phi(m)-2}. \end{aligned}$$

Proof. Let p be a prime dividing m, and $5 \leq i \leq t\phi(m) + 1$, i odd. Let $\text{ord}_p m$ denote the highest power of p dividing m. Put $\text{ord}_p m = \alpha, \text{ord}_p i = \beta$. Then $\alpha \geq 1$ and $\beta \geq 0$. We want to show that $\text{ord}_p M_i \geq 2\alpha$. We have $\text{ord}_p M_i \geq i\alpha - \beta - 1$. If $\beta \in \{0, 1\}$, then $i\alpha - \beta - 1 \geq 5\alpha - 2 \geq 2\alpha$. Suppose $\beta \geq 2$. Then $p \geq 3$ (because i is odd) and $\alpha i - \beta - 1 - 2\alpha \geq \alpha(3^\beta - 2) - \beta - 1 \geq 3^\beta - (\beta + 3) > 0$. The result follows. □

Next we wish to determine under which conditions the term M_3 can be omitted. We use the following lemma.

Lemma 2.1. *Let $m \geq 3$ and $t \geq 1$ be integers.*

(a) *If $m = 3p_1 \ldots p_k$, where $p_1, \ldots, p_k$ are primes $\equiv 2 \pmod 3$ $(k \geq 0)$, then*

$$\text{ord}_3 M_3 = \text{ord}_3 t + \text{ord}_3(t\phi(m) - 1) + 1.$$

(b) *In all other cases of m and for a prime $p \mid m$ we have*

$$\text{ord}_p M_3 \geq 2\text{ord}_p m.$$

Proof. It is easy to see that statement (a) is true. Now let p be a prime and $\alpha = \text{ord}_p m \geq 1$. Then for $p \neq 3$ we have

$$\text{ord}_p M_3 \geq -1 + 3\alpha \geq 2\alpha.$$

Let $p = 3$. If $\alpha \geq 2$, then $\text{ord}_3 M_3 \geq -2 + 3\alpha \geq 2\alpha$. Suppose now that $\alpha = 1$; there exists a prime P such that $P \equiv 1 \pmod 3$ and $P \mid m$. Then $3 \mid \phi(m)$; therefore $\text{ord}_3 \frac{1}{3} \binom{t\phi(m)}{i-1} \geq 0$ and $\text{ord}_3 M_3 \geq 3\alpha - 1 = 2\alpha$. The result follows. □

Using Lemma 2.1 we get immediately

Proposition 2.5. *For integers $m \geq 3$ and $t \geq 1$ we have $M_3 \not\equiv 0 \pmod{m^2}$ if and only if $m = 3p_1 \dots p_k$ $(k \geq 0)$, where $p_1, \dots, p_k$ are primes $\equiv 2 \pmod 3$ and $3 \nmid t(t\phi(m) - 1)$.*

If we now use Proposition 2.4 with $t = 2$ and $t = 1$, subtract the corresponding congruences and divide by m, we obtain

Corollary 2.1. *Let $m \geq 3$ be an integer and $\mathrm{ord}_3 m \neq 1$. Then*

$$\epsilon_m \phi(m) W(m) \equiv \prod_{p|m} (1 - p^{2\phi(m)-1}) B_{2\phi(m)} - \prod_{p|m} (1 - p^{\phi(m)-1}) B_{\phi(m)} \pmod m.$$

Remarks. (a) The above congruence can be considered to be the analogue for composite moduli of the congruence

$$w_p \equiv B_{2(p-1)} - B_{p-1} \pmod p$$

for an odd prime p, mentioned by E. Lehmer [10, (25)].

(b) The congruence in Propostion 2.4 for $m = p \geq 5$ (p an odd prime) gives us congruence (24) in the paper [10] of E. Lehmer. (Note that there is a mistake in this paper: for $p = 3$, $t \geq 4$ with $t \equiv 1 \pmod 3$ congruence (24) in [10] does not hold; according to Proposition 2.5 we have $M_3 \not\equiv 0 \pmod{3^2}$).

3. Wilson numbers

As we remarked in the introduction, we have $W(p) \equiv 0 \pmod p$ for $p = 5, 13$ and 563, but no other such "Wilson prime" was found up to 5×10^8. It is now natural to ask which composites m satisfy $W(m) \equiv 0 \pmod m$, $m \geq 4$. We call such numbers "Wilson numbers". The problem is similar to that concerning the Wieferich numbers (see [2]), but it appears to be more difficult. While the Wieferich numbers have been completely characterized in [2], no such characterization was found for the composite Wilson numbers. Moreover, Kloss [8] (1965) lists only one composite Wilson number up to 32 000, namely $5971 = 7 \cdot 853$. Our calculations confirmed this; we extended the search up to 5×10^8 and found 8 new composite Wilson numbers. They are listed in Table 1, following the three known Wilson primes and the number found by Kloss.

The main purpose of this section is to derive a number of congruences for Wilson quotients, some of which will facilitate the search for further composite Wilson numbers.

Now let $p^n m$ be a given modulus, with p a prime and m and n positive integers, $p \nmid m$, $n \geq 2$. We use the fact that $p^n m$ and pm have the same set of prime divisors. Now

$$\begin{aligned} P(p^n m) &= \prod_{k=0}^{p-1} \prod_{\substack{a=1 \\ (a,pm)=1}}^{p^{n-1}m} (kp^{n-1}m + a) \\ &= \left(\prod_{\substack{a=1 \\ (a,pm)=1}}^{p^{n-1}m} a \right) \prod_{k=0}^{p-1} \prod_{\substack{a=1 \\ (a,pm)=1}}^{p^{n-1}m} \left(1 + kp^{n-1}m \frac{1}{a} \right), \end{aligned}$$

Table 1. Wilson numbers $\leq 5 \times 10^8$

Wilson number	Factorization
5	prime
13	prime
563	prime
5971	$7 \cdot 853$
558771	$3 \cdot 19 \cdot 9803$
1964215	$5 \cdot 11 \cdot 71 \cdot 503$
8121909	$3 \cdot 139 \cdot 19477$
12326713	$7 \cdot 1760959$
23025711	$3 \cdot 1867 \cdot 4111$
26921605	$5 \cdot 67 \cdot 80363$
341569806	$2 \cdot 3 \cdot 181 \cdot 409 \cdot 769$
399292158	$2 \cdot 3 \cdot 17 \cdot 97 \cdot 40357$

and therefore

$$P(p^n m) \equiv P(p^{n-1}m)^p \prod_{k=0}^{p-1} \left(1 + kp^{n-1}m \sum_{\substack{a=1 \\ (a,pm)=1}}^{p^{n-1}m} \frac{1}{a} + k^2 p^{2n-2} m^2 {\sum}' \frac{1}{ab} \right) \pmod{p^{2n}m^2), \tag{3.1}$$

where the second sum $\sum'$ ranges over all a, b with $1 \leq a < b \leq p^{n-1}m$ and $(a, pm) = (b, pm) = 1$. Since $P(p^n m)$ has to be evaluated modulo $p^{2n}m^2$, the reciprocals are understood as reciprocals modulo $p^{2n}m^2$. So we may write

$$\frac{1}{a} \equiv a^{\phi(p^{2n}m^2)-1} \pmod{p^{2n}m^2}, \quad (a, pm) = 1.$$

By means of this and the following lemmas we will now evaluate the right-hand side of congruence (3.1).

Lemma 3.1. *If p is a prime and m and n are positive integers with $p \nmid m$ and $n \geq 2$, then*

$$\sum_{\substack{a=1 \\ (a,pm)=1}}^{p^{n-1}m} a^{\phi(p^{2n}m^2)-1} \equiv 0 \pmod{p^{2n-2-\delta}m},$$

where $\delta = 0$ when $p \geq 5$, and $\delta = 1$ for $p = 2$ or 3.

Proof. We use Proposition 2.3 with n and m replaced by $n' = \phi(p^{2n}m^2) - 1$ and $m' = p^{n-1}m$, respectively. Since n' is always odd, the first and third terms on the left-hand side of the congruence in Proposition 2.3 are zero. The second term, divided by $n' + 1 = \phi(p^{2n}m^2)$, is

$$A = \frac{1}{2} n' m'^2 \prod_{\substack{q \mid m' \\ q \text{ prime}}} (1 - q^{n'-2}) B_{n'-1}.$$

First, let $p \geq 5$. Since $n' - 1 \not\equiv 0 \pmod{p-1}$, $B_{n'-1}$ is p-integral by the von Staudt-Clausen Theorem. Hence A is divisible by p^{2n-2}. Also, since $1 - p^{n'-2}$ is even and $m' B_{n'-1}$ is m'-integral, we have $A \equiv 0 \pmod{m}$, which proves the lemma for $p \geq 5$. The same argument holds for $p = 3$, with the difference that $3B_{n'-1}$ is 3-integral, hence we have $\delta = 1$ in this case. We can deal with $p = 2$ in a similar way. Noting that all further terms on the left-hand side in Proposition 2.3 are divisible by $p^{2n-2}m$ (again by the von Staudt-Clausen Theorem), we see that the lemma holds. □

Lemma 3.2. *Let p, m and n be as in Lemma 3.1 and in addition assume that $n \geq 3$ for $p = 2$ and 3, and $m \geq 3$ for $p = 2$. Then*

$$\sum \frac{1}{ab} \equiv 0 \pmod{p},$$

where the summation ranges over all integers a and b with $1 \leq a < b \leq p^{n-1}m$ and $(a, pm) = (b, pm) = 1$.

Proof. If $p = 2$, then all the terms in the sum are odd, and there are $\phi(2^{n-1}m)(\phi(2^{n-1}m) - 1)/2$ of them. But $\phi(2^{n-1}m) = 2^{n-2}\phi(m)$, where $\phi(m)$ is even. So the number of terms is even for $n \geq 3$, which proves the lemma for $p = 2$ and $n \geq 3$.

For $p \geq 3$ we use the identity

$$2\sum \frac{1}{ab} = \left(\sum_{\substack{a=1 \\ (a,pm)=1}}^{p^{n-1}m} \frac{1}{a} \right)^2 - \sum_{\substack{a=1 \\ (a,pm)=1}}^{p^{n-1}m} \frac{1}{a^2}.$$

By Lemma 3.1, the first term on the right-hand side is divisible by p for $n \geq 1$. For the second term we use Proposition 2.3 again, this time with $n' = \phi(p^{2n}m^2) - 2$ and $m' = p^{n-1}m$ replacing n and m, respectively. Then the first term in the equation in Proposition 2.3, divided by $n' + 1$, becomes

$$m' \prod_{\substack{q|m' \\ q \text{ prime}}} (1 - q^{n'-1})B_{n'}.$$

As in the proof of Lemma 3.2 we see that for $p \geq 5$ and $n \geq 2$ this term is divisible by p, while for $p = 3$ that is true only for $n \geq 3$. Finally, we note that all other terms on the left-hand side of the equation in Proposition 2.3 are divisible by p. This completes the proof. □

Proposition 3.1. *Let p be a prime, and m and n positive integers, $p \nmid m$. Then*

$$W(p^n m) \equiv W(p^{n-1}m) \pmod{p^{n-1}m},$$

provided that

$$\begin{cases} n \geq 2 & \text{for } p \geq 5, \\ n \geq 3 & \text{for } p = 3, \\ n \geq 3 & \text{and } m \geq 3 \quad \text{for} \quad p = 2. \end{cases}$$

Proof. By Lemmas 3.1 and 2.2 it is clear that in all three cases the congruence (3.1) reduces to

$$P(p^n m) \equiv P(p^{n-1}m)^p \pmod{p^{2n-1}m^2}.$$

We note that in all the allowable cases we have $\epsilon_{p^nm} = \epsilon_{p^{n-1}m}$; we denote this common value by ϵ. Now with Definition 3.1 we get

$$\begin{aligned} p^nmW(p^nm)+\epsilon &\equiv (p^{n-1}mW(p^{n-1}m)+\epsilon)^p \\ &\equiv \epsilon^p + \epsilon^{p-1}pp^{n-1}mW(p^{n-1}m) \\ &\quad + \epsilon^{p-2}\frac{p(p-1)}{2}p^{2n-2}m^2W(p^{n-1}m)^2 \pmod{p^{2n-1}m^2}). \end{aligned}$$

For $p \geq 3$, this reduces to

$$p^nmW(p^nm) \equiv p^nmW(p^{n-1}m) \pmod{p^{2n-1}m^2},$$

which implies the result. In the case $p = 2$ we have $\epsilon = 1$; hence from the above congruence we obtain

$$W(2^nm) \equiv W(2^{n-1}m) + 2^{n-2}mW(2^{n-1}m)^2 \pmod{2^{n-1}m}. \tag{3.2}$$

We now show that $W(4m)$ is always even for odd $m \geq 3$. Indeed, $P(4m)$ can be written as a product of $\phi(4m)/4$ terms of the form

$$j(2m-j)(2m+j)(4m-j) = 16m^3j - 4mj^2(m+j) + j^4,$$

for odd j with $(m, j) = 1$. Since $m + j$ is even and $j^4 \equiv 1 \pmod 8$ for odd j, each of the terms is $\equiv 1 \pmod 8$ and so is their product, i.e., $P(4m) \equiv 1 \pmod 8$. But then, $W(4m)$ will be even.

Finally, using induction with (3.2), we see that $W(2^nm)$ is even for all $n \geq 2$ and all odd $m \geq 3$. This shows that the second term on the right-hand side of (3.2) vanishes $\pmod{2^{n-1}m}$, which proves the proposition for $p = 2$. □

In the last proof we saw that $W(2^nm)$ is always even for $n \geq 2$ and for odd $m \geq 3$. The following lemma deals with the case $n = 1$.

Lemma 3.3. *Let $m \geq 3$ be an odd integer. Then $W(2m)$ is odd if and only if m is a power of a prime.*

Proof. $P(2m)$ can be written as a product of $\phi(2m)/2$ terms of the form $j(2m-j) = 2mj-j^2$. Since m and j are odd, all these terms are $\equiv 1 \pmod 4$, and so $P(2m) \equiv 1 \pmod 4$. Now, if m is not a prime power, then $\epsilon_{2m} = 1$, and we see that $W(2m)$ will be even. Otherwise, $\epsilon_{2m} = -1$ and $W(2m) = (P(2m)+1)/2m \equiv 1 \pmod 2$. □

The next result deals with some cases not covered by Proposition 3.1.

Proposition 3.2. *The following congruences hold:*

(a) *For integers $n \geq 4$,*

$$W(2^n) \equiv W(2^{n-1}) \pmod{2^{n-2}}.$$

In particular, for all $n \geq 1$,

$$W(2^n) \equiv 1 \pmod 4.$$

(b) *Let $m \geq 3$ be an odd integer. If m is not a power of a prime, then*

$$W(4m) \equiv W(2m) \pmod{2m}.$$

If m is a power of a prime p, then

$$W(4m) \equiv -W(2m) \pmod m$$

and

$$W(4m) \equiv \begin{cases} 0 & \textit{if} \quad p \equiv 1 \textit{ or } 3 \pmod{8}, \\ & \pmod{4} \\ 2 & \textit{if} \quad p \equiv 5 \textit{ or } 7 \pmod{8}. \end{cases}$$

(c) *For integers $m \geq 1$ with $3 \nmid m$,*

$$W(9m) \equiv W(3m) \pmod{m}.$$

If in addition m has a prime factor $q \equiv 1 \pmod{3}$, then

$$W(9m) \equiv W(3m) \pmod{3m}.$$

Proof. (a) We use (3.1) with odd m and $p = 2$. Lemma 3.1 gives, for $n \geq 2$,

$$P(2^n m) \equiv P(2^{n-1}m)^2 \pmod{2^{n-2}m^2}. \tag{3.3}$$

Letting $m = 1$ and noting $\epsilon_{2^n} = \epsilon_{2^{n-1}} = 1$ we can deduce the first congruence. By induction we see $W(2^n) \equiv W(8) \equiv 1 \pmod{4}$ for all $n \geq 3$. Also, $W(4) = W(2) = 1$.

(b) We set $n = 2$ in (3.3) and let $m \geq 3$ be an odd integer. Note that $\epsilon_{2m} = \epsilon_m$, while $\epsilon_{4m} = 1$ always. Hence (3.3) becomes

$$4mW(4m) + 1 \equiv (2mW(2m) + \epsilon_m)^2 \pmod{4m^2},$$

which gives

$$W(4m) \equiv \epsilon_m W(2m) \pmod{m}.$$

If m is a prime or a power of a prime, then $\epsilon_m = -1$ and we immediately get the assertion. Otherwise $\epsilon_m = 1$ and by Lemma 3.3 and the remark preceding it we have $W(4m) \equiv W(2m) \pmod{2}$, which shows the first congruence.

Now suppose that $m = p^n$, where n is a positive integer and p an odd prime. Using Proposition 3.1 we have for $p \geq 5$ and $n \geq 2$,

$$W(4p^n) \equiv W(4p) \pmod{4}$$

and for $p = 3$, $n \geq 3$,

$$W(4 \cdot 3^n) \equiv W(4 \cdot 9) \equiv 0 \pmod{4}.$$

So we may suppose $n = 1$, hence $m = p$. Then

$$\begin{aligned} P(4p) &= \prod_{\substack{j=1 \\ j \text{ even}}}^{p-1} (p-j)(p+j)(3p-j)(3p+j) = \prod_{\substack{j=1 \\ j \text{ even}}}^{p-1} (9p^4 - 10p^2j^2 + j^4) \\ &\equiv \prod_{\substack{j=1 \\ j \text{ even}}}^{p-1} (9 + 6p^2j^2) \pmod{16} \\ &= \prod_{k=1}^{(p-1)/2} (9 + 3 \cdot 8p^2k^2) \equiv \prod_{k=1}^{(p-1)/2} (9 + 3 \cdot 8k^2) \pmod{16}. \end{aligned}$$

If k is odd, then $9 + 3 \cdot 8k^2 \equiv 1 \pmod{16}$ and if k is even, then $9 + 3 \cdot 8k^2 \equiv 9 \pmod{16}$, and the third part of (b) follows.

(c) We use (3.1) with $p = 3$, $p \nmid m$, and $n = 2$. Then by Lemma 3.1,

$$P(9m) \equiv P(3m)^3 \pmod{9m^2}.$$

Note that $\epsilon_{9m} = \epsilon_{3m}$ for all $m \geq 1$. Using this congruence we obtain the first assertion. Finally, if m has a prime factor $q \equiv 1 \pmod 3$, then Lemmas 3.1 and 3.2 can be improved. Indeed, the Euler factor of A in the proof of Lemma 3.1 is now divisible by 3 and therefore Lemma 3.1 holds with $\delta = 0$. Similarly, the appropriate Euler factor in the proof of Lemma 3.2 is divisible by 3. Hence Lemma 3.2 holds for $p = 3$ and $n \geq 2$, and so does Proposition 3.2 in this case. □

Corollary 3.1. (a) *If p^n is a Wilson number, where p is a prime and n a positive integer, then p^r is a Wilson number for all $1 \leq r \leq n$.*

(b) *No prime power p^n, where $n \geq 1$ and $p < 5 \times 10^8$, $p \neq 5$, 13, 563 can be a Wilson number; $5^N, 13^N$ and 563^N are not Wilson numbers for any integer $N \geq 2$.*

(c) *No number of the form $2p^n, n \geq 1$ and p an odd prime, can be a Wilson number.*

Proof. (a) For $p = 2$, this follows from Proposition 3.2 (a). For $p = 3$, we use Proposition 3.1 with $m = 1$ and note that $W(9) \equiv 6 \pmod 9$. For $p \geq 5$ we use again Proposition 3.1.

(b) By direct computation we see that $5^2, 13^2$ and 563^2 are not Wilson numbers. The rest follows from the fact that $W(p) \not\equiv 0 \pmod p$ for $p < 5 \times 10^8$.

(c) This follows directly from Lemma 3.3. □

4. Wilson quotients $W(3m)$ and $W(9m)$

In this section we will refine the results of Proposition 3.2 for certain integers m and consider the question whether $W(3m)$ or $W(9m)$ can be Wilson numbers. Recall that by Proposition 3.1 it is (essentially) sufficient to consider squarefree moduli. Here we will only consider squarefree integers $m \geq 5$ with all prime divisors congruent to 2 modulo 3.

First we need a result which is related to the "inclusion-exclusion principle". It can be proved, e.g., by induction on k.

Lemma 4.1. *Let C be a finite set of nonzero complex numbers, $k \in \mathbb{N}$, and $A_1, \dots, A_k \subseteq C$. Let $K = \{1, 2, \dots, k\}$, and for $X \subseteq K$ put*

$$\alpha(X) = \prod x \ (x \in \bigcap_{i \in X} A_i).$$

Then

$$\prod x (x \in C - \bigcup_{i=1}^{k} A_i) = \prod_{X \subseteq K} \alpha(X)^{(-1)^{|X|}}.$$

Note that as usual $|X|$ denotes the number of elements of the set X, and concerning the empty set $\emptyset$ we let $\prod_{x \in \emptyset} x = 1$ and $\bigcap_{i \in \emptyset} A_i = C$ by convention. We introduce the following notation. For a nonnegative integer h put

$$Q_1(h) = \begin{cases} 2 & \text{if } h \text{ is even} \\ 5 & \text{if } h \text{ is odd} \end{cases} \equiv 2^{(-1)^h} \pmod 9, \quad \text{and } Q_2(h) = -1.$$

Lemma 4.2. *Let h be a nonnegative integer and $p_1, \dots, p_h$ be primes, $p_j \equiv 2 \pmod 3$, $j = 1, \dots, h$. Denote $N = p_1 \cdot \dots \cdot p_h$. Then for $u \in \{1, 2\}$,*

$$\prod_{\substack{1 \le x \le 3^u N \\ 3 \nmid x}} x \equiv Q_u(h)(-1)^\eta \pmod{3^{u+1}},$$

where

$$\eta = \begin{cases} 0 & \text{if } 2 \notin \{p_1, \dots, p_h\}, \\ 1 & \text{if } 2 \in \{p_1, \dots, p_h\}. \end{cases}$$

(If $h = 0$, then $\{p_1, \dots, p_h\} = \emptyset$ by convention, and $N = 1$.)

Proof. We write $N = w + 3U$, where $U \ge 0$ is an integer and $w = 1$ or $w = 2$ (if $h = 0$, $p_1 \cdot \dots \cdot p_h$ is understood to be 1). It is obvious that h is even if and only if $w = 1$. Also, if $2 \notin \{p_1, \dots, p_h\}$, then h is even if and only if U is even; in the case $2 \in \{p_1, \dots, p_h\}$ h is even if and only if U is odd. Now we have

$$\Pi_1 = \prod_{\substack{1 \le x \le 3N \\ 3 \nmid x}} x = 1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \cdot \dots \cdot (9U + 1) D_1(w),$$

where $D_1(w)$ is an integer satisfying

$$D_1(w) \equiv \begin{cases} 2 \\ 2 \cdot 4 \cdot 5 \end{cases} \pmod 9 \qquad \begin{matrix} \text{if } w = 1, \\ \text{if } w = 2, \end{matrix}$$
$$\equiv 2^w \pmod 9,$$

hence

$$\Pi_1 \equiv (-1)^U 2^w \equiv Q_1(h)(-1)^\eta \pmod 9.$$

Similarly

$$\Pi_2 = \prod_{\substack{1 \le x \le 9N \\ 3 \nmid x}} x = (1 \cdot 2 \cdot 4 \cdot 5 \cdot \dots \cdot 26) \cdot \dots \cdot (27U + 1) D_2(w),$$

where the integer $D_2(w)$ satisfies

$$D_2(w) \equiv \begin{cases} 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \\ 2 \cdot 4 \cdot 5 \cdot 7 \cdot \dots \cdot 17 \end{cases} \equiv (-1)^w \pmod{27}.$$

Therefore

$$\Pi_2 \equiv (-1)^U D_2(w) \equiv Q_2(h)(-1)^\eta \pmod{27}. \qquad \square$$

For the remainder of this section we assume that $k \ge 1$ is an integer, $p_1, \dots, p_k$ are different primes, $p_i \equiv 2 \pmod 3$ for each $1 \le i \le k$, $m = p_1 \cdot \dots \cdot p_k$, $K = \{1, 2, \dots, k\}$, and for $X \subseteq K$

$$\pi(X) = \prod_{i \in X} p_i, \qquad \pi(\emptyset) = 1,$$

$$\eta(X) = \begin{cases} 0 & \text{if } 2 \notin \{p_i \colon i \in K - X\}, \\ 1 & \text{if } 2 \in \{p_i \colon i \in K - X\}. \end{cases}$$

Lemma 4.3. *Let $j \in K$ be fixed. Then*

$$\sum_{j\in X\subseteq K} \frac{m}{\pi(X)}(-1)^{|X|} \equiv 2 \pmod 3.$$

Proof. Suppose $j \in K$. Then

$$\sum_{j\in X\subseteq K} \frac{m}{\pi(X)}(-1)^{|X|} = \sum_{Y\subseteq K-\{j\}} \pi(Y)(-1)^{k-|Y|} \equiv -\sum_{r=0}^{k-1} \binom{k-1}{r} 2^r (-1)^{k-1-r}$$
$$= -(2-1)^{k-1} \equiv 2 \pmod 3. \quad \square$$

Lemma 4.4.

$$\sum_{X\subseteq K} \eta(X)(-1)^{|X|} = \begin{cases} 1 & \textit{if } k=1 \textit{ and } p_1 = 2, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. If $2 \notin \{p_i\colon i \in K\}$, then $\eta(X) = 0$ for each $X \subseteq K$. Suppose now that $2 = p_j$ for some $j \in K$. Then

$$\sum_{X\subseteq K} \eta(X)(-1)^{|X|} = \sum_{j\in K-X} (-1)^{|X|} = \sum_{r=0}^{k-1} \binom{k-1}{r} (-1)^r = \begin{cases} 1 & \text{for } k=1, \\ 0 & \text{for } k \geq 2. \end{cases}$$

$\square$

Lemma 4.5.

$$\prod_{X\subseteq K} Q_u(k-|X|)^{(-1)^{|X|}} \equiv \begin{cases} 7 \pmod 9 & \textit{for } u=1, \\ 1 \pmod{27} & \textit{for } u=2. \end{cases}$$

Proof. By definition of the $Q_u(h)$ we have

$$\prod_{X\subseteq K} Q_1(k-|X|)^{(-1)^{|X|}} \equiv 2^{(-1)^k 2^k} \equiv 7 \pmod 9$$

since $(-1)^k 2^k \equiv 4 \pmod 6$, and

$$\prod_{X\subseteq K} Q_2(k-|X|)^{(-1)^{|X|}} = \prod_{X\subseteq K} (-1)^{(-1)^{|X|}} = (-1)^{\sum\limits_{X\subseteq K} (-1)^{|X|}} = 1. \quad \square$$

Theorem 4.1. *Let m, k be integers, $m \geq 5$, $k \geq 1$, $p_1, \dots, p_k$ distinct primes $\equiv 2$ $\pmod 3$, and $m = p_1 \cdot \dots \cdot p_k$. Then*

$$P(3m) \equiv 7p_1^4 \cdot \dots \cdot p_k^4 \pmod 9,$$
$$P(9m) \equiv p_1^{12} \cdot \dots \cdot p_k^{12} \pmod{27}.$$

Proof. Let $u \in \{1, 2\}$, $C^u = \{1 \leq x \leq 3^u m\colon 3 \nmid x\}$, $A_i^u = \{x \in C^u\colon p_i | x\}$ for $i \in K$, $\delta_u = P(3^u m) = \prod x(x \in C^u - \bigcup_{i=1}^k A_i^u)$, $\alpha_u(X) = \prod x(x \in \bigcap_{i\in X} A_i^u)$ for $X \subseteq K$. By Lemma 4.1 we have

$$\delta_u = \prod_{X\subseteq K} \alpha_u(X)^{(-1)^{|X|}}.$$

Suppose $X \subseteq K$. Then $x \in \bigcap_{i\in X} A_i^u$ if and only if there exists an integer y, $1 \le y \le 3^u m/\pi(X)$, $3 \nmid y$, such that $x = \pi(X)y$. Since the number of such y equals $2 \cdot 3^{u-1} m/\pi(X)$, we have by Lemma 4.2

$$\alpha_u(X) \equiv \pi(X)^{2\cdot 3^{u-1} m/\pi(X)} Q_u(k - |X|)(-1)^{\eta(X)} \pmod{3^{u+1}}.$$

Using Lemma 4.3 we get

$$\prod_{X\subseteq K} \pi(X)^{(2\cdot 3^{u-1} m/\pi(X))(-1)^{|X|}} \equiv \pi(K)^{4\cdot 3^{u-1}} \pmod{3^{u+1}}.$$

Lemmas 4.4 and 4.5 now complete the proof. □

Corollary 4.1. *Let* $a = \#\{1 \le i \le k\colon\ p_i \equiv 2 \pmod 9\}$, $b = \#\{1 \le i \le k\colon\ p_i \equiv 5 \pmod 9\}$. *Then*

$$P(3m) \equiv 7^{a+1}4^b \pmod 9,$$
$$P(9m) \equiv 19^a 10^b \pmod{27}.$$

From this we will determine $W(3m)$ and $W(9m) \pmod 3$. Since $7^2 \equiv 4 \pmod 9$, $7^3 \equiv 1 \pmod 9$ and $10^2 \equiv 19 \pmod{27}$, $10^3 \equiv 1 \pmod{27}$, the values $P(3m) \pmod 9$ and $P(9m) \pmod{27}$ depend on the values of a and $b \mod 3$. In fact, we have

$P(3m) \equiv 7 \pmod 9, P(9m) \equiv 1 \pmod{27}$ when $b \equiv a \pmod 3$,
$P(3m) \equiv 1 \pmod 9, P(9m) \equiv 10 \pmod{27}$ when $b \equiv a+1 \pmod 3$,
$P(3m) \equiv 4 \pmod 9, P(9m) \equiv 19 \pmod{27}$ when $b \equiv a+2 \pmod 3$.

Now since $mW(3m) = \big(P(3m)-1\big)/3$ and $mW(9m) = \big(P(9m)-1\big)/9$, we have

$mW(3m) \equiv 2 \pmod 3, mW(9m) \equiv 0 \pmod 3$ when $b \equiv a \pmod 3$,
$mW(3m) \equiv 0 \pmod 3, mW(9m) \equiv 1 \pmod 3$ when $b \equiv a+1 \pmod 3$,
$mW(3m) \equiv 1 \pmod 3, mW(9m) \equiv 2 \pmod 3$ when $b \equiv a+2 \pmod 3$.

With this last list, and observing that $W(6) = 1$, $W(18) = 4727 \equiv 2 \pmod 3$, we get

Theorem 4.2. *Let $m \ge 2$ be a squarefree integer with all prime factors congruent to* $2 \pmod 3$*, and a and b be as in Corollary 4.1. Then*

(a) $W(3m) \not\equiv W(9m) \pmod 3$. *In particular, $3m$ and $9m$ cannot be simultaneously Wilson numbers.*
(b) $W(3m)$*, with $b \equiv a$ or $b \equiv a+2$* $\pmod 3$*, is never a Wilson number.*
(c) $W(9m)$*, with $b \equiv a+1$ or $b \equiv a+2$* $\pmod 3$*, is never a Wilson number.*

Finally in this section, we determine $W(9p) \pmod 9$, where p is a prime, $p \equiv 2 \pmod 3$. In fact, since we are interested in finding Wilson numbers, we may restrict our attention to $p \equiv 8 \pmod 9$ (since necessarily $a = b = 0$; see Theorem 4.2 (c)) or, which amounts to the same, $p \equiv -1 \pmod{18}$.

Theorem 4.3. *Let p be a prime, $p \equiv -1$* $\pmod{18}$*. Then*

$$W(9p) \equiv \begin{cases} 0 \pmod 9 & \textit{if } p \equiv 35 \pmod{54}, \\ 3 \pmod 9 & \textit{if } p \equiv 17 \pmod{54}, \\ 6 \pmod 9 & \textit{if } p \equiv -1 \pmod{54}. \end{cases}$$

Proof. We have, with $J := 3j+1$,

$$\begin{aligned} P(9p) &= \prod_{\substack{j=1\\(j,3p)=1}}^{3p-1} j(3p+j)(6p+j)\\ &= \prod_{j=0}^{p-1}{}' J(3p-J)(3p+J)(6p-J)(6p+J)(9p-J)\\ &= \prod_{j=0}^{p-1}{}' \bigl\{[9pJ-J^2][9p^2-J^2][36p^2-J^2]\bigr\}, \end{aligned}$$

where $\prod'$ indicates that the term belonging to $j=(2p-1)/3$ is omitted from the product. We now expand the last expression and use the facts that $p\equiv -1 \pmod 9$ and $27j^3\equiv 27j \pmod{81}$. Then

$$\begin{aligned} P(9p) &\equiv \prod_{j=0}^{p-1}{}' \bigl\{45(3j+1)^4-9(3j+1)^5-(3j+1)^6\bigr\}\\ &\equiv \prod_{j=0}^{p-1}{}' \bigl\{35+9j+27j^2\bigr\} \pmod{81}. \end{aligned}$$

The complete product (i.e., including the term for $j=(2p-1)/3$) is congruent to

$$\begin{aligned} &35^p+35^{p-1}\bigl[9\frac{(p-1)p}{2}+27\frac{(p-1)p(2p-1)}{6}\bigr]\\ &\quad= 35^p+35^{p-1}9(p-1)p^2\\ &\quad\equiv 35^{p-1}(35-18)=17\cdot 35^{p-1} \pmod{81} \end{aligned}$$

since $p\equiv -1 \pmod 9$. Now since $35^{18}\equiv 1 \pmod{81}$, we obtain in all three cases $35^{p-1}\equiv 35^{16}\equiv -8 \pmod{81}$, thus the product is congruent to $-8\cdot 17\equiv 26 \pmod{81}$. Next we consider the omitted term for $j=(2p-1)/3$ which turns out to be $35-6p+12p^2\equiv 26$, -1, or $53 \pmod{81}$ for $p\equiv 8$, -10, or $-1 \pmod{27}$, respectively. Hence

$$P(9p)\equiv\begin{cases} 26/26\equiv 1 \pmod{81} & \text{for } p\equiv 8 \pmod{27},\\ 26/(-1)\equiv 55 \pmod{81} & \text{for } p\equiv -10 \pmod{27},\\ 26/53\equiv 28 \pmod{81} & \text{for } p\equiv -1 \pmod{27}. \end{cases}$$

With $W(9p)=\bigl(P(9p)-1\bigr)/9p\equiv\bigl(P(9p)-1\bigr)/(-9) \pmod 9$ we finally obtain the assertion. □

An immediate consequence of the last two theorems is the following

Corollary 4.2. *Let p be a prime, $p\equiv 2 \pmod 3$. Then a necessary condition for $9p$ to be a Wilson number is that $p\equiv 35 \pmod{54}$.*

5. Some congruences involving Fermat quotients

Proposition 2.1. exhibits a close connection between the generalized Wilson quotients and the Euler quotients (which are in fact generalized Fermat quotients) modulo composite integers m. In this section we will derive congruences connecting

$W(m)$ with Fermat quotients of prime moduli, and derive some easy consequences. These proved to be particularly helpful in the search for Wilson numbers.

Theorem 5.1. *Let p be an odd prime and $m > 2$ an integer not divisible by p. Then*

$$-mW(pm) \equiv W(p)\phi(m) + \sum_{r|m} q_p(r)\frac{\phi(m)}{r-1} \pmod{p}, \tag{5.1}$$

where the sum is taken over all primes r that divide m.

Proof. Let $f(p,n)$ denote the product of all integers between 1 and pn that are not divisible by p. Then for $d \mid m$, the product of the integers between 1 and pm that are divisible by d and relatively prime to p is $f(p,m/d)d^{(p-1)m/d}$. Hence Lemma 4.1 gives

$$P(pm) = \prod_{d|m}(f(p,m/d)d^{(p-1)m/d})^{\mu(d)}. \tag{5.2}$$

First we note that $f(p,n) \equiv P(p)^n \pmod{p^2}$; this follows from an argument similar to that around (3.1). Therefore

$$\prod_{d|m} f(p,m/d)^{\mu(d)} \equiv \prod_{d|m} P(p)^{\mu(d)m/d} = P(p)^{\phi(m)} \pmod{p^2}, \tag{5.3}$$

by a well-known relation between the functions $\mu(n)$ and $\phi(n)$. Next we use the identity

$$\prod_{d|m} d^{\mu(d)m/d} = \prod_{r|m} r^{-\phi(m)/(r-1)}, \tag{5.4}$$

where the right-hand product is taken over all primes r dividing m. To show this, we fix a prime divisor r of m and write $m = r^\alpha m'$, with $(m',r) = 1$. Let N be the highest power of r dividing the left-hand side of (5.4). Since $\mu(d) = 0$ when $r^2 \mid d$, we have

$$\begin{aligned} N = \sum_{\substack{d|m\\ r|d}} \mu(d)\frac{m}{d} &= \sum_{d|m} \mu(d)\frac{m}{d} - \sum_{\substack{d|m\\ r\nmid d}} \mu(d)\frac{m}{d} \\ &= \phi(m) - r^\alpha \sum_{d|m'} \mu(d)\frac{m'}{d} \\ &= \phi(m) - r^\alpha\phi(m') = \phi(m)\frac{-1}{r-1}, \end{aligned}$$

where the last equality follows from the basic properties of the ϕ-function. This proves (5.4).

Now, (5.2)–(5.4) and the definitions of the Wilson and Fermat quotients give

$$P(pm) \equiv (-1+pW(p))^{\phi(m)} \prod_{r|m}(1+pq_p(r))^{-\phi(m)/(r-1)} \pmod{p^2}.$$

Using the fact that $(1+pq_p(r))^{-1} \equiv 1 - pq_p(r) \pmod{p^2}$, we get

$$\begin{aligned} P(pm) &\equiv (1 - pW(p)\phi(m)) \prod_{r|m} \left(1 - pq_p(r)\frac{\phi(m)}{r-1}\right) \\ &\equiv 1 - pW(p)\phi(m) - p\sum_{r|m} q_p(r)\frac{\phi(m)}{r-1} \pmod{p^2}. \end{aligned}$$

Subtracting 1 and dividing by $-p$, we obtain (5.1). □

The following immediate consequences will be useful in the search for Wilson numbers.

Corollary 5.1. *Let p and r be two distinct odd primes. Then*

(a) $-rW(pr) \equiv (r-1)W(p) + q_p(r) \pmod{p}$*;*
(b) $-2W(4p) \equiv W(p) + q_p(2) \pmod{p}$*;*
(c) $-3W(9p) \equiv 2W(p) + q_p(3) \pmod{p}$ $(p \neq 3)$.

Corollary 5.2. (a) *Let $p \equiv 1$ or $3 \pmod{8}$. Then $4p$ is a Wilson number if and only if $q_p(2) + W(p) \equiv 0 \pmod{p}$.*
(b) *Let $p \equiv 35 \pmod{54}$. Then $9p$ is a Wilson number if and only if $q_p(3) + 2W(p) \equiv 0 \pmod{p}$.*

Proof. By Corollary 5.1, the "only if" is clear in both cases. On the other hand, $W(4p) \equiv 0 \pmod{4}$ by Proposition 3.2(b) and $W(9p) \equiv 0 \pmod{9}$ by Theorem 4.3. This, combined with Corollary 5.1, proves the other direction in both cases. □

Corollary 5.3. *Let p, r, and s be distinct primes, $p > 2$. Then*

$$-rsW(prs) \equiv (r-1)(s-1)W(p) + (s-1)q_p(r) + (r-1)q_p(s) \pmod{p}.$$

6. Remarks on computation

In this last section we will make some remarks concerning computations or, to be more specific, the search for further composite Wilson numbers. First we summarize relevant results from Sections 3 and 4.

If $2 \nmid m$ and $3 \nmid m$, then by Proposition 3.1 we know that if m is a Wilson number, then the product m' of all distinct prime factors of m is also a Wilson number. Hence it suffices to consider squarefree numbers of this kind. By Corollary 3.1(b) we need not consider primes if $m \leq 5 \times 10^8$.

If $2 \mid m$ and m has two or more distinct odd prime divisors, then by Proposition 3.2(b) and Proposition 3.1 it suffices again to consider the product m' of all distinct prime factors of m.

If $2 \mid m$ and m has exactly one other prime factor, then by Corollary 3.1(c) and Proposition 3.1 we may restrict our attention to $m = 4p$, $p \geq 5$. (Note that by Proposition 3.1 the cases $m = 4 \cdot 3$ and $m = 4 \cdot 3^2$ need to be considered separately; but $W(12) \equiv -4 \pmod{12}$ and $W(36) \equiv 16 \pmod{36}$). Now by Proposition 3.2(b), $W(4p) \equiv 2 \pmod{4}$ if $p \equiv 5$ or $7 \pmod{8}$; hence we may restrict our attention to the case $m = 4p$ with $p \equiv 1$ or $3 \pmod{8}$.

If $3 \mid m$ and m has a prime factor $q \equiv 1 \pmod{3}$, then by Proposition 3.2(c) (2nd part) and Proposition 3.1 it suffices again to consider the squarefree number m', the product of all distinct prime divisors of m.

If $3 \mid m$ and all other prime factors of m are $\equiv 2 \pmod{3}$, then in addition to the squarefree number of the preceding paragraph we must consider the number $9m''$, where m'' is the product of all the other prime factors. But by Theorem 4.2 we may restrict our attention to the cases where the number of prime divisors $\equiv 2 \pmod 9$ of m'' is congruent (modulo 3) to the number of prime divisors $\equiv 5 \pmod 9$ of m'':

In summary, we need only check the following numbers m:

- squarefree numbers with two or more prime factors.
- numbers of the form $4p$, where $p \geq 11$ is a prime, $p \equiv 1$ or $3 \pmod 8$.
- numbers of the form $9m''$, where the prime factors of m'' are all $\equiv 2 \pmod 3$ and the number of prime divisors $\equiv 2 \pmod 9$ is congruent $\pmod 3$ to the number of prime divisors $\equiv 5 \pmod 9$.

In the actual search, we found it advantageous to do the following separate calculations.

1. All squarefree integers with at least two different prime factors, excluding integers of the form $2p$ (which can never be a Wilson number), $3p, 5p, 7p$, as well as $6p, 10p$, and $14p$, where p is a prime.

The given squarefree number n is factored, and then the right-hand side of (5.1) is evaluated, where the smallest odd prime factor of n is used as initial p. If this expression is $\not\equiv 0 \pmod p$, n cannot be a Wilson number. However, if it is divisible by p, then the next larger prime factor of n is used as new p, and so on, until the expression in question is $\not\equiv 0 \pmod p$. If it is divisible by p for all odd prime factors p of n, then n has to be a Wilson number (recall that $W(2m) \equiv 0 \pmod 2$ whenever m is composite).

Since the Wilson quotient $W(p)$ is the most expensive part to compute, all values of $W(p) \pmod p$ for $p < 10^5$ were stored for easy look-up, while for $p > 10^5$, $W(p) \pmod p$ was computed using a program made available to us by Richard Crandall who had also developed the underlying algorithm; for detailed descriptions, see [3] or [4],

2. Numbers of the form $9m''$, with m'' as defined earlier in this section. Excluded from this calculation were those m'' that are of the form p and $2p$ (p prime). The mechanics of the calculation are similar to part 1.

3. All the remaining cases, namely numbers of the form $3p, 4p, 5p, 6p, 7p, 9p, 10p, 14p$, and $18p$, for primes p, were treated separately from cases 1 and 2. Here, $W(p)$ was computed only once and the value was used for all these cases, as described below.

(a) First we consider the cases rp, with $r \in \{3, 5, 7\}$. We use Corollary 5.1(a) with the roles of r and p interchanged, and we observe that $W(3) = 1$, $W(5) = 0$, and $W(7) \equiv 5 \pmod 7$. Also, $q_r(p) \pmod r$ depends on $p \pmod{r^2}$ and is easily computed. (It is also easy to see that $q_r(p) \pmod r$ takes on each of the values $0, 1, \ldots, r-1$ exactly $r-1$ times as p traverses a reduced residue system modulo r^2. This follows, e.g., from the congruence

$$q_r(ar+b) \equiv q_r(b) - \frac{a}{b} \pmod r,$$

where $p = ar + b$, $1 \leq b \leq r-1$; see [9]). This leaves $r-1$ residue classes modulo r^2 for p to be checked, namely those for which $W(pr) \equiv 0 \pmod r$. These are recorded in Table 2, along with the right-hand side of the corresponding congruence of Corollary 5.1(a).

TABLE 2. Small multiples of large primes

n	$p \equiv$	to compute $\pmod{p}$
$3p$	$1,\ 5 \pmod{9}$	$2W(p) + q_p(3)$
$4p$	$1,\ 3 \pmod{8}$	$W(p) + q_p(2)$
$5p$	$1,\ 7,\ 18,\ 24 \pmod{25}$	$4W(p) + q_p(5)$
$6p$	$1,\ 2 \pmod{9}$	$2W(p) + 2q_p(2) + q_p(3)$
$7p$	$1,\ 2,\ 20,\ 33,\ 45,\ 46 \pmod{49}$	$6W(p) + q_p(7)$
$9p$	$8 \pmod{27}$	$2W(p) + q_p(3)$
$10p$	$1,\ 4,\ 8,\ 12 \pmod{25}$	$4W(p) + 4q_p(2) + q_p(5)$
$14p$	$1,\ 18,\ 19,\ 30,\ 31,\ 48 \pmod{49}$	$6W(p) + 6q_p(2) + q_p(7)$
$18p$	$5 \pmod{9}$	$2W(p) + 2q_p(2) + q_p(3)$

(b) The cases $2rp$, with $r \in \{3, 5, 7\}$ are treated similarly. Corollary 5.3 with $s = 2$ and with the roles of p and r reversed gives

$$-2pW(2rp) \equiv (p-1)\,(W(r) + q_r(2)) + q_r(p) \pmod{r}. \tag{6.1}$$

We note that $q_3(2) = 1$, $q_5(2) = 3$, and $q_7(2) \equiv 2 \pmod{7}$, and we record in Table 2 the residue classes for $p \pmod{r^2}$ for which (6.1) is $\equiv 0 \pmod{r}$, along with the corresponding right-hand side of the congruence in Corollary 5.3.

(c) The cases $4p$ and $9p$. These are dealt with in Corollary 5.2; they are also summarized in Table 2.

(d) Finally we note that by Theorem 4.2(c), $18p$ cannot be a Wilson number unless $p \equiv 5 \pmod{9}$. Also, Theorem 5.1 gives

$$-6W(18p) \equiv 2W(p) + 2q_p(2) + q_p(3) \pmod{p};$$

this provides the last entry of Table 2.

For each prime p occurring in the second column of Table 2, the expressions in the third column of Table 2 were computed. We actually recorded all those cases for which the expressions were less than 1000 in absolute value, in order to get some output and opportunities to check the calculations.

As rp reached 5×10^8 (for $r \in \{3, 4, 5, 6, 7, 9, 10, 14, 18\}$), the corresponding rows in Table 2 were removed from consideration, until for $10^8 < p < 1.25 \times 10^8$, $W(p)$ needs to be computed only for $p \equiv 1, 3 \pmod{8}$ and $p \equiv 1, 5 \pmod{9}$, and for $1.25 \times 10^8 < p < 5/3 \times 10^8$ we need $W(p)$ only for $p \equiv 1, 5 \pmod{9}$.

The computations were done at Dalhousie University on a network of 8–10 SPARCstations of varying speeds. Cases 1 and 2 were quickly dealt with: One processor was able to search an interval of length approximately 13 million (near 5×10^8) in 24 hours. Case 3, however, was substantially slower, due to the necessity of computing $W(p)$ for rather large primes p; near 10^8, the fastest machine took 24 hours to search through the relevant primes in an interval of length approximately 460,000.

To conclude, we mention that a rough heuristic argument suggests that the expected number of Wilson numbers below a given limit N should be approximately $(6/\pi^2)\log N$. Thus, for $N = 5 \times 10^8$ we get 12.18, while exactly 12 Wilson numbers (including the 3 Wilson primes) have been found. This argument is based on the unproven assumption that the values of $W(m)$ are uniformly distributed modulo m, and on the well-known fact that the proportion of square-free numbers among all positive integers is asymptotically $6/\pi^2$.

Acknowledgments

We wish to thank Richard E. Crandall for his generous help with this project. We also thank the referee of an earlier version of this paper for suggesting and proving Theorem 5.1 which vastly increased the range of our search.

Most of this paper was prepared while the second and third authors were visiting the Science University of Tokyo in Noda, Chiba, Japan, in the Spring of 1994. They wish to thank the Department of Mathematics for the support and hospitality received.

References

1. T. Agoh, *On Bernoulli and Euler numbers*, Manuscripta Math. **61** (1988), 1–10. MR **89i:**11030
2. T. Agoh, K. Dilcher, and L. Skula, *Fermat quotients for composite moduli*, J. Number Theory **66** (1997), 29–50.
3. R. E. Crandall, *Topics in Advanced Scientific Computation*, TELOS/Springer-Verlag, Santa Clara, CA, 1996. MR **97g:**65005
4. R. E. Crandall, K. Dilcher and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433–449. MR **97c:**11004
5. L. E. Dickson, *History of the Theory of Numbers*, vol. 1, Divisibility and Primality, Chelsea Pub. Company, New York, N.Y., 1966. MR **39:**6807a
6. H. Dubner, *Searching for Wilson primes*, J. Recreational Math. **21** (1989), 19–20.
7. R. H. Gonter and E. G. Kundert, *All prime numbers up to 18,876,041 have been tested without finding a new Wilson prime*, Preprint (1994).
8. K. E. Kloss, *Some number theoretic calculations*, J. Res. Nat. Bureau of Stand., B, **69** (1965), 335-339. MR **32:**7473
9. M. Lerch, *Zur Theorie des Fermatschen Quotienten* $\frac{a^{p-1}-1}{p} = q(a)$, Math. Annalen **60** (1905), 471–490.
10. E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. **39** (1938), 350–360.
11. P. Ribenboim, *The Book of Prime Number Records*, Springer-Verlag, New York, 1988. MR **89e:**11052
12. P. Ribenboim, *The Little Book of Big Primes*, Springer-Verlag, New York, 1991. MR **92i:**11008

Department of Mathematics, Science University of Tokyo, Noda, Chiba 278, Japan
E-mail address: agoh@ma.noda.sut.ac.jp

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada
E-mail address: dilcher@mscs.dal.ca

Department of Mathematics, Faculty of Science, Masaryk University, 66295 Brno, Czech Republic
E-mail address: skula@math.muni.cz