University of Western Australia
DEPARTMENT OF MATHEMATICS

**UWA ACADEMY
FOR YOUNG MATHEMATICIANS**

Number Theory II: Problems with Solutions

Greg Gamble

1. About all we know of Diophantus' life is his epitaph from which his age at death is to be deduced:

   > Diophantus spent one-sixth of his life in childhood, one-twelfth in youth, and another one-seventh in bachelorhood. A son was born five years after his marriage and died four years before his father at half his father's age.

   Solution. Let x be Diophantus' age at death. Then

   $$x - 4 - \big((\tfrac{1}{6} + \tfrac{1}{12} + \tfrac{1}{7})x + 5\big) = \tfrac{1}{2}x.$$

   Rearranging, we get

   $$\big(\tfrac{1}{2} - (\tfrac{1}{6} + \tfrac{1}{12} + \tfrac{1}{7})\big)x = 9$$
   $$\tfrac{3}{28}x = 9$$

   Hence, $x = 9.\frac{28}{3} = 84$. Diophantus died at the age of 84.

2. Augustus de Morgan, a nineteenth-century mathematician, stated:

   > I was x years old in the year x^2.

   When was he born?

   Solution. Since $42^2 = 1764$, $43^2 = 1849$ and $44^2 = 1936$, $x = 43$ and $x^2 = 1849$. So Augustus de Morgan was born in 1806.

3. Prove that for every integer n:

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

   Show that $n^9 - n$ is not necessarily divisible by 9. *Hint:* Try $n = 2$.
   What general result is suggested by the above?

   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) n is *congruent* to exactly one of $-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5$ *modulo* 11. 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 $n \mid n^{11} - n$.

Now $2^9 - 2 = 510$ and $9 \nmid 510$; so 9 need not divide $n^9 - n$. The general result suggested by the above is the Corollary to Fermat's Little Theorem, which may be written in the following way:

If n is an integer and p is a prime then $p \mid n^p - n$.

4. Prove that $3^{6n} - 2^{6n}$ is divisible by 35, for every positive integer n.

Solution. Let $N = 3^{6n} - 2^{6n}$. Now $35 = \operatorname{lcm}(5, 7)$. 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 $35 = \operatorname{lcm}(5, 7)$ divides $N = 3^{6n} - 2^{6n}$.

*5. What is the final digit of $7^{7^{7^{7^{7^{7^{7}}}}}}$.

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

$$7^{7^{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}}$$

a *tower* of 7s. Our problem has a tower of 7 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 7 7s, we need to determine what a tower of 6 7s is congruent to *modulo* 4. Now, $7 \equiv -1 \pmod 4$. Hence, *modulo* 4,

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

where m is a natural number. A tower of 5 7s is certainly odd. So, a tower of 6 7s is congruent to -1 *modulo* 4 (and $-1 \equiv 3 \pmod 4$). So, a tower of 7 7s is congruent to -7 *modulo* 10 (and $-7 \equiv 3 \pmod{10}$). Hence, a tower of 7 7s must end in a 3.

Homework exercises.

1. Prove that for any natural number n that

$$17 \text{ divides } 2^n.3^{2n} - 1.$$

Solution.

$$\begin{aligned} 2^n.3^{2n} - 1 &= (2.3^2)^n - 1 \\ &= 18^n - 1 \\ &\equiv 1^n - 1 \pmod{17} \\ &\equiv 0 \pmod{17}. \end{aligned}$$

So $17 \,|\, 2^n.3^{2n} - 1$. (Remember: $N \equiv 0 \pmod{m}$ means *exactly* the same thing as $m \,|\, N$.)

2. Prove that for any natural number n

$$17^n - 12^n - 24^n + 19^n$$

is divisible by 35.

Solution. Let $N = 17^n - 12^n - 24^n + 19^n$. Now $35 = \text{lcm}(5,7)$. So to check that $35 \,|\, N$, it is enough to show that $5 \,|\, N$ *and* $7 \,|\, N$.

- Firstly,

$$\begin{aligned} N &= 17^n - 12^n - 24^n + 19^n \\ &\equiv 2^n - 2^n - 4^n + 4^n \pmod{5} \\ &\equiv 0 \pmod{5}, \end{aligned}$$

and hence $5 \,|\, N$.

- Similarly,

$$\begin{aligned} N &= 17^n - 12^n - 24^n + 19^n \\ &\equiv 3^n - 5^n - 3^n + 5^n \pmod{7} \\ &\equiv 0 \pmod{7}, \end{aligned}$$

and hence $7 \,|\, N$.

Thus, since $5 \,|\, N$ and $7 \,|\, N$, we have $35 = \text{lcm}(5,7)$ divides $N = 17^n - 12^n - 24^n + 19^n$.

3. Using Fermat's Little Theorem, prove that for all positive integers a and b:

(i) 3 divides $(a+b)^3 - a^3 - b^3$;

(ii) 5 divides $(a+b)^5 - a^5 - b^5$.

Can you generalise these results?

Solution. We use the Corollary to Fermat's Little Theorem:

If p is prime and n is an integer then $n^p \equiv n \pmod{p}$.

(i) Thus $(a+b)^3 \equiv (a+b) \pmod 3$, $a^3 \equiv a \pmod 3$ and $b^3 \equiv b \pmod 3$. Hence

$$\begin{aligned}(a+b)^3 - a^3 - b^3 &\equiv a + b - a - b \pmod 3\\ &\equiv 0 \pmod 3\end{aligned}$$

So $3 \mid (a+b)^3 - a^3 - b^3$.

(ii) Similarly, $(a+b)^5 \equiv (a+b) \pmod 5$, $a^5 \equiv a \pmod 5$ and $b^5 \equiv b \pmod 5$. Hence

$$\begin{aligned}(a+b)^5 - a^5 - b^5 &\equiv a + b - a - b \pmod 5\\ &\equiv 0 \pmod 5\end{aligned}$$

So $5 \mid (a+b)^5 - a^5 - b^5$.

The generalisation of the above results is:

For any integers a, b and for any prime p,

$$p \mid (a+b)^p - a^p - b^p.$$

*4. Prove that $5^{99} + 11^{99} + 17^{99}$ is divisible by 33.

Solution. Let $N = 5^{99} + 11^{99} + 17^{99}$. Now $33 = \operatorname{lcm}(3, 11)$. So to check that $33 \mid N$, it is enough to show that $3 \mid N$ *and* $11 \mid N$. Again, we shall use congruences.

- Firstly,

$$\begin{aligned}N &= 5^{99} + 11^{99} + 17^{99}\\ &\equiv 2^{99} + 2^{99} + 2^{99} \pmod 3\\ &\equiv 3.2^{99} \pmod 3\\ &\equiv 0 \pmod 3,\end{aligned}$$

and hence $3 \mid N$.

- Similarly,

$$\begin{aligned}N &= 5^{99} + 11^{99} + 17^{99}\\ &\equiv 5^{99} + 0^{99} + (-5)^{99} \pmod{11}\\ &\equiv 5^{99} + 0 - 5^{99} \pmod{11}\\ &\equiv 0 \pmod{11},\end{aligned}$$

and hence $11 \mid N$.

Thus, since $3 \mid N$ and $11 \mid N$, we have $33 = \operatorname{lcm}(3, 11)$ divides $N = 5^{99} + 11^{99} + 17^{99}$.

*5. What is the final digit of $(((((((((((7^7)^7)^7)^7)^7)^7)^7)^7)^7)^7)$? (7 occurs as a power 10 times.)

Solution. The final digit of a (decimal) number is its remainder *modulo* 10. Now $7^2 = 49 \equiv -1 \pmod{10}$. So $7^7 = (7^2)^3.7 \equiv -7 \pmod{10}$, 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

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

where the sign is $+$ if all together there is an *even* number of 7s appearing as powers in the formula, and $-$ if there is an *odd* number of 7s appearing as powers in the formula. Now, 10 is even. So the final digit of the given formula is 7.

$*$6. *(17th International Olympiad, 1975, Problem 4)* 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.

Hints: First show that the sum of the digits of B is fairly small (in fact: less than 16). Then use the fact that, for any natural number N,

$$N \equiv (\text{sum of the digits of } N) \pmod 9.$$

Solution.

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

$$4444^{4444} < 10^{4.4444} = 10^{17776},$$

and so 4444^{4444} cannot have more than 17 776 digits. Thus, A the sum of the digits of 4444^{4444}, cannot be more than $17\,776.9 = 159\,984$, (since each digit is at most a 9). Of the natural numbers less than or equal to 159 984, the number with the largest digit sum is 99 999. 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 result given in the hint:

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

(Note that this result was proved when we proved the divisibility rule for 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.

$$\begin{aligned} 4444^{4444} &\equiv (4+4+4+4)^{4444} && \pmod 9 \\ &\equiv 16^{4444} && \pmod 9 \\ &\equiv (-2)^{4444} && \pmod 9 \\ &\equiv (-2)^{3.1481+1} && \pmod 9 \\ &\equiv \left((-2)^3\right)^{1481}.(-2) && \pmod 9 \\ &\equiv (-8)^{1481}.(-2) && \pmod 9 \\ &\equiv 1^{1481}.(-2) && \pmod 9 \\ &\equiv 1.(-2) && \pmod 9 \\ &\equiv 7 && \pmod 9 \end{aligned}$$

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

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