10. Linear congruences

In general we are going to be interested in the problem of solving polynomial equations modulo an integer m. Following Gauss, we can work in the ring $\mathbb{Z}_m$ and find all solutions to polynomial equations with coefficients in this ring. One huge advantage of this approach is that we can count the number of solutions in the ring $\mathbb{Z}_m$, simply because $\mathbb{Z}_m$ is finite.

As a warm up we consider linear equations. It is easy to do the case of one equation.

Theorem 10.1. *Let $m > 1$ be a natural number and let a and b be integers. Let $d = (a, m)$.*

The equation

$$ax \equiv b \mod m$$

has a solution if and only if $d|b$.

In this case, there is one solution, call it x_0, to the equation

$$(a/d)x = (b/d) \equiv \quad \mod m/d,$$

and there are d solutions

$$x_0 \qquad x_0 + \frac{m}{d} \qquad x_0 + 2\frac{m}{d} \qquad \dots \qquad \text{and} \qquad x_0 + (d-1)\frac{m}{d},$$

to the equation

$$ax \equiv b \mod m.$$

Proof. Solving the equation

$$ax \equiv b \mod m$$

is equivalent to solving the equation

$$ax + (-m)y = b$$

in integers x and y.

Indeed, if x_0 is a solution to

$$ax \equiv b \mod m$$

then $ax_0 \equiv b \mod m$. It follows that $ax_0 - b$ is divisible by m, that is, there is an integer y_0 such that $ax_0 - b = my_0$. Rewriting, we see that

$$ax_0 + (-m)y_0 = b,$$

so that (x_0, y_0) is a solution to $ax + (-m)y = b$.

Vice-versa, if (x_0, y_0) is a solution of

$$ax + (-m)y = b$$

then $ax_0 \equiv b \mod m$ so that x_0 is a solution of

$$ax \equiv b \mod m.$$

Now we already know that the linear Diophantine equation

$$ax + (-m)y = b$$

has a solution if and only if $d|b$. In this case, pick a solution (x_0, y_0) to the equation

$$(a/d)x + (-m/d)y = b/d.$$

Then every solution to the equation

$$(a/d)x + (-m/d)y = b/d.$$

is given by

$$x = x_0 + \frac{mt}{d} \qquad \text{and} \qquad y = y_0 + \frac{ta}{d}.$$

These are all equivalent modulo m/d, so the equation

$$(a/d)x \equiv (b/d) \mod m/d,$$

has a unique solution and we get d solutions

$$x_0 \qquad x_0 + \frac{m}{d} \qquad x_0 + 2\frac{m}{d} \qquad \dots \qquad \text{and} \qquad x_0 + (d-1)\frac{m}{d},$$

to the equation

$$ax \equiv b \mod m. \qquad \square$$

Question 10.2. *Find all solutions of the equation*

$$9x \equiv 15 \mod 51.$$

First note that $(9, 51) = 3$ and $3|15$, so this equation does have a solution and it is equivalent to the equation

$$3x \equiv 5 \mod 17.$$

This is also equivalent to the equation

$$3x + 17y = 5.$$

We can solve this as usual by applying the Euclidean algorithm

$$\begin{aligned} 17 &= 5 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Therefore

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (17 - 5 \cdot 3) \\ &= 3 \cdot 6 + 17 \cdot -1. \end{aligned}$$

Multiplying by 5 we get

$$3 \cdot 30 + 17 \cdot -5 = 5.$$

Reducing modulo 17 we get

$$3 \cdot 13 \equiv 5 \mod 17.$$

Thus $x = 13$ is one possible solution. The others are given by jumps of 17,

$$13, \qquad 30 \qquad \text{and} \qquad 47.$$

Now let us turn to the problem of solving simultaneous linear equations. The interesting feature of this problem is that it is possible to solve two or more equations with respect to different moduli. Now one linear equation of the form

$$ax \equiv b \mod m$$

is equivalent to a collection of equations of the form

$$x \equiv c \mod m$$

where c might take a collection of values. It follows that working on each equation one at a time, when the modulus is fixed, we can reduce our equations to a collection of simultaneous equations

$$\begin{aligned} x &\equiv c_1 \mod m_1 \\ x &\equiv c_2 \mod m_2 \\ \vdots &\ \ \ddots \qquad \vdots \\ x &\equiv c_k \mod m_k. \end{aligned}$$

Note that these equations might be incompatible. For example, we cannot solve

$$\begin{aligned} x &\equiv 0 \mod 2 \\ x &\equiv 1 \mod 2. \end{aligned}$$

In this case any solution is supposed to be both even and odd, which is impossible.

The problem is when two moduli are not coprime. Amazingly, if the moduli are coprime there is a simple way to solve a system of equations.

Theorem 10.3 (Chinese remainder theorem)**.** *If the moduli $m_1, m_2, \dots, m_r$ are pairwise coprime, that is $(m_i, m_j) = 1$ for $i \neq j$, then the system* *of equations*

$$\begin{aligned} x &\equiv c_1 \mod m_1 \\ x &\equiv c_2 \mod m_2 \\ \vdots & \ddots \qquad \vdots \\ x &\equiv c_k \mod m_r, \end{aligned}$$

has one solution, given by a residue class modulo the product, $m = m_1 m_2 \dots m_r$.

Proof. This system is completely described, if we fix the moduli and their order, by a vector $(c_1, c_2, \dots, c_r)$. Even better, we can view replace c_i be a residue class $\bar{c}_i$ modulo m. Thus any equation is represented by a vector

$$(\bar{c}_1, \bar{c}_2, \dots, \bar{c}_r) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}.$$

Now if a is a solution to these equations and $b \equiv a \mod m$ then b is also a solution. Indeed, as m_i divides m, it follows that $b \equiv a \mod m_i$. Thus the solutions to this equation are naturally residue classes modulo m, $\bar{a} \in \mathbb{Z}_m$.

Suppose that a and $b \in \mathbb{Z}_m$ are two solutions to the same equation. Then $a \equiv b \mod m_i$, for all $1 \leq i \leq r$. Thus m_i divides $a - b$ for all $1 \leq i \leq r$. As $(m_i, m_j) = 1$ it follows that the product m divides $a - b$. Thus $a \equiv b \mod m$.

Thus each equation has at most one solution. On the other hand, every element $a \in \mathbb{Z}_m$ is the solution to the equation with $c_i \equiv a \mod m_i$. Note that there are m equations, since we can choose $c_1, c_2, \dots, c_r$ freely. As $\mathbb{Z}_m$ also has m equations, it follows that there is a one to one correspondence between equations and solutions. In other words, each equation has exactly one solution modulo m. □

In fact we have much more than a one to one correspondence between $\mathbb{Z}_m$ and the product of the sets $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$.

In general, given two rings R and S one can make another ring $R \oplus S$ as follows. The elements of $R \oplus S$ are just the elements of the Cartesian product. We have to decide how to add and how to multiply and then we have to check the axioms for a ring. To add and multiply, just add and multiply component by component:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \qquad \text{and} \qquad (r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2).$$

It is not hard to check that this rule of addition and multiplication is associative. One checks this component by component. $(0, 0)$ plays the role of zero, $(-r, -s)$ is the additive inverse of (r, s) and $(1, 1)$ plays the role of one.

Theorem 10.4 (Chinese remainder theorem, bis)**.** *If $m_1, m_2, \dots, m_r$ are pairwise coprime natural numbers then the two rings*

$$\mathbb{Z}_m \qquad \textit{and} \qquad \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \dots \oplus \mathbb{Z}_{m_r}.$$

are isomorphic.

Proof. We have already written down a bijection between the two underlying sets. It suffices to check that this bijection is a homomorphism, so that it respects addition, multiplication and sends one to one. But all of these statements are clear, because the addition and multiplication on both sides is the natural one inherited from the integers $\mathbb{Z}$. □

Note that this the Chinese remainder theorem is quite useful in practice. If you want do arithmetic modulo m, it is enough to do arithmetic modulo m_i, for every $1 \leq i \leq r$. Consider the problem of trying to solve an equation with vector

$$(c_1, c_2, \dots, c_r).$$

If we let e_i be the vector with an 1 in the ith entry and zero everywhere else, then we have

$$(c_1, c_2, \dots, c_r) = c_1 e_1 + c e_2 + \dots + c_r e_r.$$

If we can solve the equation with vector e_i then we can solve the general equation by taking the appropriate linear combination.

Suppose that y_i is a solution of the equations for the vector e_i. Then the solution to the equations for the vector $(c_1, c_2, \dots, c_r)$ is

$$c_1 y_1 + c_2 y_2 + \dots + c_r y_r.$$

Consider trying to find y_i. We want

$$y_i \equiv 0 \mod m_j.$$

Thus y_i is a multiple of m_j, for all $j \neq i$, so that y_i is a multiple of $m/m + i$. Thus

$$y_i = z_i \frac{m}{m_i}.$$

We want to choose z_i so that

$$\frac{m}{m_i} z_i \equiv 1 \mod m_i.$$

Putting all of this together, once we have found $z_1, z_2, \dots, z_r$ then

$$x = c_1 \frac{m}{m_1} z_1 + c_2 \frac{m}{m_2} z_2 + \dots + c_r \frac{m}{m_r} z_r$$

has the property that

$$x \equiv c_i \mod m_i,$$

for all $1 \leq i \leq r$.

Question 10.5. *Solve the three equations*

$$\begin{aligned} x &= 3 \mod 5\\ x &= 7 \mod 11\\ x &= 4 \mod 13. \end{aligned}$$

We use the method above. We first have to solve

$$\begin{aligned} 11 \cdot 13 z_1 &= 1 \mod 5\\ 5 \cdot 13 z_2 &= 1 \mod 11\\ 5 \cdot 11 z_3 &= 1 \mod 13. \end{aligned}$$

These reduce to

$$\begin{aligned} 3 z_1 &= 1 \mod 5\\ 10 z_2 &= 1 \mod 11\\ 3 z_3 &= 1 \mod 13. \end{aligned}$$

These have solutions

$$\begin{aligned} z_1 &= 2 \mod 5\\ z_2 &= 10 \mod 11\\ z_3 &= 9 \mod 13. \end{aligned}$$

The solution to the equation above is

$$\begin{aligned} x &= 11 \cdot 13 \cdot 2 \cdot 3 + 5 \cdot 13 \cdot 10 \cdot 7 + 5 \cdot 11 \cdot 9 \cdot 4\\ &\equiv 11 \cdot 13 + 5 \cdot 13 \cdot 6 - 5 \cdot 11 \cdot 3 \mod 5 \cdot 11 \cdot 13\\ &\equiv 41 \cdot 13 - 5 \cdot 11 \cdot 3 \mod 5 \cdot 11 \cdot 13\\ &= -41 \cdot 2 + 41 \cdot 5 \cdot 3 - 5 \cdot 11 \cdot 3\\ &= -41 \cdot 2 + 30 \cdot 5 \cdot 3\\ &= 368. \end{aligned}$$

Finally, we deal with the case that the moduli are not necessarily coprime.

Theorem 10.6. *The system of equations*

$$\begin{aligned} x &\equiv c_1 \mod m_1\\ x &\equiv c_2 \mod m_2\\ \vdots & \ddots \qquad \vdots\\ x &\equiv c_k \mod m_r, \end{aligned}$$

has a solution if and only if $(m_i, m_j) | c_i - c_j$ *for all* i *and* j. *In this case the general solution is a residue class modulo* $[m_1, m_2, \dots, m_r]$.

In particular a finite set of arithmetic progressions intersects if and only if any pair of them intersect.

Proof. Suppose that a is a solution. As $a \equiv c_i \mod m_i$ and $a \equiv c_j \mod m_j$ there are integers k and l such that $a = c_i + m_i k$ and $a = c_j + m_j l$. It follows that $c_i + m_i k = c_j + m_j l$, so that $c_i - c_j = m_i k + m_j l$. It follows that $(m_i, m_j)|(c_i - c_j)$.

Now suppose that $(m_i, m_j)|(c_i - c_j)$ for all i and j. Let p be a prime. Suppose that $m_i = p^{e_i} m'_i$, where m_i is coprime to p. By the Chinese remainder theorem, it suffices to solve each of these equations modulo $p_i^{e_i}$. Thus we may assume that $m'_i = 1$ so that $m_i = p^{e_i}$ are all powers of the same prime p.

Rearranging we may assume that $e_1 \geq e_2 \geq e_3 \dots$. In this case, $(m_1, m_j) = m_j$. If $a = c_1$ then

$$\begin{aligned} a &\equiv c_1 \mod m_j \\ &\equiv c_j \mod m_j. \end{aligned}$$

Thus $a = c_1$ is a solution to these equations. □