Introduction to modular arithmetic S1

Diophantine Equations

Diophantus - born probably sometime between AD 201 and 215; died around 84 years old, probably sometime between AD 285 and 299 was an Alexandrian Hellenistic mathematician.

Note the convention used throughout. A dot (.), unless at the end of a sentence, always stands for multiplication, e.g., $3.2 = 6$ (and not 3 point 2).

Consider the fraction $\frac{54}{11}$. This can be written as

$$54 \div 11 = 54/11 = \frac{54}{11} = 4\frac{10}{11} = 4 + \frac{10}{11} = 4.\frac{11}{11} + \frac{10}{11} = \frac{44+10}{11} = \frac{54}{11}.$$

But note that we can also write $\frac{54}{11}$ as

$$\frac{54}{11} = 5 - \frac{1}{11}.$$

The point of doing this is to get the numerator of the fraction as small as possible. You can see that the numerator 1 in $\frac{1}{11}$ is smaller than the numerator in $\frac{10}{11}$. We shall use this idea often.

Oranges and Lemons

Example 1

Oranges cost 7c and lemons cost 5c. I spend a total of 26c. How many oranges and lemons did I buy?

If x = number of oranges and y = number of lemons then

$$7x + 5y = 26.$$

Can you guess a solution?

This is one equation in two variables and would therefore appear to have an infinite number of solutions. Give x any value you like and you can solve and get a value for y, or vice versa.

But there is one unstated fact that is involved.

It is that the solution must be in integers - you cannot have, say, $2\frac{3}{4}$ oranges for example.This makes solutions possible.

A reduction procedure.

Divide the equation by the *smallest coefficient* of the variables - which is 5, to get

$$\begin{aligned} x + \frac{2x}{5} + y &= 5 + \frac{1}{5} \\ \text{or } x + \frac{2x-1}{5} + y &= 0. \end{aligned}$$

Now x and y are integers, so $\frac{2x-1}{5}$ *must be an integer.* Let $\frac{2x-1}{5} = z$ (an integer). Then we have the equation

$$2x = 5z + 1.$$

Divide the equation by the *smallest coefficient* of the variables - which is 2, to get

$$x = 2z + \frac{z+1}{2}.$$

So then, again, x, z are integers so $\frac{z+1}{2}$ must be an integer. Let $\frac{z+1}{2} = t$ (an integer). Then we have the equation

$$z = 2t - 1.$$

And now we are at an end. Starting with x and y, we can express each of these in terms of z, but the equation $2x = 5z + 1$ did NOT have a coefficient of 1 for either variable so we had to go to another equation, with another variable t, namely $z = 2t + 1$. And here z has coefficient 1.

So now we can go backward, getting every variable in terms of t. Then, substituting for z

$$\begin{aligned} x &= 2(2t-1) + t = 5t - 2. \\ y &= \frac{26 - 7x}{5} = \frac{26 - 7(5t-2)}{5} = \frac{40 - 35t}{5} = 8 - 7t. \end{aligned}$$

Now we can give t any integer value and the values of x and y we get will satisfy the original equation $7x + 5y = 26$. There are an infinite number of solutions, just by giving t various integer values. This might result in some values of x and y being +ve and/or -ve.

For our problem, we do not want a negative number of oranges or lemons. Thus we require $x > 0$ and $y > 0$. That is

$$\begin{aligned} x &= 5t - 2 > 0 \\ y &= 8 - 7t > 0. \end{aligned}$$

From the second we must have $t \leq 1$ and considering this in the first inequality we must have $t > \frac{2}{5}$, so that $\frac{2}{5} < t \leq 1$. This is only possible if $t = 1$. Then

$$\begin{aligned} x &= 3 \\ y &= 1. \end{aligned}$$

The solution is 3 oranges and 1 lemon.

CHECK

$$7.3 + 5.1 = 26 \qquad \text{correct!}$$

Example 2

Oranges now cost 97c and lemons 54c. A total of $32.25 is spent. How many oranges and lemons are bought?

If x = number of oranges and y = number of lemons the relevant equation is

$$97x + 54y = 3225.$$

We will divide by the smallest coefficient, 54. But let us be a bit clever here. On dividing by 54, we would usually write for the lhs $x + \frac{43x}{54}$. The coefficient, 43 of x is large - we would like to have the smallest coefficient as possible - ideally, as we proceed we would like to see just $1x$, that is, just x. Instead now, let's go just over 97 and subtract, as in

$2x - \frac{11x}{54}$ - clearly 11 is smaller than 43.

Dividing by 54 we have (trying to get a smaller coefficient of x in the fraction)

$$\begin{aligned} 2x - \frac{11x}{54} + y &= 59 + \frac{39}{54} \\ &= 60 - \frac{15}{54} \end{aligned}$$

where, simillarly. we have produced a smaller numerator 15 compared with 39.

Now taking $-\frac{11x}{54}$ over to the rhs we have the 'fraction' $\frac{11x}{54} - \frac{15}{54}$; but this must be an integer as everything else in the equation is. So we put

$$11x - 15 = 54z \qquad \text{(z integral)}$$

Dividing by the smallest coefficient 11 we get

$$x - 1 - \frac{4}{11} = 5z - \frac{z}{11}.$$

Therefore, again the fraction '$\frac{4}{11} - \frac{z}{11}$' must be an integer. So put

$$4 - z = 11t \qquad \text{(t integral)}.$$

Then, with $z = 4 - 11t$ we get

$$\begin{aligned} x &= 1 + 5(4 - 11t) + t \\ &= 21 - 54t. \end{aligned}$$

Again, to shorten the route of backward substitutions, substitute for x directly in the original equation, to get y. We have

$$\begin{aligned} 54y &= -97(21 - 54t) + 3225 = 97.54t + 1188 \\ y &= 97t + 22. \end{aligned}$$

We now wish for positive numbers of oranges and lemons - that is, $x > 0$ and $y > 0$, so that

$$\begin{aligned} x &= 21 - 54t > 0 \\ y &= 97t + 22 > 0. \end{aligned}$$

If $t \geq 1$, x will be -ve, and if $t \leq -1$, y will be -ve. The first inequality means $t \leq 0$, and the second means $t \geq 0$. The only solution occurs when $t = 0$ so that

$$\begin{aligned} x &= 21 \text{ oranges} \\ y &= 22 \text{ lemons}. \end{aligned}$$

Exercise

Solve in integers the equations

$$\begin{aligned} 3x - 6y + 16z &= 1 \\ 2x + 5y - 6z &= 2. \end{aligned}$$

Solve the first equation for x, y, z in terms of two variables. Use this in the second equation to get x, y, z in terms of one variable. What +ve solutions are there, if any?

Modular arithmetic

Ways of writing $\frac{22}{7}$,

$$22 \div 7 = 22/7 = \frac{22}{7} = 3\frac{1}{7} = 3 + \frac{1}{7} = 3.\frac{7}{7} + \frac{1}{7} = \frac{21}{7} + \frac{1}{7} = \frac{22}{7}.$$

We can also think of 22 divided by 7, which goes in 3 times leaving a remainder of 1, that is

$$22 = 3.7 + 1.$$

Write this instead as

$$22 = 1 + 3.7.$$

We now introduce the notation of a congruence, from this example, by writing

$$22 \equiv 1 (\mathrm{mod}\, 7)$$

which means 22 - 1 is divisible by 7. The wording is, (we read it as): 22 is congruent to $1 (\mathrm{mod}\, 7)$.

Obviously we can add or subtract multiples of 7 to each side, since it will still be true that the difference between left and right hand sides of the congruence is divisible by 7. Thus

$$\begin{aligned} 29 &\equiv 1 (\mathrm{mod}\, 7) \\ 22 &\equiv 15 (\mathrm{mod}\, 7) \\ 99 &\equiv 22 (\mathrm{mod}\, 7) \\ 99 &\equiv -13 (\mathrm{mod}\, 7) \end{aligned}$$

$$\begin{aligned} 1^6 &\equiv 1 (\mathrm{mod}\, 7) \\ 2^6 &= 64 \equiv 1 (\mathrm{mod}\, 7) \\ 3^6 &= 729 \equiv 1 (\mathrm{mod}\, 7) \\ 4^6 &= 4096 \equiv 1 (\mathrm{mod}\, 7) \\ 5^6 &= 15625 \equiv 1 (\mathrm{mod}\, 7) \\ 6^6 &= 46656 \equiv 1 (\mathrm{mod}\, 7) \end{aligned}$$

Does it seem strange/interesting to you that the same power (6) of these numbers all have a remainder of 1 when divided by 7? Yet, for example, 3^3 is not congruent to $1 (\mathrm{mod}\, 4)$, nor is 2^3. Why does this happen?

When we write

$$a \equiv b (\mathrm{mod}\, m)$$

we mean that a divided by m leaves a remainder of b. Written as an equation, rather than a congruence, this is

$$a = b + k.m \qquad \text{where } k \text{ is some integer (compare } 22 = 1 + 3.7).$$

In mathematics, fractions, are called *rational numbers*.

We have the following notation for sets of numbers
$\mathbb{N}$ - set of natural numbers $\{0, 1, 2, \ldots\}$
$\mathbb{Z}$ - set of integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Q}$ - set of rational numbers $\{\frac{p}{q} \quad | \quad p, q \in \mathbb{Z}, q \neq 0\}$
$\mathbb{R}$ - set of real numbers - generally defined by a 'Dedekind cut' on the real line of numbers
$\mathbb{C}$ - set of complex numbers $\{a + bi \quad | \quad a, b \in \mathbb{R},\ i^2 = -1\}$

In modular arithmetic we only deal with integers (numbers belonging to the set $\mathbb{Z}$).
Observe the following

$$13 \equiv 7 \pmod 3$$

We read this as "13 is congruent to 7 mod 3". What this means is that $13 - 7$ is divisible by 3. That is, $13 - 7 = 3k$ where k is some integer - or $13 = 7 + 3k.(k = 2)$

Note that

$$13 \equiv 7 \pmod 2$$

also.

Note also that we can add or subtract multiples of 2 from either side if we wish. Thus

$$13 = 11 + 2 \equiv 7 \pmod 2$$

Writing in full form this is

$$11 + 2 = 7 + 2k_1 \qquad \text{where } k_1 \text{ is an integer}$$

So, it is equally true that

$$11 = 7 + 2(k_1 - 1)$$

so it is equally true

$$\begin{aligned} 11 &\equiv 7 \pmod 2 \\ \text{or also } 11 &\equiv 5 \pmod 2 \\ \text{or also } 13 &\equiv 3 \pmod 2 \\ &\text{etc.} \end{aligned}$$

If an integer N is divisible by an integer m we have $N = km$ where k is an integer. Putting this in modular form we can write

$$N \equiv 0 \pmod m.$$

The integer m is called the *modulus*.

Examples of (A) adding congruences, (B) mulitplying both sides of a congruence by any integer, (C) multiplying two (and hence any number) of congruences together. In all case the result is a valid congruence.

We consider the congruences

$$\begin{aligned} 20 &\equiv 2 \pmod 6 \\ 21 &\equiv -3 \pmod 6 \end{aligned}$$

(A) Adding each side of the two congruences gives

$$41 \equiv -1 (\mathrm{mod}\, 6)$$

and indeed this is true. So we can add - or also subtract any number of congruences.

(B) Multipying the first congruence by, say, -5, gives

$$-100 \equiv -10 (\mathrm{mod}\, 6)$$

and this is a valid congruence.

(C) Multiplying the first and second congruences (left and right-hand sides) gives

$$420 \equiv -6 (\mathrm{mod}\, 6)$$

and this too is true as a congruence.

Simple proofs of these propositions are given next.

Proposition 1

In general notation, suppose

$$\begin{aligned} a &\equiv b \ (\mathrm{mod}\, m), \text{ and} \\ c &\equiv d \ (\mathrm{mod}\, m) \end{aligned}$$

Then we can add or subtract congruences, so that

$$a \pm c \equiv b \pm d \ (\mathrm{mod}\, m).$$

Proof:

We have

$$\begin{aligned} a &= b + k_1 m \qquad \text{where } k_1 \text{ is an integer} \\ c &= d + k_2 m \qquad \text{where } k_2 \text{ is an integer} \end{aligned}$$

Adding or subtracting we have

$$a \pm c = b \pm d + (k_1 \pm k_2) m$$

which means

$$a \pm c \equiv b \pm d \ (\mathrm{mod}\, m).$$

Proposition 2

With the same notation as above if k is any integer, it is obvious that

$$ka \equiv kb \ (\mathrm{mod}\, m)$$

So we can multiply any congruence by any integer and it is still true.

Proposition 3
With the same notation as above

$$ac \equiv bd \pmod{m}.$$

Proof:
We have, from above,

$$ac = bd + (bk_2 + dk_1 + k_1k_2m)m$$

So in any case

$$ac \equiv bd \pmod{m}.$$

Can you make up a numerical example to illustrate props 1, 2 and 3?
In particular, if $c = a$ and $d = b$, we have

$$\begin{aligned} a^2 &\equiv b^2 \pmod{m} \\ a^3 &\equiv b^3 \pmod{m} \\ &\cdots \\ a^n &\equiv b^n \pmod{m} \end{aligned}$$

Think for example of a as large and b as small. For instance

$$\begin{aligned} 23 &\equiv 3 (\mathrm{mod}\, 5) \\ \text{so } 279841 &= 23^4 \equiv 81 \equiv 1 \,\mathrm{mod}(5) \end{aligned}$$

We will develop this further, later.

Modular equations
Can we solve for x in the equation

$$17x \equiv 3 \pmod{5}$$

This is the same as the congruence

$$15x + 2x \equiv 2x \equiv 3 \pmod{5}.$$

Multiply the congruence by 3 on both sides, aiming to get a single x on the lhs

$$6x \equiv x \equiv 9 \equiv 4 \pmod{5}.$$

There we have the solution of the congruence, CHECK

$$17.4 = 68 \equiv 3 \pmod{5}.$$

Example2 Oranges and lemons
We have the equation

$$97x + 54y = 3225.$$

Write this as a congruence

$$97x \equiv 3225 \pmod{54}$$

Use your calculator here to write

$$\begin{aligned} 97x &= 108x - 11x \equiv 60.54 - 15 \pmod{54} \\ \text{or } -11x &\equiv -15 \pmod{54} \\ \text{or } 55x &\equiv 75 \pmod{54} \\ \text{or } x &\equiv 21 \pmod{54} \end{aligned}$$

Therefore

$$x = 21 + 54t \qquad \text{where } t \text{ is some integer}$$

Then substituting for x in the original equation $97x + 54y = 3225$ we get

$$\begin{aligned} 54y &= 1188 - 97.54t \\ \text{or } y &= 22 - 97t. \end{aligned}$$

Now again we require, $x > 0$, $y > 0$ so that

$$\begin{aligned} x &= 21 + 54t > 0 \\ y &= 22 - 97t > 0 \end{aligned}$$

For +ve (positive) solutions this is only possible if $t = 0$ whereupon

$$\begin{aligned} x &= 21 \\ y &= 22. \end{aligned}$$

CHECK

$$97.21 + 54.22 = ?$$