Ciphers and Number Theory 4

1. Solve the following equations.

   (a) $x = 187 \bmod 45$.

   (b) $x = 143 \times 237 \times 361 \times 422 \bmod 11$.

   (c) $x = 3^{182} \bmod 14$.

2. For each of the following, either find the inverse of a in $\mathbb{Z}_n$ or show that it does not exist.

   (a) $a = 5$ and $n = 11$.

   (b) $a = 8$ and $n = 14$.

   (c) $a = 17$ and $n = 131$.

3. Write down the multiplication tables for $\mathbb{Z}_7$ and $\mathbb{Z}_6$. In each case list the elements which are invertible and give their inverses.

4. We normally write numbers in base 10, that is a number a is represented as a sequence of digits $a_t a_{t-1} \dots a_1 a_0$ with $0 \leq a_i \leq 9$ for all i and

$$a = \sum_{i=0}^{t} a_i 10^i.$$

   For example, $134 = 1 \times 10^2 + 3 \times 10 + 4 \times 1$.

   (a) Show that $10^i \equiv 1 \bmod 9$ for all $i \in \mathbb{N}$.

   (b) Deduce that a number a as above is divisible by 9 if and only if

$$\sum_{i=0}^{t} a_i$$

   is divisible by 9.

   (c) Show that $10^i \equiv 1 \bmod 11$ if i is even and $10^i \equiv -1 \bmod 11$ if i is odd.

   (d) Deduce that a number a as above is divisible by 11 if and only if

$$\sum_{i=0}^{t} (-1)^i a_i$$

   is divisible by 11.

5. Show that the equation $ax \equiv b \bmod n$ has a solution if and only if b is divisible by (a, n).

6. Show that the relation $x \equiv y$ if $x - y$ is divisible by n is an equivalence relation, and that $\mathbb{Z}_n$ can be identified with its equivalence classes.