MATHS BASIC COURSE FOR UNDERGRADUATES

Leire Legarreta, Iker Malaina and Luis Martínez

Faculty of Science and Technology
Department of Mathematics
University of the Basque Country
SOLUTIONS: 5th SUBJECT. CONGRUENCES

SOLUTION EXERCISE 1: In congruence language, we have to find an integer number \( r \) comprehended between 0 and 12, for which \( n \equiv r \pmod{12} \), in other words, we have to reduce \( n \) to modulo 12. First of all, 
\[
4! = 24 \equiv 0 \pmod{12},
\]
and consequently if \( k \geq 4 \),
\[
k! = k(k - 1) \ldots 6 \cdot 5 \cdot 4! \equiv k(k - 1) \ldots 6 \cdot 5 \cdot 0 \equiv 0 \pmod{12}.
\]
Thus, \( n \equiv 1! + 2! + 3!(\pmod{12}) \), and therefore \( n \equiv 9 \pmod{12} \).

SOLUTION EXERCISE 2: We have to prove that the remainder of the division of 
\[
5^{2k} + 3 \cdot 2^{5k - 2}
\]
by 7 is 0. By applying congruences’ properties and since \( 3 \equiv -2^2 \pmod{7} \) is fulfilled, we get the following congruences modulo 7:
\[
5^{2k} + 3 \cdot 2^{5k - 2} \equiv 5^{2k} - 2^{5k - 2} \equiv 25^k - 32^k \pmod{7}.
\]
On the other hand, since \( 25 \equiv 4 \pmod{7} \) and \( 32 \equiv 4 \pmod{7} \), by applying congruences’ properties, we obtain that
\[
5^{2k} + 3 \cdot 2^{5k - 2} \equiv 25^k - 32^k \equiv 4^k - 4^k \equiv 0 \pmod{7}.
\]

SOLUTION EXERCISE 3: Write \( n \) in decimal form,
\[
n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k,
\]
where \( a_i \) satisfies \( 0 \leq a_i \leq 9 \). Since \( 10 \equiv 1 \pmod{9} \), applying congruences’s properties, \( 10^i \equiv 1 \pmod{9} \) and \( a_i \cdot 10^i \equiv a_i \pmod{9} \). Thus, \( n \equiv a_1 + a_2 + \cdots + a_n \pmod{9} \).

SOLUTION EXERCISE 4: Since \( 614 \equiv 2 \pmod{17} \) (\( 614 = 36 \cdot 17 + 2 \)), then \( 614^{6943} \equiv 2^{6943} \pmod{17} \). Since \( 17 \nmid 2 \), using Fermat’s Little Theorem, we have that \( 2^{16} \equiv 1 \pmod{17} \). Now, since \( 6943 = 433 \cdot 16 + 15 \),
\[
2^{6943} \equiv 2^{433 \cdot 16 + 15} \equiv (2^{16})^{433} \cdot 2^{15} \equiv 1^{433} \cdot 2^{15} \equiv 2^{15} \pmod{17}.
\]
Finally, since \( 2^4 \equiv 16 \equiv -1 \pmod{17} \), then
\[
2^{15} \equiv 2^{4 \cdot 3 + 3} \equiv (2^4)^3 \cdot 2^3 \equiv (-1)^3 \cdot 2^3 \equiv -8 \equiv 9 \pmod{17}.
\]
Thus, the remainder that we were looking for is 9.

SOLUTION EXERCISE 5: If \( x \in \mathbb{Z} \) is a solution for this linear congruence, then \( 13x = 2 + 31q \), for some \( q \in \mathbb{Z} \). Observe that \( \gcd(13, 31) = 1 \), and then by applying Bezout’s identity, there exist two integer numbers \( s, t \) for which \( 1 = 13s + 31t \). Thus,
$13s \equiv 1 \pmod{31}$, and multiplying the previous congruence by 2, we obtain $13(2s) \equiv 2 \pmod{31}$. This is, $x = 2s \ (s \in \mathbb{Z})$ is a solution for the initial congruence.

**SOLUTION EXERCISE 6:** By Fermat’s Little Theorem, the congruence $x^{p-1} \equiv 1 \pmod{p}$, or equivalently the congruence $x^{p-1} - 1 \equiv 0 \pmod{p}$ has $p - 1$ different solutions. To be more precise, the solutions of the previous congruence are: $1, 2, \ldots, p - 1$. Thus,

\[ x^{p-1} - 1 \equiv (x - 1)(x - 2) \cdots (x - (p - 1)) \pmod{p}. \]

Now, since any of those values of $x$ fulfills this congruence, by taking $x = 0$ we obtain that:

\[ -1 \equiv (-1)(-2) \cdots (- (p - 1)) \pmod{p} \equiv (-1)^{p-1} 1 \cdot 2 \cdots (p - 1) \pmod{p}, \]

this is, $(-1)^{p-1} \cdot (p-1)! + 1 \equiv 0 \pmod{p}$. In particular, if $p = 2$, we get $-1 + 1 \equiv 0 \pmod{2}$, which is obvious, and if $p$ is an odd number, we get $(p-1)! + 1 \equiv 0 \pmod{p}$.