Arithmetic Functions Related to the Arithmetic-Geometric Mean Ratio

Yasutoshi NOMURA
Department of Applied Science,
Faculty of Science,
Okayama University of Science,
Ridai-cho 1-1, Okayama 700-0005, Japan
(Received October 5, 1998)

1. Introduction and the function m (n)

It is well-known that the arithmetic mean of positive reals is not less than the geometric mean of them, the equality holding if and only if they are equal. Thus it will be interesting to ask for what n positive integers $x_1, x_2, \cdots, x_n$, $n > 1$, the **arithmetic-geometric mean quotient** $Q_n(x_1, \cdots, x_n) = (x_1^n + x_2^n + \cdots + x_n^n)/nx_1 x_2 \cdots x_n$ is an integer greater than 1. In other words, we look for positive integer solution $(x_1, \cdots, x_n, d)$ of the diophantine equation

$$x_1^n + \cdots + x_n^n = dnx_1 \cdots x_n \tag{1}$$

where $d > 1$. For convenience we call an n-tuple $x_1, \cdots, x_n$ **trivial** if $x_1 = \cdots = x_n$.

Note that the equation (1) can always be solvable in integers, since we have solutions

$$(x_1, x_2, x_3, \cdots, x_n) = (n, 1, -1, \cdots, 1, -1) \quad \text{for } n \equiv 1 \bmod 4$$
$$(x_1, x_2, x_3, \cdots, x_n) = (n, n, n, 1, -1, \cdots, 1, -1) \text{ for } n \equiv 3 \bmod 4$$

It seems to be difficult to solve (1) in general because there are too many ways of partitioning a given positive integer into positive integers. Hence we are mainly concerned with the case where almost all x's are equal to 1, that is, with the equation

$$x_1^n + \cdots + x_k^n + n - k = dnx_1 \cdots x_k,\ d > 1 \tag{2}$$

for small value k. We denote any solution of (2) by $x_1, \cdots, x_k, 1^{n-k}$.

It is shown in [4, 5] that the equation (1) are always solvable in the following cases:

i) n is even $\geqq 4$ with solution $n-1, 1^{n-1}$

ii) n is a prime congruent to 5 mod 6 with solution $n-1,\ n^2 - 3n + 3,\ 1^{n-2}$

but that (1) is insoluble for $n = 2$.

With these facts and the numerical evidence described later I dare to make the following **conjecture**:

"The equation (1) has a positive integral solution for n greater than 2."

It is also interesting to find the minimum value of d for which the equation (1) is solvable. Thus we set

$$\mathbf{m}\ (n) = \begin{cases} \infty & \text{if (1) is insolvable} \\ \min \{Q_n\ (x_1, \cdots, x_n) \colon (x_1, \cdots, x_n) \text{ is non-trivial}\} & \text{otherwise} \end{cases}$$

The following facts are sometimes helpful in the machine-search of solutions of (1).

Proposition 1.1. *Let* $x_1, \cdots, x_n$ *be an integer-solution of* (1). *Then*

1) *for* $n \equiv 1 \pmod{p-1}$ *with an odd prime* p *dividing* n *one has*

$$x_1 + \cdots + x_n \equiv 0 \pmod{p}$$

2) *for* n *even we have* $x_1 + \cdots + x_n \equiv 0 \pmod{2}$

Proof. We see from the little Fermat theorem that $x^{p-1} \equiv 1 \pmod{p}$ for x relatively prime to p, hence if n is written as $(p-1)\ q+1$

$$x^n = (x^{p-1})^q\ x \equiv x \pmod{p}.$$

Therefore, since $x^n \equiv x \pmod{p}$ in case x is divisible by p, it follows from $x_1{}^n + \cdots + x_n{}^n \equiv 0 \pmod{n}$ that $x_1 + \cdots + x_n \equiv 0 \pmod{p}$. The second claim follows from the fact that x and x^n are of the same parity.

Corollary 1.2. *Let* n *be an odd prime. Then* $x_1 + \cdots + x_n \equiv 0 \pmod{n}$.

The following proposition is proved by Sumner and Dove (see [2]):

Proposition 1.3. *Let* n *be an odd prime power* p^k. *Then the equation* (1) *has a solution* $(p^{k-1}+p^{k-2}+ \cdots +p+1, 1^{n-1})$.

Lemma 1.4. *Let* m, n *and* $p_1, \cdots, p_k$ *be positive integers. Then any solution* $(p_1{}^m, \cdots, p_k{}^m, 1^{n-k})$ *of the equation* (2) *yields a solution* $(p_1, \cdots, p_1, \cdots, p_k, \cdots, p_k, 1^{mn-mk})$ *of the equation* (1) *with* n *replaced by* mn.

Proof. This follows from the observation that $\{m\ (p_1{}^{mn} + \cdots + p_k{}^{mn}) + mn - mk\}/(mnp_1{}^m \cdots p_k{}^m)$ is reduced to $\{(p_1{}^m)^n + \cdots + (p_k{}^m)^n + n - k\}/(np_1{}^m \cdots p_k{}^m)$.

Corollary 1.5. *For* $n = m\ (p^m+1)$ *where* p *is an odd integer* $\geqq 3$, *the equation* (1) *has a solution* $(\underbrace{p, p, \cdots, p}_{m}, 1^{n-m})$.

Proof. Since p^m+1 is even, we see from i) that $(p^m, 1^{n-1})$ is a solution of (1) with $n = p^m+1$, thereby the above assertion.

Proposition 1.6. *For* $n = m^2$ *the equation* (1) *has a solution* $(m+1, 1^{n-1})$.

Proof. This follows from the fact that

$$(m+1)^n + n - 1 = m^3 + \sum_{k \geqq 2} {}_nC_k\ m^k + m^2$$

is divisible by $m+1$ and m^2 which are relatively prime.

Proposition 1.7. *For* $n = k\ (m^k-1)^2$ *where* $m, k \geqq 2$, *the equation* (1) *has a solution* $(m,$

$\cdots, m, 1^{n-k})$.

Proof. The number

$$K = km^n + n - k = km^n + k\ (m^{2k} - 2m^k)$$

is clearly divisible by m^k. Setting $t = m^k - 1$ we have, by the binomial theorem,

$$\begin{aligned} K/(km^k) &= m^{n-k} + m^k - 2 \\ &= m^{km^k(t-1)} + t - 1 \\ &= (t+1)^{m^k(t-1)} + t - 1 \\ &\equiv 1 + m^k\ (t-1)\ t + t - 1 = t^3 \equiv 0\ (\bmod t^2), \end{aligned}$$

which shows that K is divisible by $nm^k = km^k t^2$.

Proposition 1.8. *For* $n = 1 + m + m^2 + \cdots + m^{s-1}$ *where* $n \equiv 0 \bmod s$ (*e. g.* $m \equiv 1 \bmod s$ *or* $m \equiv -1 \bmod s$ *for even* s) *the equation* (1) *has a solution* $(m, 1^{n-1})$.

Proof. We have

$$(m^n + n - 1)/(nm) = (m^{n-1} + 1 + m + \cdots + m^{s-2})/n.$$

Since $n \equiv 0 \bmod s$, it follows that

$$\begin{aligned} m^{n-1} + 1 + m + \cdots m^{s-2} &\equiv m^{n-1} - m^{s-1} \\ &\equiv m^{n-1} - (-m - \cdots - m^{s-1})\ m^{s-1} \\ &\equiv m^s\ (m^{n-1-s} + 1 + m + \cdots + m^{s-2}) \bmod n \end{aligned}$$

which is, by an inductive argument,

$$\equiv m^{ks}\ (m^{s-1} + 1 + \cdots + m^{s-2}) \equiv 0 \bmod n.$$

Corollay 1.9. *For* $n = m^3 + m^2 + m + 1$ *where* m *is odd, the equation* (1) *has a solution* $(m, 1^{n-1})$.

Lemma 1.10. *If* $a^m \equiv 1 \bmod m$ *then* $a^q \equiv 1 \bmod q$ *with* $q = m^k$.

Proof. Observe from the assumption that the assertion is true for $k = 1$.

We shall prove the assertion by the induction on k and assume that the assertion holds for k, that is, $a^{m^k} - 1 \equiv 0 \bmod m^k$. Then, in the expression

$$a^{m^{k+1}} - 1 = (a^{m^k} - 1)\ ((a^{m^k})^{m-1} + \cdots + a^{m^k} + 1),$$

we have

$$a^{m^k} - 1 \equiv 0 \bmod m^k \text{ and } (a^{m^k})^{m-1} + \cdots + a^{m^k} + 1 \equiv 0 \bmod m,$$

which shows that the left hand side is divisible by m^{k+1}.

Corollary 1.11. *If* $m \equiv 1 \bmod a$ *and* $a^m \equiv 1 \bmod m$ *then the equation* (1) *has a solution* $(a, 1^{n-1})$ *for* $n = m^k$.

Proof. Observe that a and m are relatively prime and we see that $a^n + n - 1$ is divisible by a and m^k hence by an.

Proposition 1.12. *For positive integers a and m, $(a+1)^q \equiv 1 \bmod q = a^{2m}$.*

Proof. We prove this by induction on m. Since $(a+1)^{a^2} \equiv 1+a^3 \bmod a^2$ by the binomial theorem, the case $m=1$ is valid. Assuming the case $m=k$, that is, $(a+1)^{a^{2k}} = 1+qa^{2k}$ for some integer q, the binomial theorem implies that

$$\begin{aligned}(a+1)^{a^{2k+2}} &= (1+q\ a^{2k})^{a^2}\\ &\equiv 1+a^2q\ a^{2k} \equiv 1 \bmod a^{2k+2}\end{aligned}$$

which concludes the induction process.

Corollary 1.13. *For $n = a^{2m}$, $m = 1, 2, \cdots$, $(a+1, 1^{n-1})$ is a solution of the equation* (1).

2. The function ε (N)

There may be two methods for solving sequentially the equation (1). One is to seek solutions $x_1, \cdots, x_n$ among partitions $N = x_1 + \cdots + x_n$ and the other is to search factorizations $N = x_1 \cdots x_n$ for solutions of (1). The former has a defect in a rapid increase of the partition number of N as N becomes large, while the second might be executable for large N. The second method suggests the following definition:

For a positive integer N (>2) we define ε (N) to be the least positive integer p for which there exists a factorization $N = x_1 \cdots x_m$, $2 \leqq x_1 \leqq \cdots \leqq x_m$, such that Q_p $(x_1, \cdots, x_m, 1, \cdots, 1)$ is an integer greater than 1.

Following Nagell [3] we introduce the numerical function ψ (n) for a positive integer n as follows:

i) for $n = 1, 2, 4$ or p^a with odd prime p let ψ $(n) = \phi$ (n), the Euler function

ii) for $n = 2^\beta$ where $\beta \geqq 3$, ψ $(n) = \frac{1}{2}$ ϕ (n)

iii) for $n = p_1{}^{a1}$ $p_2{}^{a2} \cdots$ where $p_1, p_2, \cdots$ are distinct primes

$$\psi\ (n) = \mathrm{lcm}\ \{\psi\ (p_1{}^{a1}),\ \psi\ (p_2{}^{a2}),\ \cdots\}$$

Then, if $n > 1$ and a is relatively prime to n, then

$$a^{\psi(n)} \equiv 1 \pmod n$$

Let $(Z/nZ)^\times$ denote the multiplicative group of reduced residue classes modulo n, $n > 1$ and, for an integer a prime to n, let ord (a, n) denote the order of a in $(Z/nZ)^\times$. Thus ord $(a, n) = 1$ means $a \equiv 1 \pmod n$. We have

1) if gcd $(m, n) = 1$ then ord $(a, mn) = $ l c m {ord (a, m), ord (a, n)}

2) for a prime p ord $(a, p^k) = p^{k-1}$ ord (a, p)

3) for a prime $p > 3$ $2^{3p} \equiv 8 \pmod{3p}$, for we have $(2^3)^p = 8^p \equiv 8 \pmod p$ and $(2^p)^3 \equiv 2^p \equiv (-1)^p \equiv -1 \pmod 3$, thereby obtaining $2^{3p} - 8 \equiv 0 \pmod{3p}$

4) $2^n \equiv 2 \pmod p$ for $n = p^a$ with odd prime p, for we have

$$2^n = (2^{p^{a-1}})^p \equiv 2^{p^{a-1}} \equiv 2 \pmod p$$

by the Fermat theorem.

Lemma 2.1. *For any odd $n > 1$ we have $2^n \not\equiv 1 \bmod n$.*

Proof. Let

$$n = p_1^{a_1} \cdots p_k^{a_k}$$

be the prime power factorization of n and assume that there exists p_t such that $s = \operatorname{ord}(2, p_t)$ is even. Then write $n = p_t^{a_t} q$ and $q = us+r$ where $0 \leqq r < s$. Since q is odd, it follows that $r > 0$ and

$$2^n \equiv (2^{p_t})^q \equiv 2^q = (2^s)^u 2^r \equiv 2^r \not\equiv 1 \pmod{p_t},$$

which implies that $2^n \not\equiv 1 \pmod{n}$. When all $\operatorname{ord}(2, p_j)$ is odd, choose t so that $s = \operatorname{ord}(2, p_t) < p_j$ for all $j \neq t$. Then, for $n = p_t^{a_t} q$, q is not divisible by $s > 1$ and so we can argue in the same way as above.

Lemma 2.2. *For a positive integer n $(n+1)^n+n^2-1$ is divisible by $n^2(n+1)$.*

Proof. We see from the binomial theorem that

$$(n+1)^{n-1} \equiv (n-1)\, n+1 \bmod n^2$$

whence we have

$$\begin{aligned}(n+1)^n+n^2-1 &= (n+1)\,\{(n+1)^{n-1}+n-1\}\\ &\equiv (n+1)\,\{(n-1)\,n+1+n-1\} \equiv 0 \bmod n^2(n+1)\end{aligned}$$

We may deduce, from (i) of section 1 and Lemma 2.2,

Theorem 2.3. *$\varepsilon(N) \leqq (N-1)^2$ and, for odd N, $\varepsilon(N) \leqq N+1$.*

With the above theorem we define an integer N to be **simple** if

$$\begin{aligned}\varepsilon(N) &= N+1 \quad \text{for odd } N\\ \varepsilon(N) &= (N-1)^2 \text{ for even } N\end{aligned}$$

Lemma 2.4. *For any even integer $a \geqq 2$ and for integer $n \geqq 1$, let $b = (a+1)^n$. Then*

$$a^b+1 \equiv 0 \pmod{b}$$

Proof. We prove this lemma by induction on n. Since b is odd, this is obvious for $n = 1$. Assume that the congruence holds for $n = k$. Setting $t = (a+1)^k$ yields

$$a^{t(a+1)}+1 = (a^t+1)\,\{(a^t)^a-(a^t)^{a-1}+\cdots+1\},$$

in which we have, by the assumption,

$$\begin{aligned}a^t+1 &\equiv 0 \bmod t,\\ (a^t)^a-(a^t)^{a-1}+\cdots+1 &\equiv (-1)^a-(-1)^{a-1}+\cdots+1\\ &= a+1 \equiv 0 \bmod a+1.\end{aligned}$$

Hence one gets $a^{t(a+1)}+1 \equiv 0 \bmod (a+1)^{k+1}$.

Corollary 2.5.

1) $(a^2)^{(a+1)^k} \equiv 1 \bmod (a+1)^k$ *for even* $a \geqq 2$.

2) $2^{3^n}+1 \equiv 0 \bmod 3^n$, $n \geqq 1$.

Proposition 2.6. *Let k be an integer $k \geqq 1$. Then*

1) *for* $n = (3^k-1)(2^{3^k}+1)$ *the equation* (1) *has a solution*

$$(2, \cdots, 2, 1^{n-3^k})$$

2) *For* $n = 2^{3^k}+1$ *the equation* (1) *has solutions*

$$(2^t, 1^{n-1}),$$

where $t = 2, 4, \cdots, 3^k-1$ *are even.*

Proof. Let $m = 3^k-1$; then, by the preceding corollary, $2^{m+1}+1 = (m+1)q$ for some odd q. Then

1) Since $m\,2^{m+1}-1 = (m+1)\,2^{m+1}-(2^{m+1}+1) = (m+1)s$ for odd $s = 2^{m+1}-q$, we see that

$$\begin{aligned}(m2^n+n-m)/(n2^m) &= (m2^n+m2^{m+1})/[m\,(2^{m+1}+1)\,2^m] \\ &= 2\,(2^{(m+1)s}+1)/(2^{m+1}+1)\end{aligned}$$

is an even integer.

2)
$$\begin{aligned}[(2^t)^n+n-1]/(n2^t) &= (2^{nt}+2^{m+1})/[(m+1)\,q2^t] \\ &= (2^{m+1}/2^t)\,\{(2^{(m+1)(qt-1)}+1)/(2^{m+1}+1)\}\end{aligned}$$

is an integer, since $t \leqq m$ and $qt-1$ is odd.

Lemma 2.7. *Let* $n = m^s+1$. *Then* $m^{2s} \equiv 1 \pmod n$.

Proof. This is obvious from $m^{2s}-1 = (m^s-1)(m^s+1)$.

Corollary 2.8. *Suppose* $n = m^s+1$ *with odd s and* $m \equiv -1 \pmod{2s}$. *Then the equation* (1) *has a solution* $(m, 1^{n-1})$.

Proof. Observing that $n \equiv 0 \bmod 2s$ and that $m^n-1 \equiv m^n-m^{2s} = m^{2s}(m^{n-2s}-1) \bmod n$ we may infer by the induction that m^n+n-1 is divisible by nm.

Proposition 2.9. *Let* $n = (m+1)(m^2+m+1) = m^3+2m^2+2m+1$ *with* $m \equiv \pm 1 \bmod 6$. *Then* $m^6 \equiv 1 \pmod n$ *and the equation* (1) *has a solution* $(m, 1^{n-1})$.

Proof. We have $1 \equiv (n-1)^2 = m^2(m^2+2m+2)^2 = m^6+4m^2n \equiv m^6 \bmod n$. It follows by induction that $m^n-1 \equiv m^6(m^{n-6}-1) \equiv 0 \bmod n$.

Proposition 2.10. *Let* $n = (m-1)(m^2-1) = m^3-m^2-m+1$. *Then* $m^{2m-2} \equiv 1 \pmod n$.

Proof. We have

$$\begin{aligned}(m^2)^{m-1}-1 &= (m^2-1)(m^{2(m-2)}-1+m^{2(m-3)}-1+\cdots+m^2-1+m-2+1) \\ &\equiv 0 \bmod (m^2-1)(m-1).\end{aligned}$$

Corollary 2.11. *For odd* $m > 2$ *and* $n = (m-1)(m^2-1)$ *the equation* (1) *has a solution* $(m, 1^{n-1})$.

Proof. This follows from the fact that $(m-1)(m^2-1)$ is divisible by $2(m-1)$.

Proposition 2.12. *For* $n=(m+1)(m^2+m+1)$ *we have* $m^6 \equiv 1 \pmod{n}$ *and, if* $m \equiv \pm 1 \bmod 6$ *then the equation* (1) *has a solution* $(m, 1^{n-1})$.

Proof. The first half follows from the identity

$$m^6-1=(m-1)(m^2+m+1)(m+1)(m^2-m+1) \tag{3}$$

The second half follows from the fact that $6 \mid n$, because $m+1 \equiv 0 \bmod 6$ if $m \equiv -1 \bmod 6$ and, if $m \equiv 1 \bmod 6$ then $m+1 \equiv 0 \bmod 2$ and $m^2+m+1 \equiv 0 \bmod 3$. Similarly one gets, from (3),

Proposition 2.13. *For* $n=(m+1)(m^2-m+1)$ *we have* $m^6 \equiv 1 \pmod{n}$ *and, if* $m \equiv -1 \bmod 6$ *then the equation* (1) *has a solution* $(m, 1^{n-1})$.

Lemma 2.14. *There hold following congruences*:

$$\begin{aligned}
&m^6-1 \equiv 0 \pmod{(m+1)(m^2+m+1)}\\
&m^6+1 \equiv 0 \pmod{m^2+1}\\
&m^{6r}+m^{6(r-1)}+\cdots+m^6+1 \equiv r+1 \pmod{m+1}\\
&m^{6s}-m^{6(s-1)}+\cdots-m^6+1 \equiv 1 \pmod{m+1},
\end{aligned}$$

where s is even. Thus $m^{6r}+m^{6(r-1)}+\cdots+m^6+1 \equiv 0 \bmod m+1$ *if and only if* $r \equiv -1 \bmod m+1$.

Proof. The first two follows from the factorizations:

$$\begin{aligned}
m^6-1&=(m-1)(m^2+m+1)(m+1)(m^2-m+1),\\
m^6+1&=(m^2+1)(m^4-m^2+1)
\end{aligned}$$

Hence $m^6 \equiv 1 \pmod{m+1}$ implies, by the binomial theorem applied to $m=(m+1)-1$, the remaining congruences.

Proposition 2.15. *For* $n=(m+1)(m^2+m+1)(m^3+m^2+m+1)$ *there hold*

$$m^{k(m+1)} \equiv 1 \pmod{n} \text{ with } k=2, 12, 6, 4, 6 \text{ and } 12$$

according as $m \equiv -1, 0, 1, 2, 3$ *and* $4 \pmod 6$.

Proof. Observe that $m^3+m^2+m+1=(m+1)(m^2+1)$.

For $m=6t-1$ we have

$$\begin{aligned}
m^{2(m+1)}-1&=(m^{6t}-1)(m^{6t}+1)\\
&=(m^6-1)(m^6+1)(m^{6(t-1)}-m^{6(t-2)}+\cdots+1)\\
&\quad(m^{6(t-1)}+m^{6(t-2)}+\cdots+m^6+1)
\end{aligned}$$

in which the last factor is $\equiv t \bmod m+1$ by Lemma 2.14, *a fortiori* $\equiv 0 \bmod t$. Since $m^2-m+1 \equiv 0 \bmod 3$ and $m-1 \equiv 0 \bmod 2$ we see from Lemma 2.14 that $m^{2(m+1)}-1$ is divisible by n.

Next consider the case $m \equiv 0$ or $4 \bmod 6$; then

$$m^{12(m+1)}-1=(m^{6(m+1)}-1)(m^{6(m+1)}+1)$$
$$=(m^6-1)(m^6+1)(m^{6m}-m^{6m(m-1)}+\cdots-m^6+1)(m^{6m}+\cdots+m^6+1)$$

in which the last factor is $\equiv m+1\equiv 0$ (mod $m+1$) by Lemma 2.14, whence our assertion again by Lemma 2.14.

For the case $m\equiv 1$ or 3 mod 6 we consider

$$m^{6(m+1)}-1=(m-1)(m+1)(m^2+m+1)(m^2-m+1)(m^{6m}+m^{6(m-1)}+\cdots+m^6+1)$$

in which the last factor can be written as

$$(m^6+1)(m^{6(m-1)}+m^{6(m-3)}+\cdots+m^{12}+1)$$

whose last factor is $\equiv(m-1)/2+1$ (mod $m+1$), since $m^6\equiv 1$ (mod $m+1$). Thus our assertion follows from the fact that $m-1$ is even.

For $m\equiv 2$ mod 6 we set $m=6t+2$; then

$$m^{4(m+1)}-1=m^{12(2t+1)}-1$$
$$=(m^6-1)(m^2+1)(m^4-m^2+1)(m^{12.2t}+m^{12(2t-1)}+\cdots+m^{12}+1)$$

in which the last factor is $\equiv 2t+1$ mod $m+1$ since $m^{12}\equiv 1$ mod $m+1$, and $m^2-m+1\equiv 0$ mod 3. This proves our assertion.

Lemma 2.16.

1) *For* $q=8t+1$, $2^{2q}\equiv 1$ (mod q) *implies* $2^{2q-4}(1+2^{2q})+t\equiv 0$ (mod q).

2) *For odd* m *and* $n=m^3s+2$, $m^n\equiv 1$ (mod n) implies $m^{n-3}(1+m^n)+s\equiv 0$ (mod n).

Proof.

1) We see from $-2^3t\equiv 1$ (mod q) that

$$2^{2q-4}(1+2^{2q})+t\equiv 2^{2q-3}+t\equiv 2^{2q-3}(-2^3t)+t$$
$$\equiv -2^{2q}t+t\equiv -t+t\equiv 0 \pmod q$$

2) Using $-m^3s\equiv 2$ (mod n) we have

$$m^{n-3}(1+m^n)+s\equiv 2m^{n-3}+s\equiv -m^3sm^{n-3}+s$$
$$\equiv -s+s\equiv 0 \pmod n.$$

Corollary 2.17. *For* $n=m^3s+2$ *with odd* m *and* $m^n\equiv 1$ (mod n) *the equation* (1) *has a solution* $(1^{n-2}, m, m^2)$. *For* $n=2q$, $q=8t+1$ *with* $2^{2q}\equiv 1$ (mod q) *the equation* (1) *has a solution* $(1^{n-2}, 2, 4)$.

Proof. Since $(m^n+m^{2n}+n-2)/(nm^3)=\{m^{n-3}(1+m^n)+s\}/n$, the assertion for odd m follows from Lemma 2.16, 2). For $m=2$ we have

$$2^{n-3}(1+2^n)+2t=2\{2^{n-4}(1+2^n)+t\}\equiv 0 \pmod{2q}.$$

Lemma 2.18.

1) *For any integer* $t\geqq 3$ $t^{t(t-2)}+t-2\equiv 0$ (mod $(t-1)^2$).

2) *For odd* $t \geqq 1 t^{t(t+2)}+t+2 \equiv 0 \pmod{(t+1)^2}$.

Proof. We see from the binomial theorem that

$$\begin{aligned}(t-1+1)^{t(t-2)}+t-2 &\equiv 1+t\,(t-2)\,(t-1)+t-2\\ &= (t-1)\,(t^2-2t+1) \equiv 0 \pmod{(t-1)^2},\end{aligned}$$

which proves the first part. Similarly we have

$$\begin{aligned}(t+1-1)^{t(t+2)}+t+2 &\equiv (-1)^{t(t+2)}+t\,(t+2)\,(t+1)+t+2\\ &= (t+1)\,(t^2+2t+1) \equiv 0 \pmod{(t+1)^2}.\end{aligned}$$

Corollary 2.19. *For* $n = t\,(t-2)+1$ *the equation* (1) *has a solution* $(1^{n-1}, t)$. *For* $n = t\,(t+2)+1$ *with odd* t *the equation* (1) *has a solution* $(1^{n-1}, t)$.

Lemma 2.20. *For* $n = t\,(2t-3)+1 = (2t-1)\,(t-1)$,

$$t^{n-1}+2t-3 \equiv 0 \pmod{n} \text{ if and only if } t^n \equiv 1 \pmod{n}.$$

Proof. Since t and n are relatively prime it follows that

$$\begin{aligned}t^{n-1}+2t-3 \equiv 0 \bmod n \text{ iff } t\,(t^{n-1}+2t-3)\\ \equiv 0 \bmod n \text{ iff } t^n-1 \equiv 0 \bmod n\end{aligned}$$

Corollary 2.21. *If* $t^n \equiv 1 \pmod{n}$ *for* $n = (2t-1)\,(t-1)$ *then the equation* (1) *has a solution* $(t, 1^{n-1})$.

Now we observe that an integer $q = 2p$ where p is odd prime is simple if, and only if both congruences

$$q^n+n-1 \equiv 0 \pmod{qn} \text{ and } 2^n+p^n+n-2 \equiv 0 \pmod{2pn}$$

are not true for each n with $1 \leqq n < (q-1)^2$. Note that the former holds only if there exits a positive integer k such that $n = qk+1$, where $k < q-2$. Then, since n and q are relatively prime, it is equivalent to $q^{n-1}+k \equiv 0 \pmod{n}$, which implies that $q^n+kq+1 \equiv 1 \pmod{n}$, that is,

$$q^n \equiv 1 \pmod{n}.$$

Lemma 2.22. *Let* q *be an even natural number and let* $n = qk+1$, $k \geqq 1$. *Assume that* $q^n \equiv 1 \pmod{n}$. *Then* $q-1$ *is divisible by the minimal prime factor* p *of the order* ord (q, n), *and hence* gcd $(n, q-1) > 1$.

Proof. Write $t = \mathrm{ord}\,(q, n)$; then $t \mid n$ implies that $p \mid n$, hence $q^t \equiv 1 \pmod{p}$. Since n and q are relatively prime, hence $\gcd(q, p) = 1$, we see from the Fermat theorem that $q^{p-1} \equiv 1 \pmod{p}$. Thus

$$\mathrm{ord}\,(q, p) \mid t \text{ and } \mathrm{ord}\,(q, p) \mid p-1.$$

Since all prime factors of t are $\geqq p$, it follows that $\mathrm{ord}\,(q, p) = 1$, that is, $q \equiv 1 \pmod{p}$, whence our assertion.

Corollary 2.23. *Let q be an even positive integer such that $q-1$ is prime. Then, for each k with $1 \leqq k < q-2$, we have non-congruences*

$$q^n \not\equiv 1 \pmod{n}, \; n = qk+1.$$

Proof. Since $n = (q-1)\,k+k+1$, $2 \leqq k+1 \leqq q-2$, it is obvious that $\gcd(n, q-1) = 1$, whence our assertion by the contrapositive.

Corollary 2.24. *Let $q-1 = p_1p_2$ with odd prime p_1, p_2 and assume* $\mathrm{ord}\,(q, q\,(p_1-1)+1)$ *and* $\mathrm{ord}\,(q, q\,(p_2-1)+1)$ *are even. Then, for all k with $1 \leqq k \leqq q-3$, we have non-congruences $q^n \not\equiv 1 \pmod{n}$ with $n = qk+1$.*

Next, since the latter congruence holds only if n is odd, we assume n is odd. Then it is equivalent to $2^n+p^n+n-2 \equiv 0 \pmod{np}$. We consider the case $n = kp$, that is, the congruence $2^{kp}+p^{kp}+kp-2 \equiv 0 \pmod{kp^2}$. More weak congruence is $2^{kp}+kp-2 \equiv 0 \pmod{p^2}$. This does not hold if

$$(p^2-kp+2)^{p-1} \not\equiv 1 \pmod{p^2}, \tag{3}$$

since $(2^{kp})^{p-1} = (2^k)^{\varphi(p^2)} \equiv 1 \pmod{p^2}$ for odd prime p implies $2^{kp} \equiv 2-kp \pmod{p^2}$. But the non-congruences for $k \leqq 4p-4$ do not hold for few p, as machine-search shows within some large range p, in which the cases except $k = 1$, $p = 3$ or 11 can be excluded. Hence we make the following **conjecture**:

For odd prime p such that $2p-1$ is a prime and that $p > 3$, $2p$ is simple.

Remark. The famous Wieferich congruence $2^{p-1} \equiv 1 \pmod{p^2}$ holds only for $p = 1093$, 3511 in the range $p \leqq 6\times10^9$ (see [1, 2]). We can shows by a machine-search that the inequality

$$\mathrm{ord}\,(2+(k-1)\,p,\, p^2) \neq \mathrm{ord}\,(p^2-kp+2,\, p^2)$$

holds if and only if either $(2+(k-1)\,p)^{p-1} \equiv 1 \pmod{p^2}$ or $(p^2+2-kp)^{p-1} \equiv 1 \pmod{p^2}$ for large range of prime p.

3. Tables

To make up the Table I we have used the computer package "GAP" together with the following program "allfac. gap" which gives a list of the factorization lists composed with factors $\geqq k$ of x. With this program on memory "facag. gap" gives solutions of (1) for $n = p$ from p_1 to p_2.

```
allfac: = function (x, k)
  local a, b;
  if IsPrime (x) or k*k > x then
        return [[x]];
  fi;
  b: = [[x]];
```

```
    for a in [k ·· RootInt (x)] do
      if RemInt (x, a) = 0 then
        Append (b, List (allfac (x/a, a), y → Concatenation ([a], y)));
      fi;
    od;
    return b;
  end;

facag: = function (n1, n2, p1, p2)
  local f, g, n, p. j;
  n: = n1;
  while n ≦ n2 do
    f: = allfac (n, 2);
    for p in [p1 ··· p2] do
      for j in [1 ··· Number (f)] do
        g: = f [j];
if p > Number (g) and RemInt ((Sum (List (g, z → z^p))+p−Number (g)), p*n) = 0 then
          Print ("p =", p, " ", g, " ");
fi;
      od;
    od;
    n: = n+2;
  od;
end;
```

Table I m (n) for n $\leqq$ 200

n	m (n)	solution $x_1, \cdots, x_n$
3	2	1, 2, 3
4	$\leqq$ 7	1, 1, 1, 3
5	$\leqq$ 4	5, 11, 12, 13, 19
6	$\leqq$ 521	1, 1, 1, 1, 1, 5
7	$\leqq$ 98460	2, 3, 5, 9, 47, 56, 88
8	$\leqq$ 42151	1^5, 9, 9, 11
9	$\leqq$ 1253	1, 1, 6, 10, 11, 14, 14, 14, 19
10	$\leqq$ 2861165	1^4, 3, 8, 12, 15, 15, 23
11	$\leqq$ 44392	1^6, 2, 2, 2, 5, 5
12	$\leqq$ 23775972551	1^{11}, 11
13	$\leqq$ 231924582674735980	1^7, 2, 8, 8, 8, 8, 89
14	$\leqq$ 21633936185161	1^{13}, 13
15	$\leqq$ 11306274409	1^{13}, 4, 7
16	$\leqq$ 896807	1^{15}, 3
17	$\leqq$ 22 digits	1^{12}, 5, 16, 34, 47, 56
18	$\leqq$ 7282	1^{16}, 2, 2
19	$\leqq$ 351561282356642220105	1^{13}, 4, 4, 11, 22, 30, 30
20	$\leqq$ 38742049	1^{18}, 3, 3
21	$\leqq$ 52357696561	1^{20}, 4
22	$\leqq$ 27 digits	1^{21}, 21
23	$\leqq$ 34 digits	1^{18}, 2, 13, 14, 34, 57
24	$\leqq$ 30 digits	1^{23}, 23
25	$\leqq$ 189535253532864676	1^{24}, 6
26	$\leqq$ 16962579960192958638269305	1^{23}, 2, 8, 13
27	$\leqq$ 28 digits	1^{26}, 13
28	$\leqq$ 39 digits	1^{27}, 27
29	$\leqq$ 53 digits	1^{24}, 3, 42, 53, 93, 133
30	$\leqq$ 41 digits	1^{29}, 29
31	$\leqq$ 57 digits	1^{27}, 8, 100, 109, 128
32	$\leqq$ 40 digits	1^{30}, 13, 23
33	$\leqq$ 41 digits	1^{29}, 2, 3, 14, 24
34	$\leqq$ 40 digits	1^{30}, 2, 2, 3, 19
35	$\leqq$ 37 digits	1^{32}, 2, 6, 14
36	$\leqq$ 23 digits	1^{35}, 5
37	$\leqq$ 152 digits	1^{33}, 4, 4, 4, 19935
38	$\leqq$ 57 digits	1^{37}, 37
39	$\leqq$ 47 digits	1^{32}, 3, 4, 4, 4, 7, 7, 23
40	$\leqq$ 101313878825474407	1^{39}, 3
41	$\leqq$ 86 digits	1^{39}, 5, 161
42	$\leqq$ 52357696561	1^{40}, 2, 2
43	$\leqq$ 97 digits	1^{38}, 2, 11, 12, 167, 286
44	$\leqq$ 69 digits	1^{43}, 43
45	$\leqq$ 42 digits	1^{43}, 7, 10
46	$\leqq$ 73 digits	1^{45}, 45
47	$\leqq$ 119 digits	1^{42}, 2, 2, 8, 25, 485
48	$\leqq$ 77 digits	1^{47}, 47
49	$\leqq$ 42 digits	1^{48}, 8
50	$\leqq$ 82 digits	1^{46}, 6, 29, 54, 61
51	$\leqq$ 77 digits	1^{45}, 2, 2, 4, 6, 18, 43
52	$\leqq$ 34 digits	1^{50}, 5, 5
53	$\leqq$ 116 digits	1^{48}, 2, 2, 13, 42, 211
54	$\leqq$ 75 digits	1^{52}, 11, 29
55	$\leqq$ 87 digits	1^{51}, 4, 5, 31, 49
56	$\leqq$ 94 digits	1^{55}, 55
57	$\leqq$ 46 digits	1^{56}, 7
58	$\leqq$ 92 digits	1^{55}, 7, 10, 46
59	$\leqq$ 86 digits	1^{54}, 2, 2, 2, 23, 35
60	$\leqq$ 103 digits	1^{59}, 59
61	$\leqq$ 203 digits	1^{58}, 3, 5, 2679
62	$\leqq$ 108 digits	1^{61}, 61

63	$\leqq$ 142 digits	1^{58}, 2, 2, 29, 113, 240
64	$\leqq$ 29 digits	1^{63}, 3
65	$\leqq$ 192 digits	1^{60}, 4, 20, 39, 93, 1284
66	$\leqq$ 38 digits	1^{65}, 2, 4
67	$\leqq$ 130 digits	1^{63}, 3, 9, 19, 107
68	$\leqq$ 88 digits	1^{64}, 2, 2, 2, 9, 15, 20, 25
69	$\leqq$ 140 digits	1^{65}, 4, 4, 10, 127
70	$\leqq$ 126 digits	1^{69}, 69
71	$\leqq$ 220 digits	1^{68}, 9, 52, 1575
72	$\leqq$ 130 digits	1^{71}, 71
73	$\leqq$ 240 digits	1^{70}, 2, 17, 2393
74	$\leqq$ 133 digits	1^{71}, 8, 30, 75
75	$\leqq$ 149 digits	1^{73}, 26, 111
76	$\leqq$ 129 digits	1^{74}, 3, 55
77	$\leqq$ 216 digits	1^{73}, 6, 10, 108, 823
78	$\leqq$ 144 digits	1^{77}, 77
79	$\leqq$ 128 digits	1^{74}, 2, 2, 5, 25, 50
80	$\leqq$ 149 digits	1^{79}, 79
81	$\leqq$ 47 digits	1^{80}, 4
82	$\leqq$ 160 digits	1^{78}, 2, 37, 67, 110
83	$\leqq$ 229 digits	1^{81}, 9, 657
84	$\leqq$ 38 digits	1^{81}, 3, 3, 3
85	$\leqq$ 205 digits	1^{79}, 3, 3, 4, 8, 8, 315
86	$\leqq$ 163 digits	1^{85}, 85
87	$\leqq$ 314 digits	1^{85}, 172, 4951
88	$\leqq$ 125 digits	1^{86}, 17, 29
89	$\leqq$ 217 digits	1^{85}, 4, 6, 107, 332
90	$\leqq$ 172 digits	1^{89}, 89
91	$\leqq$ 135 digits	1^{84}, 2, 2, 2, 8, 15, 18, 37
92	$\leqq$ 177 digits	1^{91}, 91
93	$\leqq$ 107 digits	1^{86}, 2, 2, 2, 2, 5, 5, 16
94	$\leqq$ 182 digits	1^{93}, 93
95	$\leqq$ 148 digits	1^{92}, 5, 32, 41
96	$\leqq$ 65 digits	1^{95}, 5
98	$\leqq$ 127 digits	1^{96}, 20, 22
100	$\leqq$ 46 digits	1^{99}, 3
101	$\leqq$ 396 digits	1^{99}, 100, 9901
102	$\leqq$ 201 digits	1^{101}, 101
103	$\leqq$ 251 digits	1^{101}, 301, 319
104	$\leqq$ 201 digits	1^{103}, 103
105	$\leqq$ 84 digits	1^{100}, 2, 3, 3, 5, 7
106	$\leqq$ 252 digits	1^{103}, 4, 101, 276
107	$\leqq$ 425 digits	1^{105}, 106, 11131
108	$\leqq$ 129 digits	1^{106}, 11, 17
110	$\leqq$ 142 digits	1^{108}, 9, 21
111	$\leqq$ 108 digits	1^{110}, 10
112	$\leqq$ 180 digits	1^{106}, 3, 5, 9, 9, 15, 47
113	$\leqq$ 455 digits	1^{111}, 112, 12433
114	$\leqq$ 230 digits	1^{113}, 113
115	$\leqq$ 243 digits	1^{112}, 2, 18, 33, 148
116	$\leqq$ 235 digits	1^{115}, 115
117	$\leqq$ 347 digits	1^{112}, 2, 5, 6, 11, 1064
118	$\leqq$ 240 digits	1^{117}, 117
119	$\leqq$ 106 digits	1^{115}, 6, 15, 34, 220
120	$\leqq$ 99 digits	1^{119}, 7
121	$\leqq$ 128 digits	1^{120}, 12
122	$\leqq$ 250 digits	1^{121}, 121
124	$\leqq$ 102 digits	1^{122}, 3, 7
125	$\leqq$ 181 digits	1^{124}, 31
126	$\leqq$ 86 digits	1^{125}, 5
127	$\leqq$ 524 digits	1^{125}, 25, 15090
128	$\leqq$ 59 digits	1^{126}, 3, 3
129	$\leqq$ 308 digits	1^{125}, 3, 4, 15, 273
130	$\leqq$ 127 digits	1^{127}, 2, 3, 10

131	≦ 444 digits	1^{128}, 2, 8, 2744
132	≦ 276 digits	1^{131}, 131
133	≦ 77 digits	1^{128}, 2, 2, 2, 2, 4
134	≦ 281 digits	1^{133}, 133
135	≦ 265 digits	1^{132}, 13, 64, 103
136	≦ 127 digits	1^{135}, 9
137	≦ 515 digits	1^{135}, 33, 6408
138	≦ 120 digits	1^{133}, 3, 3, 3, 8, 8
140	≦ 296 digits	1^{139}, 139
142	≦ 301 digits	1^{141}, 141
144	≦ 147 digits	1^{143}, 11
145	≦ 235 digits	1^{140}, 5, 6, 6, 7, 46
146	≦ 312 digits	1^{145}, 145
147	≦ 42 digits	1^{144}, 2, 2, 2
148	≦ 220 digits	1^{141}, 2, 2, 5, 5, 24, 34, 35
149	≦ 638 digits	1^{147}, 148, 21757
150	≦ 322 digits	1^{149}, 149
152	≦ 327 digits	1^{151}, 151
153	≦ 491 digits	1^{151}, 184, 1801
154	≦ 333 digits	1^{153}, 153
155	≦ 248 digits	1^{151}, 5, 15, 25, 44
156	≦ 105 digits	1^{152}, 3, 3, 3, 5
158	≦ 343 digits	1^{157}, 157
159	≦ 520 digits	1^{155}, 3, 3, 95, 2096
160	≦ 132 digits	1^{157}, 3, 7, 7
161	≦ 439 digits	1^{158}, 3, 3, 574
162	≦ 47 digits	1^{160}, 2, 2
163	≦ 315 digits	1^{160}, 26, 46, 94
164	≦ 135 digits	1^{159}, 2, 2, 2, 2, 7
165	≦ 174 digits	1^{162}, 3, 3, 12
166	≦ 364 digits	1^{165}, 165
167	≦ 319 digits	1^{164}, 23, 58, 89
168	≦ 369 digits	1^{167}, 167
169	≦ 191 digits	1^{168}, 14
170	≦ 375 digits	1^{169}, 169
171	≦ 326 digits	1^{170}, 85
172	≦ 380 digits	1^{171}, 171
173	≦ 633 digits	1^{170}, 2, 29, 4989
174	≦ 385 digits	1^{173}, 173
175	≦ 119 digits	1^{171}, 2, 2, 2, 5
176	≦ 341 digits	1^{175}, 175
178	≦ 396 digits	1^{177}, 177
179	≦ 797 digits	1^{177}, 178, 31507
180	≦ 259 digits	1^{175}, 2, 2, 2, 2, 29
182	≦ 407 digits	1^{181}, 181
183	≦ 201 digits	1^{182}, 13
184	≦ 412 digits	1^{183}, 183
185	≦ 458 digits	1^{181}, 3, 12, 17, 327
186	≦ 128 digits	1^{185}, 5
187	≦ 210 digits	1^{184}, 6, 6, 14
188	≦ 333 digits	1^{185}, 7, 9, 63
189	≦ 111 digits	1^{188}, 4
190	≦ 428 digits	1^{189}, 189
191	≦ 825 digits	1^{189}, 15, 22716
192	≦ 363 digits	1^{189}, 5, 5, 83
194	≦ 439 digits	1^{193}, 193
196	≦ 215 digits	1^{195}, 13
197	≦ 894 digits	1^{195}, 196, 38221
198	≦ 450 digits	1^{197}, 197
200	≦ 93 digits	1^{188}, 3, 3

Table II $\varepsilon(N)$ for non-simple N

N	$\varepsilon(N)$	factorization	N	$\varepsilon(N)$	factorization
6	9999	(2, 3)	8	18	(2, 4)
16	81	(16)	18	21	(2, 9)
20	18	(2, 10)	22	11	(2, 11)
28	15	(4, 7)	30	295	(3, 10)
32	259	(2, 4, 4)	36	505	(36)
40	18	(2, 20)	42	3	(3, 14)
44	42	(2, 22)	45	16	(5, 9)
48	34	(2, 24)	52	5	(4, 13)
56	162	(2, 28), (4, 14), (2, 4, 7)	58	335	(2, 29)
63	11	(3, 21)	64	133	(2, 2, 2, 2, 4)
66	795	(6, 11)	68	882	(2, 34)
70	45	(7, 10)	72	705	(8, 9)
76	1065	(76)	78	2107	(78)
80	66	(4, 20)	88	162	(4, 22)
92	42	(2, 46)	94	8649	(94)
100	513	(4, 25)	102	21	(2, 51)
104	42	(2, 4, 13)	106	2439	(106)
108	165	(3, 3, 12)	112	36	(2, 2, 2, 2, 7)
116	18	(2, 58)	120	2401	(120)
124	18	(2, 2, 31)	126	3025	(126)
128	1026	(2, 64), (4, 32), (8, 16)	135	16	(5, 27)
136	882	(2, 68)	138	1243	(3, 46)
140	162	(2, 2, 5, 7)	142	8379	(142)
143	42	(11, 13)	144	147	(2, 4, 18)
145	36	(5, 29)	147	40	(3, 49)
148	2058	(2, 2, 37)	152	42	(2, 4, 19)
156	625	(156)	160	1026	(4, 40), (10, 16)
164	162	(2, 82)	165	76	(3, 55)
168	35	(2, 6, 14)	172	1539	(4, 43)
176	84	(2, 2, 2, 2, 11)	180	2530	(2, 5, 18)
184	6050	(4, 46)	186	15625	(186)
187	100	(11, 17)	188	9234	(2, 94)
189	110	(9, 21)	192	247	(3, 64)
196	162	(2, 98), (4, 7, 7)	200	11	(2, 2, 2, 5, 5)
207	160	(9, 23)	208	26	(2, 8, 13)
216	11	(2, 2, 54)	220	2058	(10, 22)
224	36	(2, 2, 2, 4, 7)	226	32319	(226)
228	34	(2, 2, 3, 19)	231	100	(3, 7, 11)
232	18	(2, 116)	236	31625	(236)
240	2530	(2, 8, 15)	244	5634	(2, 122)
248	882	(2, 4, 31)	249	4	(3, 83)
256	513	(256)	260	18	(2, 5, 26)
261	256	(9, 29)	264	51250	(4, 66)
268	21402	(2, 134)	272	66	(2, 136)
279	272	(3, 93)	280	330	(2, 4, 5, 7), (2, 5, 28)
284	71442	(2, 142)	285	418	(3, 5, 19)
286	16875	(286)	288	26	(2, 3, 48)
292	6498	(2, 146), (2, 2, 73)	296	47250	(4, 74)
299	32	(13, 23)	300	2530	(2, 3, 50)
303	201	(3, 101)	304	324	(2, 2, 2, 38)
308	9234	(2, 11, 14)	310	2511	(10, 31)
316	6321	(316)	319	54	(11, 29)
320	1026	(4, 80), (16, 20)	324	1218	(6, 69)
328	162	(2, 164)	336	4324	(2, 2, 2, 6, 7)
340	930	(2, 2, 85)	341	246	(11, 31)
344	5490	(4, 86)	346	103455	(346)
350	13377	(352)	351	272	(9, 39)
352	147	(2, 2, 2, 2, 2, 11)	356	118098	(2, 2, 89)
360	46730	(3, 10, 12)	364	729	(364)
366	147	(2, 183)	368	354	(4, 92)
376	6930	(4, 94)	380	2530	(2, 2, 5, 19)
382	114219	(382)	384	144130	(6, 64)
388	40986	(2, 194)	395	96	(5, 79)

Table III k and prime p with $(p^2+2-kp)^{p-1} \equiv 1 \pmod{p^2}$

k	p	search range
1	3*, 11	$p \leqq 14\times10^8$
2	1897121, 52368101, 126233057	$p \leqq 6\times10^8$
3	7#, 1483597	$p \leqq 3\times10^8$
4	3*, 5**, 110057537	$p \leqq 3\times10^8$
5	6266543	$p \leqq 3\times10^8$
6	47, 27967, 46477	$p \leqq 3\times10^8$
7	3*, 13, 263	$p \leqq 3\times10^8$
8	17, 251, 15823	$p \leqq 3\times10^8$
9	5**	$p \leqq 3\times10^8$
10	7#, 1753, 1437049	$p \leqq 3\times10^8$
11	3491, 11822777	$p \leqq 3\times10^8$
12	23	$p \leqq 3\times10^8$
13	2, 19	$p \leqq 3\times10^8$
14	5**, 397	$p \leqq 3\times10^8$
15		$p \leqq 3\times10^8$
16	3*	$p \leqq 3\times10^8$
17	1847, 44566369	$p \leqq 3\times10^8$
18	101, 269, 907, 1129, 36061	$p \leqq 3\times10^8$
19	3*, 5**, 31, 16349, 32609, 107530327	$p \leqq 3\times10^8$
20	13	$p \leqq 3\times10^8$

*··· ord (8, 9) = 2; **··· ord (7, 25) = 4; #··· ord (30, 49) = 3

References

1) R. Crandall: K. Dilcher, and C. Pomerance: A search for Wieferich and Wilson primes, Math. Comp. **66**, 433-449 (1997)
2) P. L. Montgomery: New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. **61**, 361-363 (1993)
3) T. Nagell: Introduction to number theory, Chelsea Publ. Company. New York (1981)
4) Y. Nomura: Mathematics Magazine **68**, No. **5**, 399 (1995)
5) J. S. Sumner and K. L. Dove: Mathematics Magazine **69**, No. **5**, 386-388 (1996)
6) Y. Nomura: Abstracts of short communications and poster sessions in ICM98, 44 (1998)