Mathematics 4: Number Theory Problem Sheet 2

Solving Linear congruences and linear equations in integers

Before solving higher degree equations in integers, we should certainly be able to solve linear ones!

Workshop

(1) Explain how to use the Extended Euclidean Algorithm (see Q 7 below) to find the reciprocal $a^* \in \mathbb{F}_p^\times$ of $a \in \mathbb{F}_p^\times$. Here p is a prime, and $\mathbb{F}_p^\times$ is the (multiplicative group of) nonzero elements of the finite field $\mathbb{F}_p$. [So $aa^* \equiv 1 \pmod{p}$.]

(2) *Solving a set of linear congruences in integers.*
  (a) Show that solving one linear congruence $a_1x_1 + \cdots + a_mx_m \equiv b \pmod{n}$ in integers $x_1, \ldots, x_m$ is equivalent to solving a certain linear equation in integers. Here $a_1, \ldots, a_m$ are integers.
  (b) Show that solving a set of linear congruences $a_{1j}x_1 + \cdots + a_{mj}x_m \equiv b_j \pmod{n_j}$ $(j = 1, \ldots, k)$ in integers $x_1, \ldots, x_m$ is equivalent to solving a certain set of linear equations in integers. Here all the $a_{1j}, \ldots, a_{mj}$ are integers.

(3) *Solving one linear equation* $a_1x_1 + \cdots + a_mx_m = b \quad (*)$ *in integers.*
  (a) Show that if $\gcd(a_1, \ldots, a_m)$ does not divide b then $(*)$ has no solution.
  (b) Show that if $\gcd(a_1, \ldots, a_m)$ divides b then we can assume that $\gcd(a_1, \ldots, a_m) = 1$.
  (c) Suppose that $\min(|a_1|, \ldots, |a_m|) = 1$. Write down the general solution to $(*)$.
  (d) Suppose that $\min(|a_1|, \ldots, |a_m|) = r > 1$, where say $a_1 = r$. Define a new variable $t_1 = x_1 + \lfloor a_2/r \rfloor x_2 + \cdots + \lfloor a_m/r \rfloor x_m$. Rewrite $(*)$ in variables $t_1, x_2, \ldots, x_m$ as say $a_1t_1 + a_2'x_2 + \cdots + a_m'x_m = b \quad (**)$. Show that:
    - You can solve $(**)$ in integers if and only if you can solve $(*)$ in integers.
    - Putting $\max(|a_2'|, \ldots, |a_m'|) = r'$ (say), show that $r' < r$.
    - Show that the assumption that $\gcd(a_1, \ldots, a_m) = 1$ implies that $r' \neq 0$.
    - Explain how to solve $(**)$ (and hence $(*)$) if $r' = 1$.
    - Explain how proceed to solve $(**)$ (and hence $(*)$) if $r' > 1$.

(4) Apply the method of the previous question to solve each of the following equations in integers:
  (a) $3x + y + 5z = 8$.
  (b) $3x + 6y + 9z = 18$.

(c) $3x + 6y + 9z = 8$.
(d) $2x + 6y + 9z = 8$.
(e) $5x + 7y + 8z = 8$.

(5) *Solving a system of linear equations* $a_{1j}x_1 + \cdots + a_{mj}x_m = b_j \quad (j = 1, \ldots, k) \quad (*)$ *in integers.*
  (a) Show how, by solving one of the equations, one can reduce the system of equations to a system, possibly in different variables, with one fewer equation.
  (b) Hence outline how to solve a system of linear equations in integers.

Handin: due Friday, week 5, 19 Oct, before 12.10 lecture. Please hand it in at the lecture

The two postage stamp problem: which amounts can be made using only a-pence stamps and b-pence stamps?

You are expected to write clearly and legibly, giving thought to the presentation of your answer as a document written in mathematical English.

(6) Let $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$.
  (a) If $(x_0, y_0) \in \mathbb{Z}^2$ is one solution to $ax + by = n$, find, with proof the general solution $(x, y) \in \mathbb{Z}^2$.
  (b) The equation $ax + by = ab$ has the obvious solution $(b, 0)$ in integers. Show, however, that it has no solution in *positive* integers.
  (c) Show that for every integer $n > ab$ the equation $ax + by = n$ *does* have a solution in positive integers x, y. (Take (x, y) with $y \leq 0$ and x minimal.)
  (d) Show that the equation $ax + by = ab - a - b$ has no solution in nonnegative integers x, y, but that for $n > ab - a - b$ the equation $ax + by = n$ does have such a solution. (This comes straight from the previous parts of the question. How?)

Further problems

(7) **The extended Euclidean algorithm.** Given positive integers n_1, n_2, the Euclidean algorithm calculates the gcd ("greatest common divisor") g of n_1 and n_2. Recall that the extended Euclidean algorithm, which incorporates the Euclidean algorithm, not only finds g but also finds integers a and b such that $an_1 + bn_2 = g$.
  (a) Show that for any two points $\mathbf{v} = (v_1, v_2, v_3), \mathbf{w} = (w_1, w_2, w_3)$ on the plane $n_1x + n_2y = z$, that the point $f(\mathbf{v}, \mathbf{w}) = \mathbf{v} - \lfloor v_3/w_3 \rfloor \mathbf{w}$ also lies on this plane.
  (b) Start with points $\mathbf{v} = (1, 0, n_1), \mathbf{w} = (0, 1, n_2)$. At each step of the algorithm, replace the pair of points $(\mathbf{v}, \mathbf{w})$ by the pair $(\mathbf{w}, f(\mathbf{v}, \mathbf{w}))$, which then become the new pair of points $(\mathbf{v}, \mathbf{w})$. Show that eventually $w_3 = 0$. Stop the algorithm at this point.

(c) Prove in general that, when the algorithm stops, then $v_3 = g$ and $v_1 n_1 + v_2 n_2 = g$.

(8) A Chinese army is arrayed in Tiananmen square. When arrayed in columns of 100 soldiers, there are 81 left over, when arrayed in columns of 101 soldiers there are 4 left over and when arrayed in columns of 103 soldiers there are 14 left over. Given that there are less than a million soldiers in the square, exactly how many are there?

(9) Show that the system of equations

$$\begin{aligned} 5x + 7y - 2z + 10w &= 13 \\ 4x + 11y - 7z + 17w &= 11 \end{aligned}$$

has no integers solutions.

(10) Find the general integer solution (x, y, z) to the pair of equations

$$\begin{aligned} 3x + 4y + 7z &= 1 \\ 5x + 9y + 2z &= 3. \end{aligned}$$

(11) Find the general integer solution to the system of equations

$$\begin{aligned} 3x + 4y - 5z + 6w &= 8 \\ 4x + 7y - 9z + 3w &= 5 \\ 5x - 8y + 4z - 2w &= -1. \end{aligned}$$

(12) Find the general integer solution to the equation

$$ax_1 + (ka + 1)x_2 + a_3 x_3 + \cdots + a_n x_n = c.$$

Here $a, k, c, a_3, \ldots, a_n$ are given integers.

(13) (a) Let A be an $n \times m$ integer matrix with $n < m$. Show that the equation $A\mathbf{x} = \mathbf{0}$ has a nonzero integer solution $\mathbf{x}$.

(b) For the same A, and $\mathbf{b} \in \mathbb{Z}^n$, show that the equation $A\mathbf{x} = \mathbf{b}$ has either no integral solutions $\mathbf{x}$ or infinitely many.

/home/chris/NTh/wkp2_12.tex