8 Further reading

A good account of the elementary theory of congruences is given by T. Nagell, *Introduction to number theory* (Wiley, New York, 1951); this contains, in particular, a table of primitive roots. There is another, and in fact more extensive table in I. M. Vinogradov's *An introduction to the theory of numbers* (Pergamon Press, Oxford, London, New York, Paris, 1961). Again Hardy and Wright cover the subject well.

MA 523 HW3

9 Exercises

(i) Find an integer x such that $2x \equiv 1 \pmod 3$, $3x \equiv 1 \pmod 5$, $5x \equiv 1 \pmod 7$.

(ii) Prove that for any positive integers a, n with $(a, n) = 1$, $\sum \{ax/n\} = \frac{1}{2}\phi(n)$, where the summation is over all x in a reduced set of residues (mod n).

(iii) The integers a and $n > 1$ satisfy $a^{n-1} \equiv 1 \pmod n$ but $a^m \not\equiv 1 \pmod n$ for each divisor m of $n-1$, other than itself. Prove that n is a prime.

(iv) Show that the congruence $x^{p-1} - 1 \equiv 0 \pmod{p^j}$ has just $p-1$ solutions (mod p^j) for every prime power p^j.

(v) Prove that, for every natural number n, either there is no primitive root (mod n) or there are $\phi(\phi(n))$ primitive roots (mod n).

(vi) Prove that, for any prime p, the sum of all the distinct primitive roots (mod p) is congruent to $\mu(p-1)$ (mod p).

(vii) Determine all the solutions of the congruence $y^2 \equiv 5x^3 \pmod 7$ in integers x, y.

(viii) Prove that if p is a prime >3 then the numerator of $1 + \frac{1}{2} + \cdots + 1/(p-1)$ is divisible by p^2 (Wolstenholme's theorem).