Math 1C03 Introduction to Mathematical Reasoning
Term 2 Winter 2014–2015
Problem Sheet 3: congruences and modular arithmetic
to be completed by Wednesday January 28 2015

1) Write down the definition of the statement $a \equiv b \mod m$. Then use the definition to decide if the following assertions of congruence are true or false.
   i) $6 \equiv 5 \mod 4$
   ii) $13 \equiv 3 \mod 3$
   iii) $100 \equiv 25 \mod 4$
   iv) $100 \equiv 25 \mod 15$
   v) $1001 \equiv 12345 \mod 2$
   vi) $-5 \equiv 5 \mod 3$
   vii) $4^{51} \equiv 111111 \mod 2$
   viii) $10! + 1 \equiv 9 \mod 7$
   ix) $10! + 1 \equiv 82 \mod 9$

2) i) Suppose that $a \equiv b \mod m$. Prove that $a^2 \equiv b^2 \mod m$.
   ii) Suppose that $a \equiv b \mod m$. Prove that $na \equiv nb \mod m$ for any positive integer n.
   iii) Suppose that $a \equiv b \mod m$ and $a' \equiv b' \mod m$. Prove that $aa' \equiv bb' \mod m$.

3) Review Example 3.15 in the text. Use the same method to solve the following problems.
   i) Find the remainder when 3^{111} is divided by 80.
   ii) Find the remainder when $4^{23} \cdot 36^{11}$ is divided by 5.

4) i) Recall the statement of the quotient/remainer theorem when a is divided by m and when b is divided by m.
   ii) Suppose that a and b have the same remainder when divided by m. Show that $a \equiv b \mod m$.
   iii) Suppose that $a \equiv b \mod m$. Show that a and b have the same remainder when divided by m.

5) Fix a prime number p.
   i) Use the euclidean algorithm to prove that for every integer m with $1 \leq m < p$ there is a unique integer n with $1 \leq n < p$ such that $[m]_p[n]_p = [1]_p$.
   ii) Find $[(p-1)!]_p$ for $p = 5$ and $p = 7$.
   iii) In general, the product $[(p-1)!]_p$ has how many factors?
   iv) Find $[(p-1)!]_p$ in general.
   v) Deduce Wilson's Theorem: $(p-1)! \equiv -1 \mod p$.