Easier problems

1. Prove that if \((a, m) = (a - 1, m) = 1\), then

\[
1 + a + a^2 + \cdots + a^{\phi(m) - 1} \equiv 0 \pmod{m},
\]

and deduce that every prime other than 2 or 5 divides infinitely many of the integers 1, 11, 111, 1111, \ldots.

2. Show that every integer satisfies at least one of the following congruences:

\[
x \equiv 0 \pmod{2},
\]

\[
x \equiv 0 \pmod{3},
\]

\[
x \equiv 1 \pmod{4},
\]

\[
x \equiv 1 \pmod{6},
\]

\[
x \equiv 11 \pmod{12}.
\]

Such a collection of congruences (with the moduli all different) is known as a covering class. Erdős has asked whether there are covering classes with all the moduli arbitrarily large. It is still an open question.

3. Show that if \(p\) is an odd prime, then the congruence \(x^2 \equiv 1 \pmod{p^t} \ (t \in \mathbb{N})\) has only the two solutions \(x \equiv \pm 1 \pmod{p^t}\).

4. Show that the congruence \(x^2 \equiv 1 \pmod{2^t} \ (t \in \mathbb{N})\) has one solution when \(t = 1\), two solutions when \(t = 2\), and precisely the four solutions 1, 2\(^{t-1} - 1\), 2\(^{t-1} + 1\), \(-1\) when \(t \geq 3\).

Harder problems

5. Let \(n > 2\). If \(m\) is the number of solutions of the congruence \(x^2 \equiv 1 \pmod{n}\), then show that \(2|m\). Further let \(a_1, \ldots, a_{\phi(n)}\) be a system of reduced residues modulo \(n\). Prove that \(a_1a_2\cdots a_{\phi(n)} \equiv (-1)^{m/2} \pmod{n}\).

6. Show that if \(n = 4^h(8k + 7)\) for some non-negative integers \(h\) and \(k\), then \(n = x^2 + y^2 + z^2\) is insoluble in integers \(x, y, z\). If \(n\) is not of this form, then it can be show that this equation is soluable. Legendre thought he had a proof, but Gauss pointed out a gap and provided the first complete proof. Dirichlet filled the gap in Legendre’s proof.