Monday: Linear Diophantine equations and cancellation laws

Linear Diophantine equations

A *Diophantine equation* is an algebraic equation (e.g. $ax^2 + bx + cxy = d$) in which the coefficients (a, b, c and d) are integers, and for which we seek integer solutions x and y. We will consider the special case of *linear* Diophantine equations, which are of the form

$$ax + by = c, \qquad (*)$$

where $a, b, c \in \mathbb{Z}$: we seek all integers x and y satisfying the equation $(*)$. Of course, if x and y were allowed to be real numbers, then $(*)$ would be the equation of a straight line: we ask when this straight line intersects the lattice of points $\mathbb{Z}^2 = \{ (x, y) : x, y \in \mathbb{Z} \}$. In general, a straight line could intersect $\mathbb{Z}^2$ in no points (e.g. $y = x + \sqrt{2}$), in one point (e.g.$y = \sqrt{2}x$, which intersects Z^2 only at the point $(0, 0)$) or infinitely often (e.g. $y = x$). When we insist on integer coefficients only the first and the third possibilities occur.

We will ignore the case when $a = 0$ or $b = 0$: that case is easy to deal with. So for the rest of this section we will assume that $a, b \neq 0$. Put $d = \gcd(a, b)$. We know that $d \mid a$ and $d \mid b$, so for any $x, y \in \mathbb{Z}$ we have $d \mid ax + by$. Thus if $(*)$ has a solution, we must have $d \mid c$: if $d \nmid c$ then no solution is possible.

Example 1. *The equation $2x + 4y = 3$ has no solutions: if x and y satisfied the equation, then the left hand side would be even but the right hand side would be odd.*

So suppose that $d \mid c$, in other words $c = dq$ for some q. Now, we know that there exist $x_d, y_d \in \mathbb{Z}$ with $d = ax_d + by_d$. Multiplying by q we get $dq = ax_dq + by_dq$, i.e. $c = a(x_dq) + b(y_dq)$. Thus (x_dq, y_dq) is a solution of $(*)$.

Example 2. *Find a solution to the equation $4x + 7y = 13$.*

What about the general solution? What happens if we try to prove the solution is unique?

Suppose that (x, y) and (x', y') are solutions. Then we have

$$ax + by = c = ax' + by',$$

so $a(x - x') + b(y - y') = 0$, or $a(x - x') = b(y' - y)$. Does this imply that $x - x' = y' - y = 0$? No, it only implies that the number $a(x - x')$ is a common multiple of a and b. If m is any common multiple of a and b, say $m = ra = sb$, then we can put $x' = x - r$, $y' = y + s$ to get

$$a(x - x') + b(y - y') = a(x - (x - r)) + b(y - (y + s)) = ar - bs = m - m = 0,$$

as required. So the general solution is given by $x = x_d - m/a$, $y = y_d + m/b$, where m is a common multiple of a and b. Note that m is a common multiple of a and b if and only if $\operatorname{lcm}(a, b) \mid m$. So the general solution is $x = x_d - tl/a$, $y = y_d + tl/b$, where $l = \operatorname{lcm}(a, b)$ and $t \in \mathbb{Z}$. Also we know that $ld = ab$, (see Chapter Zero 6.2.19) so $l/a = b/d$ and $l/b = a/d$.

We can prove this by showing $\operatorname{lcm}(a, b) \mid ab$ and hence that if $ab = k \operatorname{lcm}(a, b)$ then k is a common divisor of a and b. Likewise $\gcd(a, b) \mid ab$ and so if $ab = l \gcd(a, b)$ then l is a common multiple of a and b. Now by 6.2.8. ($a \mid b \wedge b \mid a \implies a = \pm b$) and the fact that the only k, l which can satisfy both is $k = \gcd(a, b)$ and $l = \operatorname{lcm}(a, b)$.

Combining these facts we have the following theorem.

Theorem 3. *Let $a, b, c \in \mathbb{Z}$ with $a, b \neq 0$. Put $d = \gcd(a, b)$, and fix $x_d, y_d \in \mathbb{Z}$ with $d = ax_d + by_d$. Then the equation $ax + by = c$ has no integer solutions if $d \nmid c$, and has the general solution $x = x_d - tb/d$, $y = y_d + ta/d$ for $t \in \mathbb{Z}$ if $d \mid c$.*

Example 4. *Find the general solution of the Diophantine equation $4x + 7y = 13$.*

Example 5. *Find the general solution of the Diophantine equation $6x - 15y = 27$.*

Cancellation laws

In $\mathbb{Z}$ we have two cancellation laws: "if $a + c = b + c$ then $a = b$" and "if $ac = bc$ and $c \neq 0$ then $a = b$". The first is easy to prove from the axioms: if $a + c = b + c$ then we have

$$\begin{aligned} (a + c) + (-c) &= (b + c) + (-c) \\ a + (c + (-c)) &= b + (c + (-c)) && \text{(associative law)} \\ a + 0 &= b + 0 && \text{(definition of } -c\text{)} \\ a &= b && \text{(definition of 0)} \end{aligned}$$

However, we don't have multiplicative inverses as we do additive inverses. Of course we could jump outside $\mathbb{Z}$ and into $\mathbb{Q}$, and multiply both sides by $\frac{1}{c}$, but that relies on other things, not on the axioms for the integers. To get the cancellation law from the axioms alone, we would have to do a little work. One way to prove it would be to prove by induction that the result holds for all $c \in \mathbb{N}$, and then extend the result to negative values of c. We will leave this as an exercise.

Tuesday: Class Test

Thursday: Congruence Modulo n

When we considered equivalence relations we had as an example the relation $\sim$ on $\mathbb{Z}$ defined by declaring that for $m, n \in \mathbb{Z}$ we have

$$m \sim n \iff 5 \mid m - n.$$

We showed that $\sim$ is an equivalence relation. This relation is called *congruence modulo 5*. In general, if $n \in \mathbb{N}$ we say that a and b are congruent modulo n if $n \mid a - b$: we write this relation $a \equiv b \pmod{n}$. This relation is an equivalence relation for every $n \in \mathbb{N}$. The set of equivalence classes is called the *integers modulo n*, written $\mathbb{Z}_n$. For $a \in \mathbb{Z}$, we call the equivalence class of a under congruence modulo n the *congruence class* of a, and denote it by $\overline{a}$.

Example 6. *Fix $n = 5$. Find $\overline{0}$, $\overline{1}$, $\overline{10}$ and $\overline{16}$.*

Lemma 7. *Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Then $a \equiv b \pmod{n}$ iff a and b give the same remainder when divided by n.*

From this we know that there are exactly n congruence classes in $\mathbb{Z}_n$, because there are n possible remainders $0, 1, \ldots, n - 1$. So we have

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

The set $\mathbb{Z}_n$ inherits some properties from $\mathbb{Z}$. The most important is that we can define addition and multiplication on $\mathbb{Z}_n$ in a natural way.

Definition. *We define the operations $+_n$ and $\cdot_n$ on $\mathbb{Z}_n$ by declaring that, for $a, b \in \mathbb{Z}$,*

$$\overline{a} +_n \overline{b} = \overline{a+b} \qquad \textit{and} \qquad \overline{a} \cdot_n \overline{b} = \overline{ab}.$$

Of course we can write down any definition we like: we could define n to be the least positive solution of the equation $x = x + 1$.... For this definition to make sense we have to make sure that the operations are *well-defined*. For example, with $n = 5$, consider finding $\overline{3} +_5 \overline{7}$ and finding $\overline{18} +_5 \overline{22}$. We have

$$\overline{3} +_5 \overline{7} = \overline{3+7} = \overline{10} = \overline{0} \qquad \text{and} \qquad \overline{18} +_5 \overline{22} = \overline{18+22} = \overline{40} = \overline{0}.$$

Thus we get the same answer both times. This is just as well, because $\overline{3} = \overline{18}$ and $\overline{7} = \overline{22}$, so we were doing the same sum in both cases.

For the definitions of $+_n$ and $\cdot_n$ to make sense, we must ensure that if $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$ then we get the same answer when we work out $\overline{a} +_n \overline{b}$ and when we work out $\overline{a'} +_n \overline{b'}$, and similarly for $\cdot_n$. In other words, we must show that if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ then $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

Lemma 8. *Let $a, b, a', b' \in \mathbb{Z}$, $n \in \mathbb{N}$. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ then $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.*

To understand what we have done we should see an example where the operations would not be well defined.

Example 9. *Partition $\mathbb{Z}$ into the three sets $\Omega = \{A, B, C\}$*

$$\begin{aligned} A &= \mathbb{N} \\ B &= \{0\} \\ C &= \{\, -n : n \in \mathbb{N} \,\}. \end{aligned}$$

We try to define addition $+'$ and multiplication $\cdot'$ by taking a representative from the two classes we are adding, adding or multiply together the representatives, and finding the equivalence class of the answer. For example we have $A \cdot' B = B$ because $n \cdot 0 = 0 \in B$ for every $n \in A$, and $A \cdot' C = C$ because $m \cdot (-n) = -(mn) \in C$ for every $m \in A$, $-n \in C$. However, addition is **not** *well-defined: when we try to find $A +' C$ we could get the answer A (for example by choosing the representatives 8 and -3), B (e.g. by choosing 6 and -6) or C (e.g. by choosing 5 and -12). The answer we get depends not just on the classes but on which representative of the classes we choose.*

What can we say about arithmetic modulo n? We know that the operations $+_n$ and $\cdot_n$ are commutative and associtive, and $\cdot_n$ distributes over $+_n$. To show the last one, let $a, b, c \in \mathbb{Z}$. Then

$$\begin{aligned} \overline{a} \cdot_n (\overline{b} +_n \overline{c}) &= \overline{a} \cdot_n \overline{b+c} \\ &= \overline{a(b+c)} \\ &= \overline{ab+ac} \\ &= \overline{ab} +_n \overline{ac} \\ &= \overline{a} \cdot_n \overline{b} +_n \overline{a} \cdot_n \overline{c}. \end{aligned}$$

The commutative and associative laws follow similarly from the commutative laws and associative laws for $\mathbb{Z}$.

Friday: Division in $\mathbb{Z}_n$

The cancellation laws in $\mathbb{Z}_n$

Recall that in $\mathbb{Z}$ we have two cancellation laws: $a+c=b+c$ implies $a=b$, and $ac=bc$ implies $a=b$ for $c \neq 0$. The first of these laws carries over to $\mathbb{Z}_n$, because we can use the same argument as we did for $\mathbb{Z}$: the element $\overline{a}$ has an additive inverse $\overline{-a}$. However, the cancellation law for $\cdot_n$ does not always work. For example, fix $n=12$. Then we have $\overline{3} \cdot_{12} \overline{4} = \overline{12} = \overline{0}$, and $\overline{6} \cdot_{12} \overline{4} = \overline{24} = \overline{0}$, so $\overline{3} \cdot_{12} \overline{4} = \overline{6} \cdot_{12} \overline{4}$, but $\overline{3} \neq \overline{6}$.

The problem is that we cannot divide both sides of the equation $\overline{3} \cdot_{12} \overline{4} = \overline{6} \cdot_{12} \overline{4}$ by $\overline{4}$. What would division mean? When might division work? What should $\dfrac{\overline{a}}{\overline{b}}$ mean when $\overline{a}, \overline{b} \in \mathbb{Z}_n$?

In $\mathbb{Q}$, the fraction $\frac{a}{b}$ is the unique solution x of the equation $a = bx$. So the problem becomes the question of whether the equation $\overline{a} = \overline{b} \cdot_n \overline{x}$ has a unique solution $\overline{x}$. In general, this equation could have no solutions, a unique solution, or more than one solution.

Example 10. *Consider the equation $\overline{6} = \overline{4} \cdot_n \overline{x}$. Show that this equation has*

- *no solutions when $n = 8$*
- *two solutions when $n = 10$*
- *a unique solution when $n = 15$.*

Now, if $\overline{a} = \overline{b} \cdot \overline{x}$ has a solution $\overline{x}$, then $a \equiv bx \pmod{n}$, so $a = bx + ny$ for some $y \in \mathbb{Z}$. From our discussion of Diophantine equations, we know this happens if and only if $\gcd(b, n) \mid a$. In particular, if $\gcd(b, n) = 1$, then this equation has a solution for all a. Further, the solution will be unique:

Theorem 11. *Let $a, b \in \mathbb{Z}$, $x \in \mathbb{N}$. If b and n are relatively prime then the equation $\overline{a} = \overline{b} \cdot_n \overline{x}$ has a unique solution $\overline{x} \in \mathbb{Z}_n$.*

Corollary 12. *If p is a prime number then for every $b \not\equiv 0 \pmod{p}$ the equation $\overline{a} = \overline{b} \cdot_p \overline{x}$ has a unique solution in $\mathbb{Z}_p$.*

Thus, division works in $\mathbb{Z}_p$ just the same as it does in $\mathbb{Q}$ and $\mathbb{R}$. We will return to this example, which is an example of a *field*, when we discuss the axioms for the real numbers in Chapter 8.