Exercise Sheet 2

This sheet is due in the lecture on Tuesday 14th October, and will be discussed in the exercise class on Friday 17th October.

Exercise 2.1. *Solving linear equations.*

(1) Solve the equation $140x \equiv 98 \pmod{84}$.

(2) Solve the equation $28x \equiv 124 \pmod{116}$.

(3) Find all integer solutions to the equation $12x + 7y = 17$.

(4) Let $a, b, c \in \mathbb{Z}$ where a and b are not simultaneously zero. Show that the equation $ax + by = c$ has solutions in integers iff $\mathrm{hcf}(a, b) \mid c$.

Exercise 2.2. *Solving systems of linear equations.*

(1) Solve the system $x \equiv 1 \pmod{7},\ x \equiv 4 \pmod{9},\ x \equiv -2 \pmod{5}$.

(2) Solve the system $4x \equiv 6 \pmod{13},\ 6x \equiv 4 \pmod{8}$.

(3) Solve the system $x \equiv 7 \pmod{15},\ x \equiv 5 \pmod{9}$.

Exercise 2.3. *Cancellation law for congruences.*

Let $a, b, k, m \in \mathbb{Z}$, $k \neq 0$, $m \neq 0$.

(1) Assume $k \mid m$. Show that $ka \equiv kb \pmod{m}$ iff $a \equiv b \pmod{\frac{m}{k}}$;

(2) Assume $\mathrm{hcf}(k, m) = 1$. Show that $ka \equiv kb \pmod{m}$ iff $a \equiv b \pmod{m}$;

(3) In general, assume $\mathrm{hcf}(k, m) = d$. Show that $ka \equiv kb \pmod{m}$ iff $a \equiv b \pmod{\frac{m}{d}}$. (Hint: use parts (1) and (2).)

Exercise 2.4. *Wilson's theorem and beyond.*

(1) Let p be an odd prime. If $k \in \{1, 2, \cdots, p-1\}$, show that there is a unique b_k in this set such that $kb_k \equiv 1 \pmod{p}$.

(2) Show that $k = b_k$ iff $k = 1$ or $k = p - 1$.

(3) Use parts (1) and (2) to prove that $(p-1)! \equiv -1 \pmod{p}$. This is known as Wilson's theorem.

(4) If $n \in \mathbb{Z}$, $n > 1$, is not a prime, show that $(n-1)! \equiv 0 \pmod{n}$ unless $n = 4$.

(5) Let $n \in \mathbb{Z}$, $n > 1$. Conclude that $(n-1)! \equiv -1 \pmod{n}$ iff n is a prime.