

MATHEMATICAL OLYMPIADS LECTURE NOTES

Congruences: Problem Solutions

Greg Gamble

Problems.

1. Show that: if the sum of the digits of a natural number N is divisible by 3 then $3 \mid N$.

Solution. Suppose the decimal representation of N is $a_k a_{k-1} \dots a_0$. Then

$$N = 10^k a_k + 10^{k-1} a_{k-1} + \dots + 10a_1 + a_0.$$

Now $10 \equiv 1 \pmod{3}$; so

$$10^\ell \equiv 1 \pmod{3},$$

for *any* natural number ℓ . So

$$\begin{aligned} N &= 10^k a_k + 10^{k-1} a_{k-1} + \dots + 10a_1 + a_0 \\ &\equiv a_k + a_{k-1} + \dots + a_1 + a_0 \pmod{3}. \end{aligned}$$

$$\therefore 3 \mid N \text{ if and only if } 3 \mid a_k + a_{k-1} + \dots + a_1 + a_0.$$

In other words, *3 divides N if and only if 3 divides the sum of the digits of N .*

2. Prove that for every integer n :

$$(i) 3 \mid n^3 - n; \quad (ii) 5 \mid n^5 - n; \quad (iii) 7 \mid n^7 - n; \quad (iv) 11 \mid n^{11} - n.$$

Solution.

- (i) 3 divides exactly one of the three consecutive integers $n - 1, n, n + 1$ and

$$n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1).$$

So $3 \mid n^3 - n$.

- (ii) 5 divides exactly one of the five consecutive integers $n - 2, n - 1, n, n + 1, n + 2$. In terms of congruences, exactly one of $n - 2, n - 1, n, n + 1, n + 2$ is *congruent to 0 modulo 5*. Thus:

$$\begin{aligned} n^5 - n &= n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = n(n - 1)(n + 1)(n^2 + 1) \\ &\equiv n(n - 1)(n + 1)(n^2 - 4) \pmod{5} \\ &\equiv n(n - 1)(n + 1)(n - 2)(n + 2) \pmod{5} \\ &\equiv 0 \pmod{5} \end{aligned}$$

So $5 \mid n^5 - n$.

- (iii) Exactly one of $n - 3, n - 2, n - 1, n, n + 1, n + 2, n + 3$ is *congruent to 0 modulo 7*. Thus:

$$\begin{aligned} n^7 - n &= n(n^6 - 1) = n(n^3 - 1)(n^3 + 1) \\ &= n(n - 1)(n^2 + n + 1)(n + 1)(n^2 - n + 1) \\ &\equiv n(n - 1)(n^2 + n - 6)(n + 1)(n^2 - n - 6) \pmod{7} \\ &\equiv n(n - 1)(n + 3)(n - 2)(n + 1)(n - 3)(n + 2) \pmod{7} \\ &\equiv 0 \pmod{7} \end{aligned}$$

So $7 \mid n^7 - n$.

- (iv) We could proceed via the methods above. Instead, let us observe that n is *congruent* to exactly one of $-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5$ *modulo* 11. Then, to show that 11 divides $n^{11} - n$ for any integer n , it is simply a matter of checking, for each congruence possibility of n , that $n^{11} - n$ (or a factor of $n^{11} - n$) is *congruent* to 0 *modulo* 11. Note, first that:

$$n^{11} - n = n(n^{10} - 1).$$

- If $n \equiv 0 \pmod{11}$ there is nothing to check since n is a factor of $n^{11} - n$.
- $(-1)^{10} - 1 \equiv 1^{10} - 1 \equiv 0 \pmod{11}$. So $n^{10} - 1 \equiv 0 \pmod{11}$ if $n \equiv \pm 1 \pmod{11}$.
- $2^5 = 32 \equiv -1 \pmod{11}$. So $2^{10} = (2^5)^2 \equiv 1 \pmod{11}$.
Hence $(-2)^{10} - 1 \equiv 2^{10} - 1 \equiv 0 \pmod{11}$.
So $n^{10} - 1 \equiv 0 \pmod{11}$ if $n \equiv \pm 2 \pmod{11}$.
- $3^5 = 243 \equiv 1 \pmod{11}$. So $3^{10} = (3^5)^2 \equiv 1 \pmod{11}$.
Hence $(-3)^{10} - 1 \equiv 3^{10} - 1 \equiv 0 \pmod{11}$.
So $n^{10} - 1 \equiv 0 \pmod{11}$ if $n \equiv \pm 3 \pmod{11}$.
- $2^5 = 32 \equiv -1 \pmod{11}$. So $4^{10} = (2^5)^4 \equiv 1 \pmod{11}$.
Hence $(-4)^{10} - 1 \equiv 4^{10} - 1 \equiv 0 \pmod{11}$.
So $n^{10} - 1 \equiv 0 \pmod{11}$ if $n \equiv \pm 4 \pmod{11}$.
- $5^2 = 25 \equiv 4 \pmod{11}$ and $4^5 = (2^5)^2 \equiv 1 \pmod{11}$.
So $5^{10} = (5^2)^5 \equiv 4^5 \equiv 1 \pmod{11}$. Hence $(-5)^{10} - 1 \equiv 5^{10} - 1 \equiv 0 \pmod{11}$.
So $n^{10} - 1 \equiv 0 \pmod{11}$ if $n \equiv \pm 5 \pmod{11}$.

So, for each congruence possibility of n , we find a factor of $n^{11} - n$ is *congruent* to 0 *modulo* 11. So for any integer n , $n^{11} - n \equiv 0 \pmod{11}$. Hence for any integer n , $n \mid n^{11} - n$.

3. Show that $n^9 - n$ is not necessarily divisible by 9.

Solution. Now $2^9 - 2 = 510$ and $9 \nmid 510$; so 9 need not divide $n^9 - n$.



The general result suggested by the previous two questions is:

Fermat's Little Theorem. If n is an integer and p is a prime then $p \mid n^p - n$.

4. Prove the following:

- (i) $3^{6n} - 2^{6n}$ is divisible by 35, for every positive integer n ;

Solution. Let $N = 3^{6n} - 2^{6n}$. Now $35 = \text{lcm}(5, 7)$. So to check that $35 \mid N$, it is enough to show that $5 \mid N$ and $7 \mid N$.

- Firstly,

$$\begin{aligned} N &= 3^{6n} - 2^{6n} = 9^{3n} - 4^{3n} \\ &\equiv 4^{3n} - 4^{3n} \pmod{5} \\ &\equiv 0 \pmod{5}, \end{aligned}$$

and hence $5 \mid N$.

- Similarly,

$$\begin{aligned} N &= 3^{6n} - 2^{6n} = 27^{2n} - 8^{2n} \\ &\equiv (-1)^{2n} - 1^{2n} \pmod{7} \\ &\equiv 1^n - 1^n \pmod{7} \\ &\equiv 0 \pmod{7}, \end{aligned}$$

and hence $7 \mid N$.

Thus, since $5 \mid N$ and $7 \mid N$, we have $35 = \text{lcm}(5, 7)$ divides $N = 3^{6n} - 2^{6n}$.

(ii) $n^5 - 5n^3 + 4n$ is divisible by 120, for every integer n .

Solution. Let $N = n^5 - 5n^3 + 4n$. Then


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

So N is the product of the five consecutive integers: $(n-2), (n-1), n, (n+1), (n+2)$. Exactly one of these integers is divisible by 5, at least one is divisible by 4 and at least one is divisible by 3. Further, if $k \in \{-2, -1, 0, 1, 2\}$ and $n+k$ is a factor of N that is divisible by 4, then either $n+k-2$ or $n+k+2$ is a factor of N both of which are even. That is, either $(n+k)(n+k-2) \mid N$ or $(n+k)(n+k+2) \mid N$; in either case, we see that $8 \mid N$. Hence, $120 = \text{lcm}(3, 5, 8)$ divides $N = n^5 - 5n^3 + 4n$.

(iii) for all integers m and n , $mn(m^{60} - n^{60})$ is divisible by 56 786 730.

Hint: $56\,786\,730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$.

Solution. Here we need Fermat's Little Theorem and Euclid's Lemma (for primes), which is given below. From these we deduce some fairly easy but quite powerful results.

 **Euclid's Lemma.** If a prime p divides a product of integers ab then p must divide at least one of a or b .

Corollary 1. If n is an integer and p is a prime then $p \mid n$ or $p \mid n^{p-1} - 1$.

Proof. Observe $n^p - n = n(n^{p-1} - 1)$. Hence the result follows immediately from Fermat's Little Theorem and Euclid's Lemma. \square

Corollary 2. If m, n are integers, p is a prime and ℓ is a natural number then p divides

$$mn(m^{\ell(p-1)} - n^{\ell(p-1)}).$$

Proof. If $p \mid m$ or $p \mid n$ then the result is true. So, suppose that $p \nmid m$ and $p \nmid n$. Then by the previous corollary $p \mid m^{p-1} - 1$ and $p \mid n^{p-1} - 1$. Hence,

$$m^{p-1} \equiv 1 \equiv n^{p-1} \pmod{p}$$

and so, for any natural number ℓ ,

$$m^{\ell(p-1)} \equiv 1 \equiv n^{\ell(p-1)} \pmod{p};$$

so that $m^{\ell(p-1)} - n^{\ell(p-1)} \equiv 0 \pmod{p}$, i.e.

$$p \mid m^{\ell(p-1)} - n^{\ell(p-1)}.$$

So, in all cases, $p \mid mn(m^{\ell(p-1)} - n^{\ell(p-1)})$. \square

Now observe the following:

$$\begin{aligned} mn(m^{60} - n^{60}) &= mn(m^{60(2-1)} - n^{60(2-1)}) \\ &= mn(m^{30(3-1)} - n^{30(3-1)}) \\ &= mn(m^{15(5-1)} - n^{15(5-1)}) \\ &= mn(m^{12(7-1)} - n^{12(7-1)}) \\ &= mn(m^{10(11-1)} - n^{10(11-1)}) \\ &= mn(m^{5(13-1)} - n^{5(13-1)}) \\ &= mn(m^{2(31-1)} - n^{2(31-1)}) \\ &= mn(m^{1(61-1)} - n^{1(61-1)}). \end{aligned}$$

Hence, by the above corollary, each of the primes 2, 3, 5, 7, 11, 13, 31 and 61 divides $mn(m^{60} - n^{60})$. So, $56\,786\,730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$ divides $mn(m^{60} - n^{60})$.

5. Prove that $n^2 + 3n + 5$ is never divisible by 121 for any positive integer n .

Solution. Observe that

$$n^2 + 3n + 5 = (n + 7)(n - 4) + 33,$$

so that $11 \mid n^2 + 3n + 5$ if and only if $11 \mid (n + 7)(n - 4)$. Thus, if $11 \nmid (n + 7)(n - 4)$ then 11 (and hence 121) does *not* divide $n^2 + 3n + 5$. So, assume 11 divides $(n + 7)(n - 4)$. Then $11 \mid n + 7$ or $11 \mid n - 4$; but then 11 must divide *both* of $n + 7$ and $n - 4$, since

$$n + 7 \equiv n - 4 \pmod{11}.$$

Thus, $121 \mid (n + 7)(n - 4)$. However, $121 \nmid 33$. So $121 \nmid n^2 + 3n + 5 = (n + 7)(n - 4) + 33$. Hence, in all cases, $121 \nmid n^2 + 3n + 5$.

6. What is the final digit of $(\dots(((7^7)^7)^7)\dots^7)$.

There are 1001 7s in the formula.

Solution. The final digit of a (decimal) number is its remainder *modulo* 10. Now $7^2 = 49 \equiv -1 \pmod{10}$. So $7^7 = (7^2)^3 \cdot 7 \equiv -7 \pmod{10}$, and

$$(7^7)^7 \equiv (-7)^7 \equiv -(7^7) \equiv -(-7) \equiv 7 \pmod{10}.$$

Proceeding in this way, we see that $((7^7)^7)^7 \equiv 7 \pmod{10}$, and in general

$$(\dots(((7^7)^7)^7)\dots^7) \equiv \pm 7 \pmod{10},$$

where the sign is + if all together there is an *odd* number of 7s in the formula, and - if there is an *even* number of 7s. Now, 1001 is odd. So the final digit of the given formula is 7.

7. What is the final digit of $7^{7^{7^{\dots^7}}}$.

There are 1001 7s in the formula.

Solution. Firstly, we will call an expression of the form

$$7^{7^{7^{\dots^7}}}$$

a *tower* of 7s. Observe that

$$7^4 = (7^2)^2 \equiv (-1)^2 \equiv 1 \pmod{10}.$$

Hence, *modulo* 10,

$$7^k \equiv \begin{cases} 1 & \text{if } k \equiv 0 \pmod{4} \\ 7 & \text{if } k \equiv 1 \pmod{4} \\ -1 & \text{if } k \equiv 2 \pmod{4} \\ -7 & \text{if } k \equiv 3 \pmod{4}, \end{cases}$$

where k is a natural number. Thus to determine the last digit of a tower of 1001 7s, we need to determine what a tower of 1000 7s is congruent to *modulo* 4. Now, $7 \equiv -1 \pmod{4}$. Hence, *modulo* 4,

$$7^m \equiv \begin{cases} 1 & \text{if } m \text{ is even} \\ -1 & \text{if } m \text{ is odd,} \end{cases}$$

where m is a natural number. A tower of 999 7s is certainly odd. So, a tower of 1000 7s is congruent to $-1 \pmod{4}$ (and $-1 \equiv 3 \pmod{4}$). So, a tower of 1001 7s is congruent to $-7 \pmod{10}$ (and $-7 \equiv 3 \pmod{10}$). Hence, a tower of 1001 7s must end in a 3.

8. When 4444^{4444} is written in decimal notation, the sum of its digits is A . Let B be the sum of the digits of A . Find the sum of the digits of B .

Solution.

- First we will show that the sum of the digits of B is fairly small. Now $4444 < 10\,000 = 10^4$. Hence

$$4444^{4444} < 10^{4 \cdot 4444} = 10^{17776},$$

and so 4444^{4444} cannot have more than 17776 digits. Thus, A the sum of the digits of 4444^{4444} , cannot be more than $17776 \cdot 9 = 159984$, (since each digit is at most a 9). Of the natural numbers less than or equal to 159984, the number with the largest digit sum is 99999. So B is not more than 45. Of the natural numbers less than or equal to 45, the number with the largest digit sum is 39. So the sum of the digits of B is not more than 12.

- Now we use the following result, (which is easily proved in the same way as question 1) *recursively*.

$$\text{For any natural number } N, \quad N \equiv (\text{sum of the digits of } N) \pmod{9}.$$

Using this result we see that 4444^{4444} is *congruent* to its digit sum A , *modulo* 9. Using the result again, we see that A is *congruent* to its digit sum B , *modulo* 9. Using the result one further time, we see that B is *congruent* to its digit sum, *modulo* 9. That is,

$$\begin{aligned} 4444^{4444} &\equiv A && \pmod{9} \\ &\equiv B && \pmod{9} \\ &\equiv (\text{sum of the digits of } B) && \pmod{9} \end{aligned}$$

- Now we determine what 4444^{4444} is congruent to *modulo* 9.

$$\begin{aligned} 4444^{4444} &\equiv (4 + 4 + 4 + 4)^{4444} \pmod{9} \\ &\equiv 16^{4444} \pmod{9} \\ &\equiv (-2)^{4444} \pmod{9} \\ &\equiv (-2)^{3 \cdot 1481 + 1} \pmod{9} \\ &\equiv ((-2)^3)^{1481} \cdot (-2) \pmod{9} \\ &\equiv (-8)^{1481} \cdot (-2) \pmod{9} \\ &\equiv 1^{1481} \cdot (-2) \pmod{9} \\ &\equiv 1 \cdot (-2) \pmod{9} \\ &\equiv 7 \pmod{9} \end{aligned}$$

Putting these three facts together we get

$$(\text{the sum of the digits of } B) \equiv 7 \pmod{9}$$

and *the sum of the digits of* B is a *natural number* less than or equal to 12. Thus

$$(\text{the sum of the digits of } B) = 7.$$