Appendix week 9

Why look at Diophantine Equations?

Example 1 *Alison spends £6.20 on sweets for prizes in a contest. If a large box of sweets costs 50p and a small box 20p, how many boxes of each size did she buy?*

With her £6.20, Alison could have gone into another shop where the large box of sweets cost 49p and the small box 21p. What is the maximum she could have spent on sweets and how many boxes of each size would she have got for her money?

Solution Left to student - but you can see why we require the answers to be integers.

The general solution of $am + bn = c$.

Theorem 2 *If $am + bn = c$ is soluble and (m_0, n_0) is a solution, then all solutions are given by*

$$\left(m_0 - \frac{b}{\gcd(a,b)}t, n_0 + \frac{a}{\gcd(a,b)}t\right)$$

with $t \in \mathbb{Z}$.

Proof Write $d = \gcd(a,b)$, so $d|a$ and $d|b$. Thus there exist $u, v \in \mathbb{Z}$ such that $a = ud$ and $b = vd$. Then by Corollary in the notes,

$$\gcd(u,v) = \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Let $(m,n) \in \mathbb{Z}^2$ be any solution of $ax + by = c$. Then we have both of

$$\begin{aligned} am_0 + bn_0 &= c, \\ am + bn &= c. \end{aligned}$$

Subtract to get

$$a(m_0 - m) = b(n - n_0).$$

Divide through by d to get

$$u(m_0 - m) = v(n - n_0). \quad (1)$$

Since the left hand side is a multiple of u we have $u|v(n-n_0)$. But $\gcd(u,v)=1$ so, by Corollary in notes, $u|(n-n_0)$. That is, $n-n_0=ut$, for some $t\in\mathbb{Z}$.

Substitute back into (1) to get $u(m_0-m)=v(ut)$, i.e. $m_0-m=vt$. Then **all** solutions must be of the form

$$\begin{aligned}(m,n) &= (m_0-vt, n_0+ut) = \left(m_0-\frac{b}{d}t, n_0+\frac{a}{d}t\right)\\ &= \left(m_0-\frac{b}{\gcd(a,b)}t, n_0+\frac{a}{\gcd(a,b)}t\right),\end{aligned}$$

for $t\in\mathbb{Z}$.

We must, in fact, show that these **are** solutions of the equation. But, for any $t\in\mathbb{Z}$,

$$\begin{aligned}&a\left(m_0-\frac{b}{\gcd(a,b)}t\right)+b\left(n_0+\frac{a}{\gcd(a,b)}t\right)\\ &= (am_0+bn_0)+\left(-\frac{ab}{\gcd(a,b)}t+\frac{ba}{\gcd(a,b)}t\right)\\ &= am_0+bn_0=c,\end{aligned}$$

as required. ■

An alternative way to solve some linear congruences.

Example 3 *Solve* $5x\equiv 6 \bmod 19$.

Solution TRICK We can change any coefficients by adding multiples of 19, as in

$$5x\equiv 6\equiv 6+19\equiv 25 \bmod 19.$$

Recall by part ii) of a theorem above, if $ab_1\equiv ab_2 \bmod m$ and $\gcd(a,m)=1$ then we can divide by a to get $b_1\equiv b_2 \bmod m$.

In the present example this means we can divide by 5 to get $x\equiv 5 \bmod 19$. ■

Advice, Only look for alternative ways to solve congruences *if it doesn't take you too long to do.* But, if in doubt, use Euclid's Algorithm to solve $ax\equiv b \bmod m$.

An example of the use of congruences

Theorem 4 *The integer $a_r a_{r-1} ... a_2 a_1 a_0$ $(r \geq 1)$ in decimal notation is divisible by 11 if, and only if,*

$$a_r (-1)^r + a_{r-1} (-1)^{r-1} + ... + a_2 - a_1 + a_0,$$

i.e. the sum of digits with alternating sign, is divisible by 11.

For example, 2592579 is divisible by 11 since $2-5+9-2+5-7+9 = 11$, which is divisible by 11. For an even larger example 918291829173928171 93 has an alternating sum of 66. If you can't remember your 11 times table you can repeat the method on 66 which has an alternating sum of 0, divisible by 11.

Proof First note that if

$$a \equiv b \bmod 11 \quad \text{and} \quad 11|b \quad \text{then} \quad 11|a.$$

So it suffices to prove that

$$a_r a_{r-1} ... a_2 a_1 a_0 \equiv a_r (-1)^r + a_{r-1} (-1)^{r-1} + ... + a_2 - a_1 + a_0 \bmod 11,$$

for if 11 divides the alternating sum on the right it must divide $a_r a_{r-1} ... a_2 a_1 a_0$ as required.

Next note that

$$10 \equiv -1 \bmod 11 \quad \text{and so} \quad 10^n \equiv (-1)^n \bmod 11$$

for all $n \geq 1$. Thus

$$\begin{aligned} a_r a_{r-1} ... a_2 a_1 a_0 &= a_r 10^r + a_{r-1} 10^{r-1} + ... + a_2 10^2 + a_1 10 + a_0 \\ &\equiv a_r (-1)^r + a_{r-1} (-1)^{r-1} + ... \\ &\qquad ... + a_2 (-1)^2 + a_1 (-1) + a_0 \bmod 11 \\ &\equiv a_r (-1)^r + a_{r-1} (-1)^{r-1} + ... + a_2 - a_1 + a_0 \bmod 11, \end{aligned}$$

as required. ■

Example Is $2^{40} - 1$ divisible by 11?

Solution From a calculator $2^{40} - 1 = 1099511627775$. Here $r = 12$ and so we consider

$$1 - 0 + 9 - 9 + 5 - 1 + 1 - 6 + 2 - 7 + 7 - 7 + 5 = 0.$$

This is divisible by 11 as, is thus, $2^{40} - 1$. ■

Question for students. Find other factors of $2^{40} - 1$.

Example Is $2^{35} + 1$ divisible by 11?

Solution From a calculator $2^{35} + 1 = 34359738369$. Hence $r = 10$ and so we consider

$$3 - 4 + 3 - 5 + 9 - 7 + 3 - 8 + 3 - 6 + 9 = 0.$$

This is divisible by 11 as is thus $2^{35} + 1$. ■

Question for students. Use the method of successive squaring to find $2^{35} \bmod 11$ and thus give an alternative proof of $2^{35} + 1 \equiv 0 \bmod 11$.

The number of solutions of a congruence.

Theorem 5 *The congruence* $ax \equiv c \,(\operatorname{mod} m)$ *is soluble in integers if, and only if,* $\gcd(a,m)\,|c$. *The number of incongruent solutions modulo* m *is* $\gcd(a,m)$.

Proof The ideas for this proof can be found around p.244. But simply,

$$\begin{aligned} & \exists x \in \mathbb{Z} : ax \equiv c \,(\operatorname{mod} m) \\ \Leftrightarrow\ & \exists x, w \in \mathbb{Z} : ax = c + wm \\ \Leftrightarrow\ & \exists x, y \in \mathbb{Z} : ax + my = c, \end{aligned}$$

having written y for $-w$. We have seen that such integer solutions exist if, and only if, $\gcd(a,m)\,|c$. And we have also seen that if (x_0, y_0) is a solution of $ax + my = c$ then all solutions are given by

$$\left(x_0 + \frac{m}{d}t, y_0 - \frac{a}{d}t\right),$$

for $t \in \mathbb{Z}$, and where $d = \gcd(a,m)$. Two solutions to our original congruence, $x_0 + (m/d)\,t_1$ and $x_0 + (m/d)\,t_2$, are the same, i.e. ***congruent*** modulo m, if and only if

$$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \operatorname{mod} m.$$

Writing $m = (m/d) \times d$ we get

$$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \operatorname{mod} \left(\frac{m}{d}d\right).$$

Apply Theorem (i) above and divide through by m/d to obtain $t_1 \equiv t_2 \operatorname{mod} d$, i.e. $t_1 \equiv t_2 \operatorname{mod} \gcd(a,m)$.

Thus *incongruent* solutions are obtained by choosing $t_1 \not\equiv t_2 \operatorname{mod} \gcd(a,m)$. Hence all incongruent solutions are obtained on choosing

$$t = 0, 1, 2, ..., \gcd(a,m) - 1.$$

■

More examples of Pairs of congruences

Example 6 *Solve*

$$2x \equiv 3 \bmod 5 \quad \textit{and} \quad 3x \equiv 4 \bmod 7.$$

Solution. *First, solve each individual congruence.* The easiest way is to find the inverse of the coefficients of x.

Note that $3 \times 2 \equiv 1 \bmod 5$ so, on multiplying both sides by 3, the first congruence becomes $x \equiv 3 \times 3 \equiv 4 \bmod 5$.

Next, $5 \times 3 \equiv 1 \bmod 7$ so, on multiplying both sides by 3, the second congruence becomes $x \equiv 5 \times 4 \equiv 6 \bmod 7$.

Hence we have the system

$$x \equiv 4 \bmod 5 \quad \text{and} \quad x \equiv 6 \bmod 7.$$

Second, solve the pair of congruences. To combine these congruences we observe that

$$\begin{aligned} x &\equiv 4 \bmod 5 \Rightarrow x = 4 + 5m \text{ for some } m \in \mathbb{Z}, \\ x &\equiv 6 \bmod 7 \Rightarrow x = 6 + 7n \text{ for some } n \in \mathbb{Z}. \end{aligned}$$

Combine as in

$$4 + 5m = x = 6 + 7n,$$

which rearranges to

$$5m - 7n = 2.$$

All the numbers are small here so simply stare at this to see that $(m_0, n_0) = (6, 4)$ is **a** solution. The general solution follows from

$$5\,(m_0 + 7t) - 7\,(n_0 + 5t) = 1$$

for all $t \in \mathbb{Z}$. Thus the general solution for m is $6+7t$ which can be substituted into $x = 4 + 5m$ to get

$$x = 4 + 5\,(6 + 7t) = 34 + 35t$$

for all $t \in \mathbb{Z}$. So the solution to our simultaneous pair is $x \equiv 34 \bmod 35$. ■

Example 7 *Solve*

$$x \equiv 34 \bmod 35 \quad \textit{and} \quad 5x \equiv 7 \bmod 11.$$

Solution Note that $9 \times 5 \equiv 1 \bmod 11$ so the second congruence becomes, on multiplying both sides by 9,

$$9 \times 5x \equiv 9 \times 7 \bmod 11, \quad \text{i.e.} \quad x \equiv 8 \bmod 11.$$

Thus we have the system

$$x \equiv 34 \bmod 35 \quad \text{and} \quad x \equiv 8 \bmod 11.$$

Then

$$\begin{aligned} x &\equiv 34 \bmod 35 \Rightarrow x = 34 + 35m, \\ x &\equiv 8 \bmod 11 \Rightarrow x = 8 + 11n, \end{aligned}$$

for some $m, n \in \mathbb{Z}$. Equate to get $34 + 35m = x = 8 + 11n$, that is

$$26 = 11n - 35m. \tag{2}$$

To solve this apply Euclid's Algorithm to 35 and 11 :

$$\begin{aligned} 35 &= 3 \times 11 + 2 \\ 11 &= 5 \times 2 + 1. \end{aligned}$$

Reverse the steps to get

$$\begin{aligned} 1 &= 11 - 5 \times 2 \\ &= 11 - 5 \times (35 - 3 \times 11) \\ &= 16 \times 11 - 5 \times 35. \end{aligned}$$

Multiply by 26 to get

$$26 = 11 \times 416 - 35 \times 130.$$

So a solution to (2) is $(n_0, m_0) = (416, 130)$. The general solution follows from

$$\begin{aligned} 26 &= 11\,(n_0 + 35t) - 35\,(m_0 + 11t) \\ &= 11\,(416 + 35t) - 35\,(130 + 11t) \end{aligned}$$

for $t \in \mathbb{Z}$. The general solution for n, of $416 + 35t$ can be substituted into

$$x = 8 + 11n = 8 + 11\,(416 + 35t) = 4584 + 385t.$$

Thus the solution to our simultaneous pair is $x \equiv 4584 \equiv 349 \bmod 385$ ■

Another example of a Triplet of Congruences

Example 8 *Solve the system*

$$2x \equiv 3 \bmod 5, \quad 3x \equiv 4 \bmod 7 \quad \textit{and} \quad 5x \equiv 7 \bmod 11.$$

Solution With 3 or more congruence first solve each congruence separately. Then, take a pair, solve them to replace by a single congruence. Then take this new congruence with an unconsidered one from the original system and solve this pair. Continue.

So, in this example, start by solving

$$2x \equiv 3 \bmod 5 \quad \text{and} \quad 3x \equiv 4 \bmod 7.$$

But this was seen in the first example above, solution $x \equiv 34 \bmod 35$. Combine this new congruence with the remaining congruence from the original system, i.e.

$$x \equiv 34 \bmod 35 \quad \text{and} \quad 5x \equiv 7 \bmod 11.$$

But this was seen in the second example above, solution

$$x \equiv 349 \bmod 385.$$

Check this answer by substituting back in. ■

Chinese Remainder Theorem

We have applied a method above to solve a system of congruences with no assurance (i.e. no proof) that the method will always give a solution. That is, we do not know what conditions on a system of congruences will ensure a solution. In the next two theorems we will give conditions under which a system of congruences has a solution.

Theorem 9 ***Chinese Remainder Theorem*** *(for two linear congruences)*
Let m_1 and m_2 be coprime integers, and a_1, a_2 integers. Then the simultaneous congruences

$$x \equiv a_1 \bmod m_1 \quad \textit{and} \quad x \equiv a_2 \bmod m_2$$

have exactly one solution with $0 \le x_0 \le m_1 m_2 - 1$ and the general solution is $x \equiv x_0 \bmod m_1 m_2$.

Proof (Not in PJE) Since $(m_1, m_2) = 1$ we can find integers b_1, b_2 satisfying the congruences

$$m_2 b_1 \equiv 1 \bmod m_1 \quad \text{and} \quad m_1 b_2 \equiv 1 \bmod m_2.$$

Set

$$x^* = m_2 b_1 a_1 + m_1 b_2 a_2.$$

Then modulo m_1 the second term in x^* vanishes and we have

$$x^* \equiv (m_2 b_1)\, a_1 \equiv a_1 \bmod m_1.$$

Modulo m_2 the first term in x^* vanishes and we have

$$x^* \equiv (m_1 b_2)\, a_2 \equiv a_2 \bmod m_2.$$

Thus x^* is *a* simultaneous solution.

Of course, this x^* may not lie between 0 and $m_1 m_2 - 1$. But if y^* is another solution to the system of congruences then $x^* \equiv y^* \bmod m_1$ and $x^* \equiv y^* \bmod m_2$. So both m_1 and m_2 divide $x^* - y^*$. Since $\gcd(m_1, m_2) = 1$ we must have $m_1 m_2$ divides $x^* - y^*$, and thus $y^* = x^* + t m_1 m_2$ for $t \in \mathbb{Z}$. It is possible to choose one, *and only one*, $t_0 \in \mathbb{Z}$ with $0 \leq x^* + t_0 m_1 m_2 \leq m_1 m_2 - 1$. So only one simultaneous solution lies between 0 and $m_1 m_2 - 1$.
■

Note that to apply the Chinese Remainder Theorem we have to ensure that the congruences are of the form $x \equiv a \bmod m$, i.e. where the coefficient of x is 1.

Example 10 *Using the Chinese Remainder Theorem solve*

$$x \equiv 16 \bmod 17 \quad \textit{and} \quad x \equiv 3 \bmod 13.$$

Solution Need to find b_1 and b_2, solutions of

$$13 b_1 \equiv 1 \bmod 17 \quad \text{and} \quad 17 b_2 \equiv 1 \bmod 13.$$

The first congruence can be written as $-4b_1 \equiv 1 \bmod 17$ for which we note that $-4 \times 4 = -16 \equiv 1 \bmod 17$ so $b_1 = 4$.

For the second congruence, written as $4b_2 \equiv 1 \bmod 13$, note that $4 \times (-3) = -12 \equiv 1 \bmod 13$. So we take $b_2 = -3 \equiv 10 \bmod 13$.

Finally evaluate x^* as

$$\begin{aligned} x^* &= m_2 b_1 a_1 + m_1 b_2 a_2 \\ &= 13 \times 4 \times 16 + 17 \times 10 \times 3 = 1342 \\ &\equiv 16 \bmod 221. \end{aligned}$$

■

The virtue of the Chinese Remainder Theorem is that it can be generalized to systems of any number of linear congruences. The condition under which the system of congruences $x \equiv a_i \bmod m_i$ will have a solution if their moduli m_i satisfy $\gcd(m_i, m_j) = 1$ for all $i \neq j$. We say that the modulus are *pairwise coprime.*

How is pairwise coprime used in the following proof? Note that if $a|c$ and $b|c$ then ab does not necessarily divide c. For example $6|12$ and $4|12$ but $24 \nmid 12$. Yet coprimeness gives

Lemma 11 *If* $\gcd(a, b) = 1$, $a|c$ *and* $b|c$ *then* $ab|c$.

Proof $a|c$ and $b|c$ imply $c = ak$ and $c = b\ell$ for some $k, \ell \in \mathbb{Z}$. Equate to get $ak = b\ell$. Since a divides the left hand side it divides the right hand side, i.e. $a|b\ell$. Yet $\gcd(a, b) = 1$ so, by an earlier result, $a|\ell$. Thus $ab|b\ell$, i.e. $ab|c$ as required. ■

To combine a number of coprimality conditions the following is useful.

Lemma 12 *If* $\gcd(a, m) = 1$ *and* $\gcd(b, m) = 1$ *then* $\gcd(ab, m) = 1$.

Proof Recall $\gcd(a, m) = 1$ if, and only if, $sa + tm = 1$ for some $s, t \in \mathbb{Z}$. Similarly $\gcd(b, m) = 1$ implies $kb + \ell m = 1$ for some $k, \ell \in \mathbb{Z}$. Multiply the first equality by kb to get

$$sakb + tmkb = kb = 1 - \ell m,$$

using the second equality. Rearrange as

$$(sk)\, ab + (tkb + \ell)\, m = 1,$$

i.e. some linear combination of ab and m equals 1. This is simply the definition that $\gcd(ab, m) = 1$. ■

These lemmas can be combined to show that if $a_i|c$ for $1 \leq i \leq N$ and $\gcd(a_i, a_j) = 1$ for all $i \neq j$ then $a_1 a_2 ... a_N|c$. *Left to student.*

Theorem 13 ***Chinese Remainder Theorem*** *(for n linear congruences)* *Let* $m_1, m_2, ..., m_n$ *be integers such that* $\gcd(m_i, m_j) = 1$ *for all* $i \neq j$, *and* $a_1, a_2, ..., a_n$ *integers. Then the simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \bmod m_1, \\ x &\equiv a_2 \bmod m_2, \\ &\vdots \\ x &\equiv a_n \bmod m_n \end{aligned}$$

have exactly one solution with $0 \leq x \leq m_1 m_2 ... m_n - 1$.

Proof not given in this appendix, but the idea is to find *a* solution of the form

$$x^* = \ell_1 a_1 + \ell_2 a_2 + \ell_3 a_3 + \cdots + \ell_n a_n.$$

To satisfy $x^* \equiv a_i \bmod m_i$ for each $1 \leq i \leq n$, it suffices that

$$\ell_i \equiv 1 \bmod m_i \quad \text{and} \quad \ell_i \equiv 0 \bmod m_j \text{ for all } j \neq i.$$

Let $M = m_1 m_2 ... m_n$, the product of the moduli and, for each $1 \leq i \leq n$, define

$$\kappa_i = \frac{M}{m_i} = \prod_{\substack{j=1 \\ j \neq i}}^{n} m_j,$$

the product of all moduli *except* for m_i. Then

$$\ell_i \equiv 0 \bmod m_j \ \forall j \neq i \ \Rightarrow \ m_j | \ell_i \ \forall j \neq i \ \Rightarrow \ \left. \prod_{\substack{j=1 \\ j \neq i}}^{n} m_j \right| \ell_i,$$

using the fact that the m_i are pairwise coprime. Thus $\kappa_i | \ell_i$ for all $1 \leq i \leq n$. Then we can write $\ell_i = \kappa_i b_i$ for some $b_i \in \mathbb{Z}$.

To satisfy the first condition $\ell_i \equiv 1 \bmod m_i$ we choose b_i to satisfy $\kappa_i b_i \equiv 1 \bmod m_i$, i.e. to be the inverse of k_i modulo m_i. (The fact that all the moduli are co-prime means that $\gcd(k_i, m_i) = 1$ which ensures the inverses b_i exist). Let

$$x^* = \kappa_1 b_1 a_1 + \kappa_2 b_2 a_2 + \kappa_3 b_3 a_3 + \cdots + \kappa_n b_n a_n.$$

Finally if y^* is the general solution then $y^* = x^* + Mt$ for $t \in \mathbb{Z}$. ■