Fermat’s Little Theorem Solutions

Justin Stevens

Problem 1. Convert 11, 101, 001, 111_2 to base 8.

Solution. Since 8 = 2^3, we have to group the numbers in 3’s:

\[
11, 101, 001, 111_2 = 2^{10} + 2^9 + 2^8 + 2^6 + 2^3 + 2^2 + 2^1 + 2^0
\]

\[
= (2 + 1) 2^9 + (2^2 + 1) 2^6 + 1 \cdot 2^3 + (2^2 + 2^1 + 2^0)
\]

\[
= 3 \cdot 8^3 + 5 \cdot 8^2 + 1 \cdot 8^1 + 7 \cdot 8^0
\]

Using the commas, we see 11_2 = 3, 101_2 = 5, 001_2 = 1, 111_2 = 7.

Problem 2. Find the positive integer \(n\) such that there exists a single digit \(d\) with

\[
\frac{n}{810} = 0.d25d25d25\ldots.
\]

Solution. Using the formula for a sum of an infinite geometric series,

\[
\frac{n}{810} = \frac{100d + 25}{10^3} + \frac{100d + 25}{10^6} + \ldots
\]

\[
= \frac{100d + 25}{999}.
\]

We isolate the equation for \(n\) and simplify:

\[
n = \frac{810}{999} (100d + 25) = \frac{30}{37} \cdot 25 (4d + 1).
\]

Hence 37 | 4d + 1, so \(d = 9\). Then, \(n = 30 \cdot 25 = 750\).

Problem 3. Show that \(2^{86} + 5^{86}\) is divisible by 29.

Solution. By Fermat’s Little Theorem, \(2^{28} \equiv 1 \pmod{29}\) and \(5^{28} \equiv 1 \pmod{29}\). Therefore,

\[
2^{86} + 5^{86} \equiv 2^2 + 5^2 \equiv 0 \pmod{29}.
\]

Problem 4. (a) Prove that any integer of the form

\[
n = (6k + 1)(12k + 1)(18k + 1)
\]

is a Carmichael number if all three factors are prime.
(b) Show that 1729 is a Carmichael number.

Solution. (a) Let $6k + 1 = p, 12k + 1 = q,$ and $18k + 1 = r,$ hence $n = pqr.$ Observe that

$$n - 1 = 1296k^3 + 396k^2 + 36k$$

is divisible by $p - 1 = 6k,$ $q - 1 = 12k,$ and $r - 1 = 18k.$ Thus $n$ is Carmichael by Korselt’s Criterion since $p_i - 1 | n - 1$ for all prime divisors.

(b) Observe that $1729 = 7 \cdot 13 \cdot 19$ is of the above form, hence it is Carmichael.

Problem 5. (a) Prove that if $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$ for primes $p$ and $q,$ then

$$a^{pq} \equiv a \quad \pmod{pq}.$$ 

(b) Prove that $2^{341} \equiv 2 \pmod{341}.$

Solution. (a) Using Fermat’s Little Theorem in conjunction with the given congruences,

$$a^{pq} \equiv (a^p)^q \equiv a^q \equiv a \pmod{q}$$

$$a^{pq} \equiv (a^q)^p \equiv a^p \equiv a \pmod{p}.$$ 

Therefore, $a^{pq} \equiv a \pmod{pq}.$

(b) In light of $341 = 11 \cdot 31,$ we see $2^{10} = 1024 \equiv 1 \pmod{11}$ and $2^{10} \equiv 1 \pmod{31}:

$$2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31}$$

$$2^{31} = 2 \cdot (2^{10})^3 = 2 \cdot 1^3 \equiv 2 \pmod{11}.$$ 

Hence, by the previous example, $2^{341} \equiv 2 \pmod{341}.$
