CS 402 Cryptography

Problem Sheet 1

(1) For each pair of integers a, b below, use the Euclidean algorithm to find the greatest common divisor d. Then find integers x and y such that $ax + by = d$.
   (i) 14, 35.
   (ii) 252, 180.
   (iii) 6643, 2873.

(2) Are there positive integers x, y and z such that $2^x \cdot 3^4 \cdot 14^y = 126^z$?

(3) Show that if a positive integer n is composite (i.e. not prime) then
$$R(n) = \frac{10^n - 1}{9} = \underbrace{111\ldots11}_{n \text{ times}}$$
is composite. (Hint: show that if a divides n then $R(a)$ divides $R(n)$.)

(4) Find all solutions of $187x \equiv 12 \mod 546$.

(5) Prove that for every integer n, $n^5 - n$ is divisible by 30.

(6) Find the residues of the following.
   (i) $5^{20} \mod 7$.
   (ii) $7^{1001} \mod 11$.
   (iii) $81^{119} \mod 13$.
   (iv) $13^{216} \mod 19$.

(7) Find the remainder when 1000! is divided by 3^{333}.

(8) Find the number of invertible elements (under multiplication) in $\mathbb{Z}_n$, for $n = 4, 11, 15$. Also find the inverse of each invertible element.

(9) Use the Extended Euclidean Algorithm to find the multiplicative inverse of 111 mod 250.

(10) Show that the equation $x^2 - 7y^2 = 3$ does not have an integer solution.

(11) Use Fermat's Little Theorem to show that $2^{11213} - 1$ is not divisible by 11.