Elementary Number Theory and Cryptography,
Michaelmas 2011, Problem Sheet 4 (Congruences).

1. (a) Show that $(a + 10 \cdot b)^2 \equiv a^2 \pmod{10}$.
   (b) Using (a), or otherwise, prove that any number that is a square must have one of the following for its units digit: 0, 1, 4, 5, 6, 9.
   (c) How many different remainders for integer *squares* modulo 100 can you find? Why are there fewer such with units digit 0 or 5 than for the remaining four possible units digits? [Part (a) may be helpful.]
2. (a) Solve the linear congruence
$$3x \equiv 7 \pmod{11}\,.$$
   (b) Find an integer x such that
$$33x \equiv 1 \pmod{101}\,,$$
   and find one such that
$$29x \equiv 1 \pmod{101}\,.$$
3. (i) Show that $2, 4, 6, \ldots, 2m$ constitutes a complete set of residues modulo m, provided m is *odd*.
   (ii) Show that $1^2, 2^2, 3^2, \ldots, m^2$ is *not* a complete set of residues modulo m, if $m > 2$.
4. Denote by $\varphi(n)$ Euler's φ-function, which is defined as
$$\varphi(n) = \#\{a \in \mathbb{Z} \mid \gcd(a, n) = 1 \text{ and } 0 < a < n\}.$$
   Determine $\varphi(n)$ for the following n:
   (a) $n = 275$;
   (b) $n = 2^7$;
   (c) $n = 404$.
5. Show that, for $n > 4$ *composite*, that
$$(n-1)! \equiv 0 \pmod{n}\,.$$
   Compare this statement with the one from Wilson's Theorem.
6. Show that, for a prime p such that $p \equiv 3 \pmod 4$, one has
$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}\,.$$
7. For any prime p different from 2 and 5, prove that p divides infinitely many of the numbers
$$1,\ 11,\ 111,\ 1111,\ \ldots$$
   [Hint: try to show this statement first for (their multiples) $9, 99, 999, \ldots$]
8. (a) Show that, for a given prime p, one has
$$a^p \equiv a \pmod{p}\,,$$
   for *any* integer (i.e., regardless of whether a is coprime to p or not).
   (b) Show that if p is prime then
$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}$$
   for $0 \leqslant k \leqslant p-1$.

I. **Challenge** [hard!]:
Someone misremembers the statement of Fermat's Little Theorem, as saying that $a^{n+1} \equiv a \pmod{n}$ holds for all a if n is prime. Describe the set of integers n for which this fact is indeed true.