(265) (*MMAG, Vol. 64, no. 5, p. 351*). We will show that these are the positive integers N which are not a power of 2. Indeed let N be an integer of the form

$$N = \binom{k}{2} + kn = \frac{k(k-1)}{2} + nk \qquad (k > 1, n \geq 1).$$

Since $2N = k(k + 2n - 1)$, it follows that $2N$ must have an odd factor larger than 2, and therefore similarly for N. It follows that N cannot be a power of 2.

Conversely, let N be a positive integer which has an odd factor larger than 2. Consider the factorization of $2N$ as a product of two positive integers of which one is odd. Let A be the smallest of these two factors and B the largest. Setting $k = A$ and $n = \frac{B+1-A}{2}$, it follows that

$$\binom{k}{2} + kn = \frac{A(A-1)}{2} + A\frac{B+1-A}{2} = \frac{AB}{2} = N,$$

which gives the result.

REMARK: Since

$$\binom{k}{2} + kn = 1 + 2 + \cdots + (k-1) + kn = n + (n+1) + \cdots + (n+k-1),$$

the problem is equivalent to the one that consists of searching for the positive integers which can be written as the sum of consecutive integers.

(266) They are the integers n of the form $n = 4m + 2$, $m = 0, 1, 2 \ldots$, since $3^{4m+2} \equiv 9 \equiv -1 \pmod{10}$, while $3^{4m} \equiv 1 \pmod{10}$, $3^{4m+1} \equiv 3 \pmod{10}$ and $3^{4m+3} \equiv 7 \pmod{10}$.

(267) It is the number 5. Indeed, since $n! \equiv 0 \pmod 7$ as soon as $n \geq 7$, we have

$$\begin{aligned} 1! + 2! + \cdots + 50! &\equiv 1! + 2! + 3! + 4! + 5! + 6! \\ &\equiv 1 + 2 + 6 + 3 + 1 + 6 \equiv 5 \pmod 7. \end{aligned}$$

(268) Since for $i \geq 4$, $12|i!$, the remainder is $1 + 2 + 6 = 9$.

(269) For n odd, $10 \cdot 32^n + 1 \equiv 0 \pmod 3$, while for each even integer n, $10 \cdot 32^n + 1 \equiv 0 \pmod{11}$.

(270) The answer is YES. Since $n^6 \equiv 1 \pmod 9$ for each integer n such that $(n, 3) = 1$ and since $n^2 \equiv 4 \pmod 9$ for $n \equiv 2 \pmod 9$, it follows that if $n \equiv 2 \pmod 9$, we have $n^6 + n^2 + 4 \equiv 0 \pmod 9$. On the other hand, since $n^6 + n^2 + 4 \equiv 0 \pmod 4$ for all even n, we may conclude that $36|n^6 + n^2 + 4$ for $n = 18k + 2$, $k = 0, 1, 2, \ldots$.

(271) If the equation $3k - 1 = x^2 + 3y^2$ had a solution, then we would have $x^2 \equiv -1 \equiv 2 \pmod 3$, which is impossible because $x^2 \equiv 0, 1 \pmod 3$.

(272) We know that

$$m = \sum_{i=1}^{[\log n / \log p]} \left[\frac{n}{p^i}\right].$$

Amongst the integers $1, 2, \ldots, n$, those which are divisible by p are: $p, 2p, \ldots, k_1 p$, where $k_1 = [n/p]$. Since

$$n! = 1 \cdot 2 \cdots (p-1)(\mathbf{p})(p+1)(p+2) \cdots (2p-1)(\mathbf{2p})$$
$$\cdot(2p+1)(2p+2) \cdots (3p-1)(\mathbf{3p})((k_1-1)p+1)((k_1-1)p+2)\cdot$$
$$\cdots (k_1 p - 1)(\mathbf{k_1 p})(k_1 p + 1)(k_1 p + 2) \cdots n$$

and since from Wilson's Theorem, the product of the integers in each set $\{1, 2, \ldots, p-1\}$, $\{p+1, p+2, \ldots, 2p-1\}, \ldots, \{(k_1-1)p+1, (k_1-1)p+2, \ldots, k_1 p - 1\}$ is congruent modulo p to -1, it follows that

$$\frac{n!}{p^{k_1}} \equiv (-1)^{k_1} k_1! \left(n - \left[\frac{n}{p}\right] p\right)! \pmod{p}.$$

Now, amongst the integers $1, 2, \ldots, k_1$, those which are divisible by p are: $p, 2p, \ldots, k_2 p$, where $k_2 = [k_1/p] = [n/p^2]$. It follows that

$$\frac{n!}{p^{k_1+k_2}} \equiv (-1)^{k_1+k_2} k_2! \left(n - \left[\frac{n}{p}\right] p\right)! \left(\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right] p\right)! \pmod{p},$$

where $1 \leq k_2 < k_1$. Continuing this process, the result follows.

(273) We must show that $n^{13} - n \equiv 0 \pmod{10}$ or equivalently that $n^{13} - n \equiv 0 \pmod 2$ and $n^{13} - n \equiv 0 \pmod 5$. Using Fermat's Little Theorem, $n^2 \equiv n \pmod 2$ which implies $n^{13} \equiv n \pmod 2$. Similarly, $n^5 \equiv n \pmod 5$ implies $n^{13} \equiv n \pmod 5$.

(274) Since n must be divisible by 7 and by 11, it can be written as $n = 7^a \cdot 11^b$. But $n/7 = 7^{a-1} \cdot 11^b$ must be the 7-th power of an integer, in which case $a \equiv 1 \pmod 7$ and $b \equiv 0 \pmod 7$. Moreover, $n/11 = 7^a \cdot 11^{b-1}$ must be the 11-th power of an integer, so that $a \equiv 0 \pmod{11}$ and $b \equiv 1 \pmod{11}$. Solving this system of congruences gives $a \equiv 22 \pmod{77}$ and $b \equiv 56 \pmod{77}$. Hence, the smallest positive integer satisfying the given constraints is $n = 7^{22} \cdot 11^{56}$.

(275) Consider the system of congruences $x + j - 1 \equiv 0 \pmod{p_j^2}$, $j = 1, 2, \ldots, k$, where p_j stands for the j-th prime number. From the Chinese Remainder Theorem, this system has one solution; that is there exists an integer n which verifies these k congruences. Therefore, each of the k integers $n, n+1, \ldots, n+k-1$ is divisible by a perfect square, as required.

(276) Since $x \equiv a \pmod m$, there exists $k \in \mathbb{Z}$ such that $x = a + km$ and therefore $a + km \equiv b \pmod n$. Hence, there exists $j \in \mathbb{Z}$ such that $a + km = b + jn$, that is $km - jn = -(a-b)$. Since $(m,n)|m$ and $(m,n)|n$, it follows that $(m,n)|(a-b)$.

Reciprocally, assume that $(m,n)|(a-b)$. Then, there exists $M \in \mathbb{Z}$ such that $a - b = M(m,n)$ and since $(m,n) = k_1 m + k_2 n$, $k_1, k_2 \in \mathbb{Z}$, it follows that there exist integers j and k such that $a - b = -km + jn$, $k = -k_1 M$, $j = k_2 M$. Therefore, we have $a + km = b + jn$. Setting $x = a + km$, we obtain $x \equiv a \pmod m$ and moreover $x = a + km = b + jn$, that is $x \equiv b \pmod n$.

(277) Letting $N = \binom{p}{k}$, then

$$k! N = p(p-1) \cdots (p-k+1) \equiv 0 \pmod{p},$$

and since $(k!, p) = 1$ then $N \equiv 0 \pmod p$.

(278) (a) This follows from Problem 277 and induction on n.

(b) Since $a^p \equiv b^p \pmod{p}$, then by Fermat's Little Theorem, we have $a \equiv b \pmod{p}$ and therefore there exists an integer k such that $a = b + kp$. Hence, by the Binomial Theorem, there exists an integer K such that

$$\begin{aligned} a^p &= (b+kp)^p \\ &= b^p + \binom{p}{1} b^{p-1} kp + \binom{p}{2} b^{p-2} k^2 p^2 + \cdots + k^p p^p = b^p + Kp^2, \end{aligned}$$

where we used the result of Problem 277, thus completing the proof of part (b).

(279) Let $N = \binom{p-1}{k} = \dfrac{(p-1)(p-2)\cdots(p-k)}{k!}$. We then have

$$k!\, N \equiv (-1)^k k! \pmod{p}$$

and since $(k!, p) = 1$, we conclude that $N \equiv (-1)^k \pmod{p}$.

(280) From Wilson's Theorem,

$$\begin{aligned} (p-1)! &= (p-1)(p-2)\cdots(p-r)(p-r-1)! \\ &\equiv (-1)^r r!(p-r-1)! \equiv -1 \pmod{p}. \end{aligned}$$

Since $(-1)^r r! \equiv 1 \pmod{p}$, we obtain the result.
For the second part, it is enough to notice that $(-1)^9 9! \equiv 1 \pmod{269}$ and that $(-1)^{15} 15! \equiv 1 \pmod{479}$.

(281) Assume that a solution exists. First, if β is odd,

$$2^\beta - 1 \equiv (-1)^\beta - 1 \equiv -2 \equiv 1 \not\equiv 0 \pmod{3},$$

which contradicts the given equation. Similarly, if β is even,

$$2^\beta - 1 = \left(2^{\beta/2} - 1\right)\left(2^{\beta/2} + 1\right),$$

which means that $3 | (2^{\beta/2} - 1) > 3$ or $3 | (2^{\beta/2} + 1) > 3$, and this is why we must have that $p | (2^{\beta/2} - 1)$ and $p | (2^{\beta/2} + 1)$, implying that $p | 2$, which is not possible.

(282) (P. Giblin [**14**]) Assume that q is a prime factor of n. Since n is odd, it follows that q is odd. We will first prove that $p | (q-1)$. Observe that $4^p = 2^{n-1} \equiv 1 \pmod{n}$, so that $4^p \equiv 1 \pmod{q}$. It follows that r, the order of 4 modulo q, is a factor of p; we therefore have that $r = 1$ or $r = p$. If $r = 1$, then $4 \equiv 1 \pmod{q}$, which implies that $q = 3$, in which case $3 | n$, which contradicts the fact that n is not a multiple of 3. Hence, $r = p$, which implies that $p | q - 1$, as required. We shall finally show that $n = q$. Since $q - 1 > p$, we have $q \geq p - 1 > n/2 \geq \sqrt{n}$, because $n \geq 4$. We have thus shown that each prime factor q of n is larger than $\sqrt{n}$, which is impossible unless n itself is a prime number.

(283) (Francesco Sica) Assume that $p^k \| a - b$. Then there exists a positive integer c which is not divisible by p and such that

$$b = a + cp^k.$$

We then have

$$\begin{aligned} b^p = (a+cp^k)^p &= \sum_{i=0}^{p} \binom{p}{i} a^i c^{p-i} p^{k(p-i)} \\ &\equiv a^p + pa^{p-1}cp^k + \frac{p(p-1)}{2} a^{p-2}c^2p^{2k} \pmod{p^{k+2}} \\ &\equiv a^p + a^{p-1}cp^{k+1} \pmod{p^{k+2}}. \end{aligned}$$

We have thus established that

$$(**) \qquad a^p - b^p \equiv a^{p-1}cp^{k+1} \pmod{p^{k+2}},$$

hence, in particular $(*)$. Moreover, it follows from $(**)$ that p^{k+2} divides $a^p - b^p + a^{p-1}cp^{k+1}$, but, since $p \nmid a^{p-1}c$, it follows that p^{k+2} divides exactly $a^p - b^p$, as required.

(284) The answer is NO. If $p = 2$, then $p|1$, a contradiction. Hence, $p \geq 3$. If δ is even, then $p^\delta + 1 \equiv 1 + 1 = 2 \pmod 4$ while $2^\nu \equiv 0 \pmod 4$, a contradiction, while if δ is odd, then

$$2^\nu = p^\delta + 1 = (p+1)(p^{\delta-1} - p^{\delta-2} + \cdots - p + 1) = (p+1)Q,$$

where $Q > 1$ is odd, which is nonsense.

(285) If a solution $\{m, n\}$ exists, then it is clear that $n > 1$ and that $m > n > 1$, in which case

$$1 + n = m^2 - n^2 = (m-n)(m+n) \geq m + n > 1 + n,$$

which is nonsense.

Second solution. Assume that $1 + n + n^2 = m^2$ with $n > 1$, $m > 1$. We then have $4 + 4n + 4n^2 = 4m^2$ and therefore $(2n+1)^2 + 3 = (2m)^2$. But, the only squares which differ by 3 are 1 and 4. This implies that $n = 0$, which contradicts the fact that $n > 1$.

(286) Let (1) be the equation for which we seek the solutions and let $\{p, q\}$ be a solution. First of all, it is clear that

$$(2) \qquad p^2 + 1 < q < p^2 + p.$$

Indeed, these inequalities are consequences of the following two inequalities:

$$\begin{aligned} (p^2+1)^2 &= p^4 + 2p^2 + 1 < p^4 + p^3 + p^2 + p + 1 = q^2 \\ (p^2+p)^2 &= p^4 + 2p^3 + p^2 > p^4 + p^3 + p^2 + p + 1 = q^2. \end{aligned}$$

But it follows from (1) that $p(1 + p + p^2 + p^3) = q^2 - 1 = (q-1)(q+1)$ and this shows that $p|(q-1)(q+1)$. It follows that $p|(q-1)$ or $p|(q+1)$.

If $p|(q-1)$, then it follows from (2) that

$$p^2 < q - 1 < p^2 + p - 1, \text{ and therefore } p^2 + 1 \leq q - 1 \leq p^2 + p - 2.$$

Observing that the interval $[p^2 + 1, p^2 + p - 2]$ contains no multiple of p, it is therefore impossible that $p|(q-1)$.

If $p|(q+1)$, then, from (2), we have

$$p^2 + 2 < q + 1 < p^2 + p + 1, \text{ and therefore } p^2 + 3 \leq q + 1 \leq p^2 + p.$$

The fact that the only multiple of p in the interval $[p^2+3, p^2+p]$ is p^2+p implies that $q+1 = p^2+p$; that is $q = p^2+p-1$. Substituting this value of q in (1), we obtain

$$\begin{aligned} 1+p+p^2+p^3+p^4 &= (p^2+p-1)^2, \\ p^3-2p^2-3p &= 0, \\ p^2-2p-3 &= 0, \\ (p-3)(p+1) &= 0, \end{aligned}$$

an equation that implies that $p = 3$, which gives $q = 11$.

(287) It is easy to establish that for each integer $m \not\equiv 0 \pmod 7$, we have $m^3 \equiv +1$ or $-1 \pmod 7$. On the other hand, by hypothesis we have

$$(*) \qquad x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 \equiv 0 \pmod 7.$$

Therefore, none of the x_i's is divisible by 7, and the congruence $(*)$ is impossible. Thus the result.

(288) (*AMM, Vol. 81, 1974, p. 172*). If $p = 2$, then $2^2 + 3^2 = 13$ is not a power of an integer larger than 1. Assume that p is odd; then using Problem 8,

$$2^p + 3^p = (2+3)\sum_{k=0}^{p-1}(-1)^k 2^{p-1-k}\, 3^k,$$

and since $3 \equiv -2 \pmod 5$, we have that

$$\sum_{k=0}^{p-1}(-1)^k 2^{p-1-k} 3^k \equiv \sum_{k=0}^{p-1} 2^{p-1} = 2^{p-1}p \pmod 5.$$

If $p \neq 5$, then $2^{p-1}p \not\equiv 0 \pmod p$ and therefore $2^p + 3^p = 5k$, for $k \not\equiv 0 \pmod 5$. Hence, $2^p + 3^p$ is never the power of an integer. On the other hand, for $p = 5$, $2^5 + 3^5 = 275$ is obviously not a power of an integer. Hence, the result.

(289) Letting $n = 6k + r$, $k \in \mathbb{N}$, $0 \leq r \leq 5$, then

$$1^n + 2^n + 3^n + 4^n + 5^n + 6^n \equiv 1^r + 2^r + 3^r + 4^r + 5^r + 6^r \pmod 7.$$

Hence, if $r = 0$, we have $1^n + 2^n + 3^n + 4^n + 5^n + 6^n \equiv 6 \pmod 7$, while for $r = 1, 2, 3, 4, 5$ we have $1^n + 2^n + 3^n + 4^n + 5^n + 6^n \equiv 0 \pmod 7$. Hence, the result.

(290) The answer is YES. Indeed, by hypothesis $(n, 100) = 1$; we may therefore use Euler's Theorem and obtain that $n^{\phi(100)} \equiv 1 \pmod{100}$. Hence, $n^{40} \equiv 1 \pmod{100}$, which means that the last two digits of $n^{400} = (n^{40})^{10}$ are indeed 0 and 1.

(291) We need to examine to what values the quantities 4^0, 4^1, $4^2, \ldots$ are congruent modulo 10. But we easily verify that each of these numbers is congruent to 1, 4 or 6.

(292) We must first show that $(n+1)^3 - n^3 \not\equiv 0 \pmod 3$ for each integer $n \geq 1$. But this quantity is equal to $3n^2 + 3n + 1$, which is congruent to 1 modulo 3, thus the result. Similarly, we prove that $(n+1)^3 - n^3 \not\equiv 0 \pmod 5$, for each integer $n \geq 1$. Indeed, it is enough to consider $n = 5m + r$, $r = 0, 1, 2, 3, 4$.

(293) This is true since

$$2(32)^n + 5^2 5^n \equiv 2 \cdot 5^n - 2 \cdot 5^n \equiv 0 \pmod{27}.$$

(294) Since $98^2 \equiv -169 \equiv -13^2 \pmod{337}$, the result is immediate.

(295) Since $19^{19} \equiv 9 \pmod{10}$, then $19^{19^{19}} = 19^{9+10k}$ for a certain integer k. We thus obtain

$$19^{9+10k} \equiv 79 \pmod{100},$$

which implies that the last two digits are 7 and 9.

(296) We have $280 = 2^3 \cdot 5 \cdot 7$ and since both a and b are odd, then $a^2 \equiv 1 \pmod 8$ and $b^2 \equiv 1 \pmod 8$. Therefore, $a^{12} \equiv 1 \equiv b^{12} \pmod 8$. Using Fermat's Little Theorem, $a^4 \equiv b^4 \equiv 1 \pmod 5$ and therefore $a^{12} \equiv b^{12} \pmod 5$. Similarly, Fermat's Little Theorem allows one to obtain $a^{12} \equiv b^{12} \pmod 7$. The result then follows by combining these congruences.

(297) We only need to observe that $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ and use Fermat's Little Theorem five times.

(298) The required integer is 21424. Indeed, we must solve the congruences $n \equiv 4 \pmod{12}$, $n \equiv 4 \pmod{17}$, $n \equiv 4 \pmod{45}$, $n \equiv 4 \pmod{70}$. The first two are equivalent to $n \equiv 4 \pmod{204}$, while the last two give $n \equiv 4 \pmod{1530}$. Finally, the solution of these last two congruences is given by $n \equiv 4 \pmod{21420}$, which gives the result.

(299) The answer is YES. From Fermat's Little Theorem, $n^{13} \equiv n^7 \equiv n \pmod 7$, $n^{11} \equiv n^5 \pmod 7$ and $n^7 \equiv n \pmod 7$, so that the polynomial is congruent to $3n + 4n^5 + n + 3n^5 + 3n = 7n + 7n^5 \equiv 0 \pmod 7$. Thus the result.

(300) Since

$$\binom{2p}{p} = \frac{2p(2p-1)(2p-2)\cdots(2p-(p-1))}{p!}$$

and since

$$(2p-1)(2p-2)\cdots(2p-(p-1)) \equiv (p-1)! \pmod p,$$

it is clear that

$$\binom{2p}{p} \equiv 2\frac{(p-1)!}{(p-1)!} \equiv 2 \pmod p.$$

(301) It is clear that $7|n =$ "abc" if and only if

$$n = 100a + 10b + c \equiv 2a + 3b + c \equiv 0 \pmod 7,$$

and the result follows.

(302) It is clear that "$abcabc$" ="abc"$\cdot 1001$. But $13|1001$, thus obtaining the result.

(303) Since $2^{561} \equiv (-1)^{561} = -1 \equiv 2 \pmod 3$ and since from Fermat's Little Theorem, $2^{561} = (2^{10})^{56} \cdot 2 \equiv 2 \pmod{11}$ and $2^{561} = (2^{16})^3 \cdot 5 \cdot 2 \equiv 2 \pmod{17}$, we conclude that $2^{561} \equiv 2 \pmod{561}$. The second part can be obtained in a similar manner.

(304) Since

$$\frac{n^{13}}{5} + \frac{n^{13}}{7} = \frac{12}{35}n^{13}$$

and since we have $n^{13} \equiv n \pmod 5$ and $n^{13} \equiv n \pmod 7$, then

$$\frac{12}{35}n^{13} + \frac{23}{35}n = \frac{n^{13}}{5} + \frac{n^{13}}{7} + \frac{23}{35}n = \frac{n^{13}-n}{5} + \frac{n^{13}-n}{7} + n,$$

a number which is an integer for each $n \in \mathbb{N}$.

(305) The answer is YES. The case $n = 1$ implies that we can choose $r = 431/481$. We will show that for this rational number r, the number in the statement is an integer for each $n \in \mathbb{N}$, $(n, 481) = 1$. But this number is an integer when $(n, 481) = 1$ if and only if

$$n\left(\frac{50}{481}n^{36} + \frac{431}{481}\right) = \frac{50}{481}n^{37} + \frac{431}{481}n$$

is an integer. Since $481 = 13 \cdot 37$ and since for each $n \in \mathbb{N}$,

$$n^{37} \equiv n \pmod{37} \quad \text{and} \quad n^{13} \equiv n \pmod{13},$$

we conclude that the number $\frac{50}{481}n^{36} + r$ is an integer for all $n \in \mathbb{N}$ when $r = 431/481$.

(306) If $p = 3$, then considering the numbers 111, 111 111, 111 111 111, ..., that is all the numbers containing 3, 6, 9, ... times the digit "1", we obtain infinitely many numbers of the required form. Let $p \geq 7$, p prime. An integer N made up entirely of "1" can be written as $N = (10^n - 1)/9$. But from Fermat's Little Theorem, $10^{p-1} \equiv 1 \pmod p$, which means that $10^{m(p-1)} \equiv 1 \pmod p$ for $m = 1, 2, 3, \ldots$. Since $p \neq 3$, this means that $p|(10^{m(p-1)} - 1)/9$, for $m = 0, 1, 2, 3, \ldots$, and the result follows.

(307) Indeed, we easily check that $2^{340} \equiv 1 \pmod{341}$, while $n = 341 = 11 \cdot 31$ is not prime.

(308) (*AMM, Vol. 67, 1960, p. 923*). From Fermat's Little Theorem, it follows that $b^3 \equiv b \pmod 3$ and $b^3 \equiv b \pmod 2$ and therefore that $b^3 \equiv b \pmod 6$. Since $b^3 - b = b(b^2 - 1)$, we have

$$b^{p-1} - 1 = (b^2 - 1)(b^{p-3} + b^{p-5} + \cdots + b^2 + 1)$$

and therefore $b^3 - b$ is a factor of $b^p - b$, in which case $b^p - b \equiv 0 \pmod 6$. Fermat's Little Theorem allows one to write $b^p - b \equiv 0 \pmod p$, and since $(6, p) = 1$, we have $b^p - b \equiv 0 \pmod{6p}$. Similarly, we obtain $a^p - a \equiv 0 \pmod{6p}$. Combining the congruences $ab^p - ab \equiv 0 \pmod{6p}$ and $-ba^p + ab \equiv 0 \pmod{6p}$ then yields the result.

(309) The answer is NOT ALWAYS. Assume that n is an odd integer. Since $1 + 2 + \cdots + (n-1) = n(n-1)/2$ and since n is odd, it follows that $(n-1)/2$ is an integer and consequently the congruence is true.

Assume that n is an even integer. Letting $n = 2m$, then

$$1 + 2 + \cdots + (n-1) = m(2m-1) \not\equiv 0 \pmod{2m}.$$

(310) Using the formula $\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$ (see Problem 1), with $k = n-1$, we obtain that n must satisfy $n \equiv \pm 1 \pmod 6$.

(311) The answer is YES. Since $1^3 + 2^3 + \cdots + (n-1)^3 = n \cdot n(n-1)^2/4$ (see Problem 1), it follows that the congruence is true if $n^3 - 2n^2 + n \equiv 0 \pmod 4$. Setting $n = 4m + r$, $0 \leq r \leq 3$, we obtain that the congruence is true except in the case $n = 4m + 2$.

(312) Since

$$\begin{aligned} 5^n &= (4+1)^n \\ &= 4^n + \binom{n}{1}4^{n-1} + \cdots + \binom{n}{n-3}4^3 + \binom{n}{n-2}4^2 + \binom{n}{n-1}4 + 1, \end{aligned}$$

it follows that

$$5^n \equiv 4n + 1 \pmod{16}$$

and that

$$5^n \equiv 1 + 4n + 8n(n-1) \pmod{64}.$$

(313) If we can show that, for each integer $k \geq 1$, we have

$$5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}},$$

then the result will follow. But this last congruence can easily be obtained by induction on k. For $k = 1$, the result is immediate. Assuming that the congruence is true for k, that is that $5^{2^k} = 1 + 2^{k+2} + M2^{k+3}$ for a certain positive integer M, then squaring each side of this last equation, we obtain

$$5^{2^{k+1}} \equiv 1 + 2^{k+3} \pmod{2^{k+4}}.$$

The general case can be handled essentially in the same manner.

(314) This follows from the fact that the given expression is equal to

$$\frac{n^5 - n}{5} + \frac{n^3 - n}{3} + n,$$

which using Fermat's Little Theorem is easily seen to be an integer.

(315) It is clear that $x \equiv 0 \pmod{13}$ is not a solution. So let $1 \leq x \leq 12$. Then, from Fermat's Little Theorem, we have that $x^{12} \equiv 1 \pmod{13}$ and this is why $x^{24} \equiv 1 \pmod{13}$. The congruence to be solved can therefore be reduced to $7x \equiv 1 \pmod{13}$, which leads to the solution $x \equiv 2 \pmod{13}$.

(316) The seven pairs are $\{2,9\}$, $\{3,6\}$, $\{4,13\}$, $\{5,7\}$, $\{10,12\}$, $\{11,14\}$ and $\{8,15\}$.

(317) Since $(m_i, m_j) = 1$ for $i \neq j$, it follows from Euler's Theorem that $m_i^{\phi(m_j)} \equiv 1 \pmod{m_j}$. Since the function ϕ is a multiplicative function, we have $m_i^{\phi(m)/\phi(m_i)} \equiv 1 \pmod{m_j}$ for $i \neq j$. On the other hand, $m_j^{\phi(m)/\phi(m_j)} \equiv 0 \pmod{m_j}$, so that for $j = 1, 2, \ldots, r$, we obtain

$$m_1^{\phi(m)/\phi(m_1)} + m_2^{\phi(m)/\phi(m_2)} + \cdots + m_r^{\phi(m)/\phi(m_r)} \equiv r - 1 \pmod{m_j}.$$

Since the integers m_j are relatively prime, the result follows.

(318) From Wilson's Theorem,

$$\begin{aligned} (p-1)! &= (p-1)\cdots(p-(k-1))(p-k)! \\ &\equiv (-1)^{k-1}(k-1)!(p-k)! \equiv -1 \pmod{p}, \end{aligned}$$

and multiplying by $(-1)^{k-1}$, the result follows.

(319) The answer is YES to both questions. We first use Fermat's Little Theorem for p and then for q, in which case we obtain

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{p}, \quad p^{q-1} + q^{p-1} \equiv 1 \pmod{q},$$

since $(p, q) = 1$, and the result follows.

To prove the second part, we call upon Euler's Theorem.

(320) We have

$$3^{2n+2} = 9(9^n) = 9(8+1)^n = 9(8^n + n8^{n-1} + \cdots + 8n + 1)$$
$$= 9\left(8^n + n8^{n-1} + \cdots + 8^2\frac{n(n-1)}{2}\right) + 9(8n+1),$$

and this is why

$$3^{2n+2} \equiv 72n + 9 \equiv 8n + 9 \pmod{64}.$$

(321) We will prove that the required GCD is equal to p. First of all, from Wilson's Theorem, it follows that for p prime, $(p-1)! \equiv -1 \pmod{p}$, a congruence which can be written as $(p-2)!\,(p-1) \equiv -1 \pmod{p}$, implying that $(p-2)! \equiv 1 \pmod{p}$ and therefore that $p|\,((p-2)!-1)$. It remains to show that if $2 \leq k \leq p-1$, then k does not divide $(p-2)!-1$. But if $2 \leq k \leq p-2$ and $k|(p-2)!-1$, we obtain that $k|1$, a contradiction. It remains to consider the case when $(p-1)|\,((p-2)!-1)$. Since p is a prime number, $p-1$ is an even number, and therefore, using Problem 180, $(p-1)|(p-2)!$ except for $p-1=4$, that is when $p=5$. Hence, $(p-1) \not| \,((p-2)!-1)$ for $p \geq 5$.

(322) This follows from the fact that dividing by 7 the number 5^{6614} leaves 4 as a remainder, while dividing by 7 the number 12^{857} leaves 3 as a remainder. Indeed,

$$5^{6614} \equiv (-2)^{6614} = 2^{6614} = 2^{3\cdot 2204+2} = 8^{2204}\cdot 4 \equiv 4 \pmod{7},$$

$$12^{857} \equiv 5^{857} = 5^{6\cdot 142+5} \equiv 1^{142}\cdot 5^5 \equiv (-2)^5 = -32 \equiv 3 \pmod{7}.$$

(323) (a) Since $10 \equiv 1 \pmod{3}$, we have

$$3|N \iff a_n 10^n + \cdots + a_1 10 + a_0 \equiv 0 \pmod{3}$$
$$\iff a_n + \cdots + a_1 + a_0 \equiv 0 \pmod{3}.$$

(b) We have

$$4|N \iff a_n 10^n + \cdots + a_1 10 + a_0 \equiv 0 \pmod{4}$$
$$\iff 10a_1 + a_0 \equiv 0 \pmod{4},$$

since $10^j \equiv 0 \pmod{4}$ for each $j \geq 2$.

(c) We have

$$6|N \iff a_n 10^n + \cdots + a_1 10 + a_0 \equiv 0 \pmod{6}$$
$$\iff 4(a_n + \cdots + a_2 + a_1) + a_0 \equiv 0 \pmod{6},$$
$$\iff 4(a_n + \cdots + a_2 + a_1 + a_0) \equiv 3a_0 \pmod{6},$$

since $10^j - 4 \equiv 0 \pmod{6}$ for each $j \geq 1$; indeed, $10^j - 4 = 999\ldots96$, a number which is even and divisible by 3.

(d) If N has three digits (that is $n=2$), then the result is obvious. We examine the case $n=3$, so that $N = 1000a_3 + 100a_2 + 10a_1 + a_0$. We must prove that

$$1000a_3 + 100a_2 + 10a_1 + a_0 \equiv 0 \pmod{7}$$
$$\iff 100a_2 + 10a_1 + a_0 - a_3 \equiv 0 \pmod{7}.$$

This boils down to proving that

$$1001a_3 + 100a_2 + 10a_1 + a_0 - a_3 \equiv 0 \pmod 7$$
$$\iff 100a_2 + 10a_1 + a_0 - a_3 \equiv 0 \pmod 7,$$

an equivalence which is easily verified since $7|1001$.
To prove the case $n = 4$, we proceed essentially in the same manner, this time using the identity

$$10^4a_4 + 10^3a_3 + 10^2a_2 + 10a_1 + a_0$$
$$= 10\,010a_4 + 1001a_3 + 100a_2 + 10a_1 + a_0 - (10a_4 + a_3)$$

and by observing that $7|10\,010$. The same argument works also for the case $n = 5$.
If $n \geq 6$, we use the same argument by also observing that $10^6 - 1 = (10^3 - 1)(10^3 + 1)$, where $7|10^3 + 1$; that $10^7 - 10 = 10(10^6 - 1)$; that $10^8 - 100 = 10^2(10^6 - 1)$; and so on.

(e) We have

$$\begin{aligned} 8|N &\iff a_n10^n + \cdots + a_110 + a_0 \equiv 0 \pmod 8 \\ &\iff 100a_2 + 10a_1 + a_0 \equiv 0 \pmod 8, \end{aligned}$$

since $10^j \equiv 0 \pmod 8$ for each integer $j \geq 3$.

(f) Since $10 \equiv 1 \pmod 9$, it follows that

$$\begin{aligned} 9|N &\iff a_n10^n + \cdots + a_110 + a_0 \equiv 0 \pmod 9 \\ &\iff a_n + \cdots + a_1 + a_0 \equiv 0 \pmod 9. \end{aligned}$$

(g) We have

$$\begin{aligned} 11|N &\iff a_n10^n + \cdots + a_110 + a_0 \equiv 0 \pmod{11} \\ &\iff a_n(11-1)^n + a_{n-1}(11-1)^{n-1} + \cdots \\ &\qquad + a_1(11-1) + a_0 \equiv 0 \pmod{11} \\ &\iff (-1)^n a_n + (-1)^{n-1}a_{n-1} + \cdots \\ &\qquad + a_2 - a_1 + a_0 \equiv 0 \pmod{11} \\ &\iff (-1)^n \left\{(-1)^n a_n + (-1)^{n-1}a_{n-1} + \cdots \right. \\ &\qquad \left. + a_2 - a_1 + a_0\right\} \equiv 0 \pmod{11} \\ &\iff a_n - a_{n-1} + \cdots + (-1)^{n+1}a_1 + (-1)^n a_0 \\ &\qquad \equiv 0 \pmod{11}, \end{aligned}$$

and the result follows.

(324) Observe that $168 = 8 \cdot 3 \cdot 7$. Since $8|$"$770ab45c$", it follows that using Problem 215 we have $8|$"$45c$" and then $c = 6$. Similarly, $3|$"$770ab456$" implies $a + b \equiv 1 \pmod 3$, and $7|$"$770ab456$" implies (using Problem 323 (e)) that $456 - (10a + b) + 77 \equiv 0 \pmod 7$, that is $3a + b \equiv 1 \pmod 7$. Therefore, $a + b = 1$ and $3a + b = 1$, which allows us to conclude that $a = 0$ and $b = 1$. The three required numbers are therefore $a = 0$, $b = 1$ and $c = 6$.

(325) Since $(a, m) = 1$, using Euler's Theorem, we have

$$a^{\phi(m)} - 1 \equiv 0 \pmod m.$$

But

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

and since $(a-1, m) = 1$, the result follows.

(326) If $p|a$, then $a^{(p-1)!+1} = a \cdot a^{(p-1)!} \equiv 0 \equiv a \pmod{p}$. If $p \nmid a$, then $(a, p) = 1$, and it follows from Fermat's Little Theorem that $a^{p-1} \equiv 1 \pmod{p}$ and therefore that $a^{(p-1)!} = \left(a^{p-1}\right)^{(p-2)!} \equiv 1 \pmod{p}$, in which case $a^{(p-1)!+1} \equiv a \pmod{p}$, as required.

(327) Using Fermat's Little Theorem,

$$1^{p-1} + \cdots + (p-1)^{p-1} \equiv \underbrace{1 + \cdots + 1}_{p-1} = p - 1 \equiv -1 \pmod{p}.$$

(328) Using Fermat's Little Theorem, we have $a^p \equiv a \pmod{p}$ for each positive integer a. Hence,

$$1^p + 2^p + \cdots + (p-1)^p \equiv 1 + 2 + \cdots + p = p(p+1)/2 \equiv 0 \pmod{p},$$

since $p + 1$ is an even number.

(329) This is a consequence of the congruence $(k-1)!(p-k)! \equiv (-1)^k \pmod{p}$ (see Problem 318) and Fermat's Little Theorem, because

$$\begin{aligned}\sum_{k=1}^{p-1} &(k-1)!(p-k)!k^{p-1} \\ &\equiv -1^{p-1} + 2^{p-1} - 3^{p-1} + \cdots - (p-2)^{p-1} + (p-1)^{p-1} \\ &\equiv -1 + 1 - 1 + \cdots - 1 + 1 = 0 \pmod{p}.\end{aligned}$$

(330) From Wilson's Theorem, we have $(4n)! \equiv -1 \pmod{p}$, in which case

$$(4n)(4n-1)\cdots[4n-(2n-1)](2n)! \equiv -1 \pmod{p}.$$

Since $4n = p - 1 \equiv -1 \pmod{p}$, we have $4n - 1 \equiv -2 \pmod{p}$ and therefore $4n - 2 = p - 3 \equiv -2 \pmod{p}$, so that $4n - (2n-1) \equiv -2n \pmod{p}$, and the result follows.

For the generalization, we have from Wilson's Theorem $(m+n)! \equiv -1 \pmod{p}$, and therefore

$$(*) \qquad (m+n)(m+n-1)\cdots[m+n-(n-1)]m! \equiv -1 \pmod{p}.$$

We have $m + n = p - 1 \equiv -1 \pmod{p}$ and $m + n - 1 \equiv -2 \pmod{p}$, and so on, until we obtain $m + n - (n-1) \equiv -n \pmod{p}$. Then, substituting in $(*)$, we find

$$(**) \qquad (-1)^n m!n! \equiv -1 \pmod{p}.$$

Since $m + n$ is even, the second relation of the problem is proved. Finally, the last congruence can be obtained by setting $m = n = \frac{p-1}{2}$ in $(**)$.

(331) From Wilson's Theorem, n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$. Therefore,

$$-1 \equiv (n-1)! = (n-1)(n-2)(n-3)! \equiv 2(n-3)! \pmod{n},$$

and the result follows.

(332) This follows immediately from Fermat's Little Theorem and Wilson's Theorem. Indeed, $a^p \equiv a \pmod{p}$ and $a(p-1)! \equiv -a \pmod{p}$, allowing us to conclude that $a^p + a(p-1)! \equiv 0 \pmod{p}$.

(333) From Wilson's Theorem, $\dfrac{(n-1)!+1}{n}$ is an integer if and only if n is a prime number, in which case the sum appearing in the statement is equal to

$$\sum_{p\le x}(\pm 1)^2 = \sum_{p\le x} 1 = \pi(x),$$

as required.

(334) If $d=(r,s)$, then $r=dr_1$ and $s=ds_1$. It is clear that

$$(a^d)^{r/d} \equiv 1 \pmod{m_1} \quad \text{and} \quad (a^d)^{s/d} \equiv 1 \pmod{m_2}.$$

Therefore,

$$a^{[r,s]} = (a^d)^{(r/d)(s/d)} \equiv 1^{(s/d)} \equiv 1 \pmod{m_1},$$

$$a^{[r,s]} = (a^d)^{(s/d)(r/d)} \equiv 1^{(r/d)} \equiv 1 \pmod{m_2},$$

and the result follows.

(335) Let $m = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$. If $(a,q_i)=1$, $1 \le i \le r$, then $a^{\phi(q_i^{\alpha_i})} \equiv 1 \pmod{q_i^{\alpha_i}}$. Now, since $q_i^{\alpha_i} | m$ implies $\phi(q_i^{\alpha_i}) | \phi(m)$, then $a^{\phi(m)} \equiv 1 \pmod{q_i^{\alpha_i}}$. If $a>0$ and $q \ge 2$ are positive integers, then on the one hand, we have $q^{a-1} \ge a$ (we can prove this by induction on a) and on the other hand, for $i=1,2,\ldots,r$, we have $q_i^{\alpha_i - 1} | m$ and $q_i^{\alpha_i - 1} | \phi(m)$. Therefore,

$$(*) \qquad q_i^{\alpha_i - 1} | m - \phi(m).$$

Since $m-\phi(m) > 0$, then for $m>1$, it follows from $(*)$ that

$$m - \phi(m) \ge q_i^{\alpha_i - 1} \ge \alpha_i.$$

Therefore, in the case $(a,q_i)>1$, that is $q_i | a$, we have

$$q_i^{\alpha_i} | q_i^{m-\phi(m)} | a^{m-\phi(m)}.$$

It follows that for each positive integer a, the relation

$$q_i^{\alpha_i} | a^{m-\phi(m)} (a^{\phi(m)} - 1)$$

is true for $i=1,2,\ldots,r$ and therefore that $m | a^{m-\phi(m)}$.

(336) Let $a_1, a_2, \ldots, a_m$ be a complete residue system modulo m. Since $(m+1)/2$ is a positive integer, say $(m+1)/2 = k$, it follows that

$$\sum_{i=1}^{m} a_i \equiv \sum_{i=1}^{m} i \equiv \frac{m(m+1)}{2} \equiv mk \equiv 0 \pmod{m},$$

as was to be shown.

(337) Let $E = \{x_1, x_2, \ldots, x_n\}$ be a complete residue system. The set E' contains the same number of elements as E and for $x_i, x_j \in E$, $i \ne j$, we have $x_i \not\equiv x_j$. If

$$ax_i + b \equiv ax_j + b \pmod{m},$$

then $ax_i \equiv ax_j \pmod{m}$ and therefore $x_i \equiv x_j \pmod{m}$, which contradicts our hypothesis.

(338) The answer is YES. Indeed, the set $\{6, 12, 18, 24, 30, 36\}$ is a reduced residue system modulo 7.

(339) We must show that

$$\sum_{\substack{k\le m\\(k,m)=1}} k \equiv 0 \pmod{m}.$$

Let $a_1, a_2, \ldots, a_{\phi(m)}$ be integers smaller than m and relatively prime to m. Since $(k,m)=1 \iff (m-k,m)=1$, we have

$$\begin{aligned} a_1 + a_2 + \cdots + a_{\phi(m)} &= (m-a_1) + (m-a_2) + \cdots + (m-a_{\phi(m)}) \\ &= m\phi(m) - (a_1 + a_2 + \cdots + a_{\phi(m)}). \end{aligned}$$

Since $\phi(m)$ is an even integer when $m > 2$, we then have

$$\sum_{\substack{k\le m\\(k,m)=1}} k = \frac{\phi(m)}{2} m \equiv 0 \pmod{m}.$$

(340) The result follows immediately from Wilson's Theorem since $r_1 r_2 \cdots r_{p-1} \equiv (p-1)! \pmod{p}$.

(341) The set $\{1,3,7,9\}$ is a reduced residue system modulo 10. However,

$$E' = \{3x+2 \mid x \in E\} = \{5, 11, 23, 29\}$$

is not a reduced residue system modulo 10, since $(5,10) \neq 1$.

(342) (*MMAG, Vol. 64, 1991, p. 63*). The only solution is $(x,y,z) = (2,3,5)$. First of all, we observe that $(x,y) = (x,z) = (y,z) = 1$. Then, $2 \le x < y < z$, and combining the three given congruences we obtain

$$xy + xz + yz - 1 \equiv 0 \pmod{x, y \text{ and } z}.$$

Since x, y and z are pairwise coprime, we have

$$xy + xz + yz - 1 \equiv 0 \pmod{xyz}.$$

It follows that $xy + xz + yz - 1 = k(xyz)$ for some integer $k \ge 1$. Dividing by xyz, we obtain that

$$\frac{1}{z} + \frac{1}{y} + \frac{1}{x} = \frac{1}{xyz} + k > 1.$$

Since $x < y < z$, it follows that

$$(*) \qquad 1 < \frac{1}{x} + \frac{1}{y} + \frac{1}{z} < \frac{3}{x}$$

and this is why $x = 2$. In this case, the inequalities give

$$\frac{1}{2} < \frac{1}{y} + \frac{1}{z} < \frac{2}{y},$$

which implies that $y = 3$. It follows that the only possible values of z are 4 and 5. Hence, for $2 \le x < y < z$, the solutions are $(x,y,z) = (2,3,4)$ and $(2,3,5)$. Since 2 and 4 are not relatively prime, the only solution is $(x,y,z) = (2,3,5)$.

(343) Let p_r stand for the r–th prime number. For each integer i, $1 \leq i \leq n$, let $m_i = p_{(i-1)k+1} \cdot p_{(i-1)k+2} \cdot p_{(i-1)k+3} \cdots p_{ik-1} \cdot p_{ik}$, and consider the system of congruences

$$\begin{cases} x \equiv -1 \pmod{m_1}, \\ x \equiv -2 \pmod{m_2}, \\ \quad \vdots \\ x \equiv -n \pmod{m_n}. \end{cases}$$

Since the m_i's are pairwise coprime, the Chinese Remainder Theorem guarantees a solution x_0. Then, $m_1|(x_0+1), \ldots, m_n|(x_0+n)$. Therefore, $x_0+1, x_0+2, \ldots, x_0+n$ is a sequence of n consecutive integers which are divisible by at least k prime numbers.

For the second part ($n = 4$ and $k = 1$), we must solve

$$\begin{cases} x \equiv -1 \pmod{3}, \\ x \equiv -2 \pmod{5}, \\ x \equiv -3 \pmod{7}, \\ x \equiv -4 \pmod{11}. \end{cases}$$

In this case, $x \equiv 788 \pmod{1155}$ and therefore $x_0 = 788$. The four numbers are therefore 789, 790, 791 and 792.

(344) We must solve the system

$$\begin{cases} x \equiv 1 \pmod{3}, \\ x \equiv 2 \pmod{4}, \\ x \equiv 3 \pmod{5}. \end{cases}$$

Using the Chinese Remainder Theorem, we find that $x \equiv 58 \pmod{60}$. The required positive integers are therefore the numbers $60j + 58$, with $j = 0, 1, 2, \ldots$.

(345) We must solve the system

$$\begin{cases} a \equiv 0 \pmod{2}, \\ a+1 \equiv 0 \pmod{3}, \\ a+2 \equiv 0 \pmod{4}, \\ a+3 \equiv 0 \pmod{5}, \\ a+4 \equiv 0 \pmod{6}. \end{cases}$$

This system is equivalent to:

$$\begin{cases} a \equiv 2 \pmod{2}, \\ a \equiv 2 \pmod{3}, \\ a \equiv 2 \pmod{4}, \\ a \equiv 2 \pmod{5}, \\ a \equiv 2 \pmod{6}. \end{cases}$$

Since $[2, 3, 4, 5, 6] = 60$, we have $a \equiv 2 \pmod{60}$. Hence, the smallest integer a is 62.

(346) We obtain

$$\frac{1}{3} = 0.\overline{3}, \quad \frac{1}{3^2} = 0.\overline{1} \quad \text{of period 1,}$$

$1/3^3 = 0.\overline{037}$ of period 3, $1/3^4 = 0.\overline{012345679}$ of period 9. However,

$$\frac{1}{7} = 0.\overline{142857} \quad \text{is of period 6,}$$

and

$$\frac{1}{7^2} = 0.\overline{020408163265306122448979591836734693877551}$$

is of period 42 ($= 6 \cdot 7$). On the other hand, the period of $1/7^3$ is $6 \cdot 7 \cdot 7$. It seems reasonable to make the following conjectures:

- Let p be a prime number such that $(p, 30) = 1$; if $1/p$ is of period m, then $1/p^n$ is of period mp^{n-1}.
- For $n \geq 2$, $1/3^n$ is of period 3^{n-2}.

(347) (*TYCM, Vol. 28, no. 4, 1997, p. 320*). Assume that the decimal expansion of a/b is formed by the repetition of the block $B = ab$ of length $n \geq 1$. Then,

$$\frac{a}{b} = 0.BBB\ldots = \frac{B}{10^n - 1} = \frac{ab}{10^n - 1},$$

so that $b^2 = 10^n - 1$. Hence, for $n \geq 1$, b must be an odd integer. If $n > 1$, then $b^2 \equiv 1 \pmod 4$ and therefore $10^n - 1 \equiv 1 \pmod 4$, which is impossible. Hence, $n = 1$ and $b = 3$, and it follows that the only positive rational numbers having the required property are $1/3$ and $2/3$.

(348) First assume that $10^h \equiv 1 \pmod n$, that is that there exists an integer k such that $10^h = 1 + kn$. Then, for each fraction m/n, we have

$$10^h \frac{m}{n} = km + \frac{m}{n}. \tag{1}$$

Assume that $m/n = 0.a_1a_2a_3\ldots$; then equation (1) allows us to write

$$km + \frac{m}{n} = a_1a_2\ldots a_h.a_{h+1}a_{h+2}\ldots\ .$$

Equating integer parts and equating fractional parts shows that

$$km = a_1a_2\ldots a_h \tag{2}$$

and that

$$\frac{m}{n} = 0.a_{h+1}a_{h+2}\ldots\ . \tag{3}$$

But equation (3) confirms that the digits a_{h+1}, $a_{h+2}, \ldots$ are precisely the digits a_1, $a_2, \ldots$. This means that the expansion of m/n repeats itself after h digits and therefore that the period of m/n is h.

Conversely, if m/n is of period h, that is

$$\frac{m}{n} = 0.a_1a_2\ldots a_ha_1\ldots a_h\ldots,$$

then

$$10^h\frac{m}{n} - a_1a_2\ldots a_h = 0.a_1a_2\ldots a_h\ldots = \frac{m}{n}.$$

Consequently

$$\frac{(10^h - 1)m}{n} = a_1a_2\ldots a_h$$

is an integer. Since m and n are relatively prime, then we have $n|(10^h - 1)$.

Finally, assume that the period of m/n is h and that $10^{h_0} \equiv 1 \pmod n$. Then, m/n also has h_0 digits which repeat themselves and $h_0 \geq h$. In particular, h is the smallest positive integer satisfying $10^h \equiv 1 \pmod n$.

(349) In the solution of Problem 348, it is proved that $km = a_1a_2\ldots a_h$, which yields the result.

(350) This follows from the fact that $10^r(m/n) - (m/n) = a_1a_2 \dots a_r$.

(351) Let $N = 2^{n-1} + 2^{d-1} - 1$. We will show that $2^d - 1 \geq 3$ is a proper divisor of N, thereby showing that N is a composite number. Since $2^d - 1$ is an odd number, it is enough to show that $2^d - 1 | 2N$. But

$$\begin{aligned} 2N = 2^n + 2^d - 2 = 2^n - 1 + 2^d - 1 = (2^d)^{n/d} - 1 + 2^d - 1 \\ = (2^d - 1)(2^{d(\frac{n}{d}-1)} + 2^{d(\frac{n}{d}-2)} + \cdots + 2^d + 1) + (2^d - 1), \end{aligned}$$

which proves the result.

(352) Let $n = 2^q - 1$, where q is a prime, be such a number. Since q is odd and $\mu^2(n) = 0$, there exists an odd prime number p such that $p^2 | n$. We then have

$$2^q \equiv 1 \pmod{p^2}. \tag{1}$$

On the other hand, using Euler's Theorem, we have $2^{\phi(p^2)} \equiv 1 \pmod{p^2}$, so that

$$2^{p(p-1)} \equiv 1 \pmod{p^2}. \tag{2}$$

It follows from (1) and (2) that $q | p(p-1)$, which implies that $q | (p-1)$ (since if $q = p$, then $2^q \equiv 1 \pmod{q}$, contradicting the fact that $2^{q-1} \equiv 1 \pmod{q}$). Hence, there exists a positive integer a such that $p - 1 = aq$, which in light of (1) gives

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

thus establishing that p is a Wieferich prime.

REMARK: Only two Wieferich primes have been found so far, namely 1093 and 3511; it is known that there are no other such primes smaller than 1.25×10^{15}.

(353) We will show that the three smallest prime factors of n are 2, 3 and 11. First of all, it is clear that $2 | n$. To see that $3 | n$, it is sufficient to observe that

$$5^{96} - 7^{112} \equiv 2^{96} - 1^{112} \equiv (-1)^{96} - 1 = 1 - 1 = 0 \pmod{3}.$$

Clearly, 5 and 7 are not prime factors of n. Let us check if 11 divides n. By Fermat's Little Theorem, we have $5^{10} \equiv 1 \pmod{11}$ and $7^{10} \equiv 1 \pmod{11}$, so that

$$\begin{aligned} 5^{96} &\equiv 5^{90} \cdot 5^6 \equiv 1 \cdot 125^2 \equiv 4^2 = 16 \equiv 5 \pmod{11}, \\ 7^{112} &\equiv 7^{110} \cdot 7^2 \equiv 1 \cdot 49 = 49 \equiv 5 \pmod{11}. \end{aligned}$$

Combining these two congruences, we easily conclude that $11 | n$.

(354) Let $N = \dfrac{m^a}{2} + \dfrac{m}{2} - 1$. We will show that $m - 1 | N$. To do so, since $m - 1$ is odd, it is clear that we shall reach our goal if we can manage to show that $m - 1 | 2N$. But

$$\begin{aligned} 2N = m^a + m - 2 = m^a - 1 + m - 1 = (m-1)(m^{a-1} + m^{a-2} + \cdots \\ + m + 1) + (m - 1), \end{aligned}$$

which proves the result.