Problem 1

For each of the following congruences, find the least nonnegative integer x that satisfies it.

(a) \[ \frac{60!}{31!} \equiv x \pmod{31} \]

(b) \[ \frac{59!}{30!} \equiv x \pmod{31} \]

1a. We have
\[ x \equiv \frac{60!}{31!} = 60 \cdot 59 \cdots 33 \cdot 32 \equiv 29 \cdot 28 \cdots 2 \cdot 1 = 29! \pmod{31}. \]

Multiplying the congruence by 30 gives, by Wilson’s thm,
\[ 30x \equiv 30! \equiv -1 \pmod{1} \iff x \equiv -30 \equiv 1 \pmod{31}. \]

1b. We have
\[ x \equiv \frac{59!}{30!} = 59 \cdot 58 \cdots 32 \cdot 31 \equiv 0 \pmod{31}. \]

Problem 2

Let p and q be distinct odd prime numbers with p − 1 | q − 1. If \(a \in \mathbb{Z}\) with \((a, pq) = 1\), prove that \(a^{q-1} \equiv 1 \pmod{pq}\).

Since \(p, q\) are distinct primes, the result follows from CRT if we show that
\[ a^{q-1} \equiv 1 \pmod{q} \quad \text{and} \quad a^{q-1} \equiv 1 \pmod{p}. \]

Note that \((a, pq) = 1\) implies \((a, q) = (a, p) = 1\). Now, the first of the congruences above follows directly from FLT. For the second, we note that \(q - 1 = (p - 1)k\) leads to
\[ a^{q-1} \equiv (a^{p-1})^k \equiv 1 \pmod{p}, \]

where again we have used FLT.
**Problem 3**

Prove that $1729 = 7 \cdot 13 \cdot 19$ is a Carmichael number.

From the factorization of $n = 1729 = 7 \cdot 13 \cdot 19$ we see it is squarefree. Moreover, if $p$ is a prime divisor of $n$ then $p - 1 = 6, 12, 18$ which are clearly all factors of $n - 1$, since

$$1728 = 6 \cdot 288 = 12 \cdot 144 = 18 \cdot 96.$$ 

Thus $n$ is a Carmichael number by Korset criterion.

**Problem 4**

Use Miller’s Test in base 2 to show that $1729$ is composite.

We will apply Miller’s test for base 2. We have $n = 1729$ and

$$n - 1 = 1728 = 18 \cdot 96 = 36 \cdot 48.$$ 

We compute

$$2^{n-1} \equiv (2^{36})^{48} \equiv 1 \pmod{1729}$$

so $n$ is a pseudoprime in base 2. We proceed,

$$2^{(n-1)/2} \equiv (2^{36})^{24} \equiv 1 \pmod{1729}$$

$$2^{(n-1)/4} \equiv (2^{36})^{12} \equiv 1 \pmod{1729}$$

$$2^{(n-1)/8} \equiv (2^{36})^{6} \equiv 1 \pmod{1729}$$

$$2^{(n-1)/16} \equiv (2^{36})^{3} \equiv 1 \pmod{1729}$$

$$2^{(n-1)/32} \equiv (2^{18})^{3} \equiv 1065^{3} \equiv 1065 \not\equiv \pm 1 \pmod{1729}$$

**Problem 5**

Suppose that one digit, indicated with a question mark, in the following ISBN10 codes has been smudged and cannot be read. What should this missing digit be?

$$? - 261 - 05073 - X$$

For the code to be valid we need

$$\sum_{i=1}^{10} i \cdot a_i \equiv 0 \pmod{11} \iff 1 \cdot ? + 2 \cdot 2 + 3 \cdot 6 + 4 \cdot 1 + 5 \cdot 0 + 6 \cdot 5 + 7 \cdot 0 + 8 \cdot 7 + 9 \cdot 3 + 10 \cdot 10 \iff ? \equiv 3 \pmod{11}.$$