COM1002: Foundations of Computer Science
Problem Sheet 3: Integers Modulo n

1. Work out the following. When doing arithmetic modulo n, present your answer as an element of the set $\{0, 1, 2, \ldots, n-1\}$.

   (a) $3 + 11 \mod 12$

   (b) $13 - 20 \mod 21$

   (c) $6 \times 5 \mod 21$

   (d) $6 \times (-5) \mod 21$

   (e) $(3 \times 6) + (11 \times 2) - 4 \mod 12$

2. Solve the following equations

   (a) $12x \equiv 2 \mod 13$

   (b) $49x \equiv 14 \mod 42$

   (c) $27x \equiv 6 \mod 18$

3. You have a jug which will carry 7 litres of water, and a washbasin which holds exactly 20 litres. By pouring the contents of the jug into the basin, or by emptying the basin when it is full, how can we end up with exactly 4 litres of water in the washbasin?

4. Find all solutions of the equation $30x \equiv 234 \mod 1001$.

5. Find all solutions of the equation $33x \equiv 234 \mod 1001$.

6. Find all solutions $x \in \mathbb{Z}$ to the simultaneous equations

$$x \equiv 4 \mod 7 \qquad x \equiv 3 \mod 9.$$

7. Find all solutions $x \in \mathbb{Z}$ to the simultaneous equations

$$x \equiv 1 \mod 21 \qquad x \equiv 2 \mod 28.$$

8. Find:

(a) $10^{11} \mod 7$.

(b) $2^{10} \mod 3$.

(c) $5^{13} \mod 8$.

9. Find an integer $0 \leq x < 31$ such that $x \equiv 101010^{1955} \mod 31$.

10. Pick two prime numbers p and q. Use these numbers to generate:

(a) A *public key* (n, e) whjere $n = pq$, $1 < e < (p-1)(q-1)$ and $hcf(e, (p-1)(q-1)) = 1$.

(b) A *private key* $d > 0$ where

$$de \equiv 1 \mod (p-1)(q-1).$$