2.3 Diophantine Equations

Finding all solutions

Question If a solution exists then one can be found by Euclid's Algorithm. But could there be more than one?

Answer Yes. A method to find **all** solutions is best illustrated by examples.

Example 2.3.1 ***Not given*** *Find* ***all*** *integer solutions to* $93x + 56y = 2$.

Solution We have shown that $\gcd(93, 56) = 1$ and since $1|2$ the equation *has* integer solutions.

We have already found one such solution $(x_0, y_0) = (-6, 10)$. If (x, y) is another solution then we have both

$$\begin{aligned} 93x_0 + 56y_0 &= 2 \\ 93x + 56y &= 2. \end{aligned}$$

On subtracting,

$$93(x_0 - x) = 56(y - y_0). \tag{1}$$

Then 93 divides the left hand side so 93 divides the right hand side, i.e.

$$93|56(y - y_0).$$

Recall the result that if $a|bc$ but $\gcd(a, b) = 1$ then $a|c$. Here $93|56(y - y_0)$ but $\gcd(93, 56) = 1$ and so $93|(y - y_0)$. Thus $y - y_0 = 93t$, that is $y = y_0 + 93t$ for some $t \in \mathbb{Z}$. Substitute back into (1) to see

$$93(x_0 - x) = 56 \times 93t$$

or $x = x_0 - 56t$. Hence **all** the solutions are given by

$$(x_0 - 56t, y_0 + 93t) = (-6 - 56t, 10 + 93t)$$

for all $t \in \mathbb{Z}$. ■

To get a solution with a positive x choose $t = -1$ to get $(50, -83)$. CHECK this is a solution!

Example 2.3.2 *Find **all** integer solutions to* $166361x + 4043y = 26$.

Solution We have already found one solution $(x_0, y_0) = (284, -11686)$.

If (x, y) is another solution then we have both

$$\begin{aligned} 166361x_0 + 4043y_0 &= 26, \\ 166361x + 4043y &= 26. \end{aligned}$$

Subtracting, we get $166361\,(x_0 - x) + 4043\,(y_0 - y) = 0$ or

$$166361\,(x_0 - x) = 4043\,(y - y_0)\,. \tag{2}$$

Divide through by the 13 (the gcd of 166361 and 4043) to get

$$12797\,(x_0 - x) = 311\,(y - y_0)\,. \tag{3}$$

Now 12797 divides the LHS so it divides the RHS, i.e.

$$12797|311\,(y - y_0)\,. \tag{4}$$

Recall the result that if $\gcd(a, b) = d$ then $\gcd(a/d, b/d) = 1$. Here this means that $\gcd(12797, 311) = 1$.

Further, recall again the result that if $a|bc$ but $\gcd(a, b) = 1$ then $a|c$. Here this means that $12797|\,(y - y_0)$, i.e. $y - y_0 = 12797t$ for some $t \in \mathbb{Z}$. Substitute back in (5) to get

$$12797\,(x_0 - x) = 311 \times 12797t$$

i.e. $x_0 - x = 311t$. Thus **all** the solutions are given by

$$\begin{aligned} (x, y) &= (x_0 - 311t, y_0 + 12797t) \\ &= (284 - 311t, -11686 + 12797t) \end{aligned}$$

with $t \in \mathbb{Z}$. ■

When $t = 1$ we get $(-27, 1111)$, which you **should** check is a solution. This shows that Euclid's Algorithm, which gave $(284, -11686)$, doesn't necessarily find the "smallest" solution to a linear Diophantine equation.

Be careful. Equation (2) above stated that $166361\,(x_0 - x) = 4043\,(y - y_0)$. You could now say that

$$166361 | 4043\,(y - y_0)\,,$$

but you would be **wrong** to go on and deduce that $166361 |\,(y - y_0)$. This is because $\gcd(166361, 4043) = 13 \neq 1$ and so you cannot apply Corollary **??**. You **must** remember to divide through by the gcd, 13, to get (3).

You should be able to formalize the method of solution of the last example and prove

Theorem 2.3.3 *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 See appendix.

3 Congruences

Part V of PJE

3.1 Definitions and properties

Definition 3.1.1 *(p.232) Let $m > 0$ be an integer.*

Two integers a and b are ***congruent modulo*** *m if m divides $a - b$. We write $a \equiv b \bmod m$.*

If m does not divides $a-b$ we say that a is ***not*** *congruent or* ***incongruent*** *to b, and write $a \not\equiv b \bmod m$.*

The integer m is called the ***modulus*** *(and is non-zero).*

If $a \equiv b \bmod m$, then b is a ***residue*** *of a modulo m. When $0 \le b \le m-1$, then b is called the* ***least non-negative residue of*** *a modulo m.*

Example 3.1.2 $5 \equiv 25 \bmod 10$ *since* $10 | (5 - 25)$.

Note The definition of congruence reinterpreted as

$$\begin{aligned} a \equiv b \bmod m &\Leftrightarrow m | (a-b) \\ &\Leftrightarrow a - b = mt \text{ for some } t \in \mathbb{Z}, \\ &\Leftrightarrow a = b + mt \text{ for some } t \in \mathbb{Z}, \end{aligned}$$

Theorem 3.1.3 *Congruences modulo m satisfy*

i) ***Reflexive****, For all integers a, $a \equiv a \bmod m$, i.e.*

$$\forall a \in \mathbb{Z}, a \equiv a \bmod m.$$

ii) ***Symmetric,*** *For all integers a, b, if $a \equiv b \bmod m$ then $b \equiv a \bmod m$, i.e.*

$$\forall a, b \in \mathbb{Z}, a \equiv b \bmod m \Rightarrow b \equiv a \bmod m.$$

iii) ***Transitive****, For all integers a, b, c, if $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $a \equiv c \bmod m$, i.e.*

$$\forall a, b, c \in \mathbb{Z}, a \equiv b \bmod m \textit{ and } b \equiv c \bmod m \Rightarrow a \equiv c \bmod m.$$

Proof p.233

Theorem 3.1.4 ***Modular arithmetic***.

Suppose that a_1, a_2, b_1 *and* b_2 *are integers such that* $a_1 \equiv a_2 \bmod m$ *and* $b_1 \equiv b_2 \bmod m$. *Then*

i) $a_1 + b_1 \equiv a_2 + b_2 \bmod m$

ii) $a_1 - b_1 \equiv a_2 - b_2 \bmod m$

iii) $a_1 b_1 \equiv a_2 b_2 \bmod m$.

Proof p.233.

The next result is just a reinterpretation of the following facts about division,

$$m|ac \text{ and } a|m \;\Rightarrow \frac{m}{a}|c,$$

and

$$m|ac \text{ and } \gcd(a,m) = 1 \Rightarrow m|c.$$

Theorem 3.1.5 *(i) If* a *divides* m *then*

$$ab_1 \equiv ab_2 \bmod m \textit{ if, and only if, } b_1 \equiv b_2 \bmod \frac{m}{a}.$$

(ii) If $\gcd(a,m) = 1$ *then*

$$ab_1 \equiv ab_2 \bmod m \textit{ if, and only if, } b_1 \equiv b_2 \bmod m.$$

Proof p.241 but I'll give the proof of Part **ii** here.

($\Leftarrow$) Assume $b_1 \equiv b_2 \bmod m$. This means that $b_1 - b_2 = mt$ for some $t \in \mathbb{Z}$. Multiply through by a to get $a(b_1 - b_2) = amt$, i.e. $ab_1 - ab_2 = m(at)$. Thus $ab_1 \equiv ab_2 \bmod m$.

($\Rightarrow$) Assume $ab_1 \equiv ab_2 \bmod m$. This means that $m|(ab_1 - ab_2)$, i.e. $m|a(b_1 - b_2)$. Recall the Corollary that if $a|bc$ and $\gcd(a,b) = 1$ then $a|c$. In the present situation we are assuming $\gcd(m,a) = 1$ which, with $m|a(b_1 - b_2)$ implies $m|(b_1 - b_2)$. This is no more than the definition of $b_1 \equiv b_2 \bmod m$. ■

3.2 Solving linear congruences

Solving equations of the form $ax \equiv b \pmod{m}$, where x is an unknown integer.

Example 3.2.1 *Find **an** integer x for which $56x \equiv 1 \bmod 93$.*

Solution We have already solved this in the previous Chapter. Starting with $a = 93$ and $b = 56$ we used Euclid's Algorithm to show that

$$93 \times (-3) + 56 \times 5 = 1$$

Modulo 93 this gives $56 \times 5 \equiv 1 \bmod 93$. Hence $x = 5$ is a solution. ■

Advice for exam Don't forget to CHECK your answer.

We can attempt to solve all such linear congruences by using Euclid's Algorithm. Further, if a congruence has **an** integer solution we can then find **all** its integer solutions.

Example 3.2.2 *(**Not given in lectures**) Find **all** integers x for which*

$$5x \equiv 12 \bmod 19.$$

Solution If x **is** an integer solution, then $5x = 12 + 19t$ for some $t \in \mathbb{Z}$, which rearranges as $5x - 19t = 12$.

Such pairs of solutions $(x, t) \in \mathbb{Z}^2$ can be found by Euclid's Algorithm. Since $\gcd(5, 19) = 1$ which divides 12, this method **will** give solutions.

Start with

$$\begin{aligned} 19 &= 3 \times 5 + 4 \\ 5 &= 1 \times 4 + 1, \end{aligned}$$

Work back up to get

$$\begin{aligned} 1 &= 5 - 1 \times 4 \\ &= 5 - 1 \times (19 - 3 \times 5) \\ \text{Thus} \qquad 1 &= 4 \times 5 - 1 \times 19. \end{aligned}$$

Multiply by 12 to get

$$5 \times 48 - 19 \times 12 = 12, \tag{5}$$

so **a** solution to $5x - 19t = 12$ is $(x_0, t_0) = (48, 12)$.

Looking at (5) modulo 19 all multiples of 19 disappear and we get $5 \times 48 \equiv 12 \bmod 19$. Hence a *particular* answer to $5x \equiv 12 \bmod 19$ is $x = 48$.

For the *general* solution **a different** method is to start with the trivial

$$5 \times 19 - 19 \times 5 = 0.$$

Then multiplying by ℓ, so

$$5 \times 19\ell - 19 \times 5\ell = 0$$

for all $\ell \in \mathbb{Z}$. Add this to (5) to get

$$5(48 + 19\ell) - 19\,(12 + 5\ell) = 12$$

for any $\ell \in \mathbb{Z}$. Thus all solutions to $5x \equiv 12 \bmod 19$ are given by $x = 48 + 19\ell$, $\ell \in \mathbb{Z}$, which is the same as $x \equiv 48 \bmod 19$, itself the same as $x \equiv 10 \bmod 19$.■

Example 3.2.3 *Solve* $4043x \equiv 25 \bmod 166361$.

Solution We have seen this in the previous Chapter. Assume for contradiction that the congruence has solutions in which case the Diophantine equation

$$166361 \times (-t) + 4043x = 25$$

has solutions in integers x and t. Yet since $\gcd(166361, 4043) = 13$ and $13 \nmid 25$, this Diophantine equation has **no** integer solutions. Contradiction. Hence the congruence has **no** integer solutions. ■

Example 3.2.4 *Find all solutions in integers x to* $15x \equiv 12 \bmod 57$.

Solution

First, check there are solutions. To solve $15x \equiv 12 \bmod 57$ we will solve $15x = 12 + 57t$, i.e.

$$15x - 57t = 12$$

for $x, t \in \mathbb{Z}$. Apply Euclid's Algorithm,

$$\begin{aligned} 57 &= 3 \times 15 + 12 \\ 15 &= 1 \times 12 + 3 \\ 12 &= 4 \times 3 + 0 \end{aligned}$$

to see that $\gcd(57, 15) = 3$. Since $3|12$ the equation $15x - 57t = 12$ and thus the congruence **will** have solutions.

Second, find a particular solution. Working back up Euclid's Algorithm we see that

$$\begin{aligned} 3 &= 15 - 1 \times 12 \\ &= 15 - (57 - 3 \times 15) \\ &= 15 \times 4 - 57. \end{aligned}$$

Multiply by 4 to get

$$15 \times 16 - 57 \times 4 = 12. \tag{6}$$

So $(x_0, t_0) = (16, 4)$ is a particular solution of $15x - 57t = 12$. Looking at (6) modulo 57 we see that $15 \times 16 = 12 \bmod 57$ so **a** solution of $15x \equiv 12 \bmod 57$ is $x_0 = 16$.

Thirdly, find the general solution If (x_0, t_0) is a *particular* solution and $(x, t) \in \mathbb{Z}^2$ is a *general* solution, then

$$\begin{aligned} 15x_0 - 57t_0 &= 12 \\ 15x - 57t &= 12. \end{aligned}$$

Subtract to get

$$15\,(x_0 - x) - 57\,(t_0 - t) = 0, \tag{7}$$

or $15\,(x_0 - x) = 57\,(t_0 - t)$.

Since $15|LHS$ we deduce that $15|57\,(t_0 - t)$. But we **cannot** go on to deduce that $15|\,(t_0 - t)$ because $\gcd(15, 57) \neq 1$.

Instead divide all terms in (7) by $\gcd(15, 57) = 3$ to get

$$5\,(x_0 - x) = 19\,(t_0 - t)\,. \tag{8}$$

This time

$$5|LHS \Rightarrow 5|19\,(t_0 - t) \Rightarrow 5|\,(t_0 - t)\,,$$

allowable since $\gcd(5, 19) = 1$. Thus $t_0 - t = 5\ell$ for $\ell \in \mathbb{Z}$.

Substitute back into (8) to get $5\,(x_0 - x) = 19 \times 5\ell$, i.e. $x_0 - x = 19\ell$. Hence the general solution to (6) is

$$(x, t) = (x_0 - 19\ell, t_0 - 5\ell) = (16 - 19\ell, 4 - 5\ell)$$

for $\ell \in \mathbb{Z}$. So **all** the solutions to $15x \equiv 12 \bmod 57$ are given by $x = 16 - 19\ell, \ell \in \mathbb{Z}$.

Finally express your answer as a congruence with the original modulus. The solution $x = 16 - 19\ell, \ell \in \mathbb{Z}$, could be written as $x \equiv 16 \bmod 19$. But it is more usual to express the answer in the *same* modulus, 57, as the question. Varying $\ell(= 0, -1, -2, -3, ...)$ we find solutions $..., 16, 35, 54, 73, ...$. But $73 \equiv 16 \bmod 57$ and so after $16, 35$ and 54 we get no new solutions, $\bmod 57$. Whereas $16, 35$ and 54 are not congruent (i.e. they are *incongruent*) $\bmod 57$. So we give the solutions to $15x \equiv 12 \bmod 57$ as

$$x \equiv 16, 35, 54 \bmod 57.$$

■

Advice for exam

1) Follow the structure above,

First, check there are solutions.

Second, find a particular solution.

Thirdly, find the general solution

Finally express your answer as a congruence with the original modulus.

2) When finding the **general** solution to $ax \equiv c \bmod m$ you will come across an equality of the form

$$a(x - x_0) = m(t_0 - t).$$

At this point **always** divide through by $\gcd(a, m)$. For it $a = a' \times \gcd(a, m)$ and $m = m' \times \gcd(a, m)$ then $\gcd(a', m') = 1$ which, with

$$a'(x - x_0) = m'(t_0 - t),$$

implies $a' | (t_0 - t)$ and the solution continues....

3) When expressing your answer as a congruence give your answer

a) as a *positive* number, so the solution to $3x \equiv 1 \bmod 11$ should **not** be given as $x \equiv -7 \bmod 11$ and

b) Give your answer as an integer *smaller than the modulus*, so the solution to $3x \equiv 1 \bmod 13$ should **not** be given as $x \equiv 22 \bmod 13$.

The reason for these last two comments is that you want to minimise correct answers in the exam being marked incorrect simply because they look different to the model solutions.

Note that the number of incongruent solutions here equals 3, which is the same as $\gcd(57, 19)$. This is not a coincidence, as can be seen in the following.

Theorem 3.2.5 *The congruence $ax \equiv c \pmod{m}$ 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 and are not given here.

3.3 Multiplicative inverses.

Definition 3.3.1 *If a' is a solution of the congruence $ax \equiv 1 \pmod{m}$ then a' is called a **(multiplicative) inverse** of a modulo m and we say that a is **invertible** modulo m.*

Note The congruence $ax \equiv 1 \pmod{m}$ has solutions if, and only if, $\gcd(a, m) | 1$, i.e. $\gcd(a, m) = 1$. Thus a has an inverse modulo m iff a and m are coprime. Since the inverse is a solution of a congruence they can be found using Euclid's Algorithm.

Example 3.3.2 *Find the inverse of* $56 \bmod 93$.

Solution Above we solved $56x \equiv 1 \bmod 93$, finding $x = 5$. Hence 5 is an inverse of 56 modulo 93.

If we can find a multiplicative inverse a' to $a \bmod m$ we can then solve $ax \equiv b \bmod m$ by multiplying both sides by a' to get

$$x \equiv (a'a)\, x \equiv a'\,(ax) \equiv a'b \bmod m.$$

Example 3.3.3 *Solve* $56x \equiv 23 \bmod 93$.

Solution Multiply both sides of the equation by the inverse of $56 \bmod 93$, i.e. 5, to get $280x \equiv 115 \bmod 93$, i.e.

$$x \equiv 115 \equiv 22 \bmod 93.$$

■

The advantage of finding the inverse of 56 modulo 93 is that once found we can solve each of $56x \equiv b \bmod 93$, for **any** $b \in \mathbb{Z}$.

And of course, if 5 is the inverse of $56 \bmod 93$ then 56 is the inverse of $5 \bmod 93$. This fact can be used in:

Example 3.3.4 *Solve* $5x \equiv 23 \bmod 93$.

Solution Multiply both sides of the equation by the inverse of $5 \bmod 93$, i.e. 56, to get $280x \equiv 1288 \bmod 93$, that is,.

$$x \equiv 1288 \equiv 79 \bmod 93.$$

■

3.4 Solving Simultaneous Pairs of Linear Congruences

Consider the two linear congruences

$$x \equiv 2 \bmod 5 \quad \text{and} \quad x \equiv 1 \bmod 3.$$

Integers satisfying the first congruence include

$$... - 8, -5, 2, 7, 12, 17, 22, 27, 32, .. .$$

Those satisfying the second include

$$.. - 8, -5, -3, 1, 4, 7, 10, 13, 16, 19, 22, .. .$$

So $-8, 7$ and 22 satisfy both congruences simultaneously. What other integers satisfy both simultaneously?

Example 3.4.1 ***Not given*** *Solve the system*

$$x \equiv 2 \bmod 5 \quad \textit{and} \quad x \equiv 1 \bmod 3.$$

Solution Write $x \equiv 2 \bmod 5$ as $x = 2 + 5k$ for some $k \in \mathbb{Z}$ and write $x \equiv 1 \bmod 3$ as $x = 1 + 3\ell$ for some $\ell \in \mathbb{Z}$. Equate to get $2 + 5k = 1 + 3\ell$, or $3\ell - 5k = 1$.

We could solve this using Euclid's Algorithm, though here it is as easy to stare and see that $\ell = 2, k = 1$, is *a* solution, while

$$(k, \ell) = (1 + 3t, 2 + 5t), t \in \mathbb{Z}$$

is the general solution. Thus the x that satisfy both congruences are

$$x = 2 + 5k = 2 + 5(1 + 3t) = 7 + 15t, \text{ for all } t \in \mathbb{Z},$$

i.e. $x \equiv 7 \bmod 15$. ■

Example 3.4.2 *Solve*

$$7x \equiv 16 \bmod 17 \quad \textit{and} \quad 2x \equiv 7 \bmod 13.$$

Solution *First, solve each congruence separately.* For the first congruence Euclid's Algorithm gives

$$\begin{aligned} 17 &= 2 \times 7 + 3 \\ 7 &= 2 \times 3 + 1. \end{aligned}$$

Work back up so

$$\begin{aligned} 1 &= 7 - 2 \times 3 \\ &= 7 - 2\,(17 - 2 \times 7) \\ &= 5 \times 7 - 2 \times 17. \end{aligned}$$

Multiply through by 16

$$16 = 80 \times 7 - 32 \times 17.$$

The first congruence becomes $x \equiv 80 \bmod 17 \equiv 12 \bmod 17$.

For the second congruence use the trick of $2x \equiv 7 \equiv 20 \bmod 13$. Dividing through by 2 gives $x \equiv 10 \bmod 13$.

Secondly, solve the system

$$x \equiv 12 \bmod 17 \quad \text{and} \quad x \equiv 10 \bmod 13.$$

Rewrite as $x = 12+17s$ and $x = 10+13t$ and equate as $12+17s = 10+13t$, or $13t - 17s = 2$.

Euclid's Algorithm

$$\begin{aligned} 17 &= 13 + 4 \\ 13 &= 3 \times 4 + 1. \end{aligned}$$

Working back up

$$\begin{aligned} 1 &= 13 - 3 \times 4 \\ &= 13 - 3\,(17 - 13) \\ &= 4 \times 13 - 3 \times 17. \end{aligned}$$

Multiply by 2 to get

$$13\,(8) - 17\,(6) = 2.$$

Thus a particular solution is $(s_0, t_0) = (6, 8)$.

It is not hard to see that the general solution of $17s - 13t = 2$ is

$$(s, t) = (6 + 13k, 8 + 17k)\,,\ \ k \in \mathbb{Z}.$$

Substitute back into $x = 12 + 17s$ so

$$x = 12 + 17\,(6 + 13k) = 114 + 221k.$$

Finally write the answer as a congruence $x \equiv 114 \bmod 221$. ■

Remember to check your answer by substituting it back into the original system of congruences.

Be Careful *Only give if time*

Example 3.4.3 *Solve*

$$x \equiv 2 \bmod 6 \quad \textit{and} \quad x \equiv 1 \bmod 4.$$

Solution Integers satisfying the first congruence include

$$..., 2, 8, 14, 20, 26, ...$$

while

$$..., 1, 5, 9, 13, 17, 21, ...$$

satisfy the second. These lists have **nothing** in common, the first contains even integers the second odd integers. Thus there *appears to be* no simultaneous solutions to the two congruences.

By the method above $x \equiv 2 \bmod 6$ becomes $x = 2 + 6k$ while $x \equiv 1 \bmod 4$ becomes $x = 1 + 4\ell$. Equate to get $2 + 6k = 1 + 4\ell$, i.e.

$$4\ell + 6k = 1.$$

This has no solutions because the left hand side of this is even, the right hand side odd. ■

We exclude this second example by demanding that the moduli of the two congruences are *coprime*. If we do that it is possible to prove that the system always has a solution:

Theorem 3.4.4 ***Theorem Chinese Remainder Theorem***

Let m_1 and m_2 be coprime integers, and a_1, a_2 integers. Then the simultaneous congruences

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

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

Proof *Not given in this course.*

3.5 Solving Simultaneous Triplets of Linear Congruences

Example 3.5.1 *Solve the system*

$$\begin{aligned} 2x &\equiv 3 \bmod 5, \\ 3x &\equiv 4 \bmod 7, \\ 5x &\equiv 7 \bmod 11. \end{aligned}$$

Solution Do this in steps.
First solve each congruence individually. For congruences such as these with small coefficients I would solve by observation, i.e. try $x = 0, 1, 2, ...$ etc. until you find a solution. In this way you get the system

$$\begin{aligned} x &\equiv 4 \bmod 5, \\ x &\equiv 6 \bmod 7, \\ x &\equiv 8 \bmod 11. \end{aligned}$$

Second, take any pair and solve. For example choose the pair

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

which has the solution $x \equiv 34 \bmod 35$.
Third, introduce the unused congruence. In our example this gives the the pair

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

The solution of this is *left to students.* ■

Advice for exams You should never get such questions wrong, since you can substitute your answer back into the original congruences to see it works.

Four or more linear congruences Simply repeat the third step above until there are no more unused congruences.

3.6 Method of Successive Squaring

The Theorem on Modular Arithmetic stated that if $a_1 \equiv a_2 \bmod m$ and $b_1 \equiv b_2 \bmod m$ then $a_1 b_1 \equiv a_2 b_2 \bmod m$. A special case of this, when $a_1 = b_1$ and $a_2 = b_2$, states that if $a_1 \equiv a_2 \bmod m$ then $a_1^2 \equiv a_2^2 \bmod m$.

Application If given a modulus m and an integer a and you wish to calculate $a^2 \bmod m$ you might first calculate a^2 and then find the least non-negative residue $\bmod m$.

Alternative you could first find the least non-negative residue $r_1 \equiv a \bmod m$ and then square r_1 and find its least non-negative residue $\bmod m$.

The special case of the Theorem on Modular Arithmetic gives $r_1^2 \equiv a^2 \bmod m$ and so we get the same answer whichever method we use. The advantage of finding r_1 first is that $0 \leq r_1 < m$ and so we need only square a number no larger than m whereas the original a may have been far larger than m.

This idea can be repeated and the resulting method is best illustrated by an example.

Example 3.6.1 *Calculate the least non-negative residue of* $4^{100} \bmod 13$.

Solution The ***Method of Successive Squaring***.

$$
\begin{aligned}
4^2 &\equiv 3 \quad \bmod 13, \\
4^4 &\equiv 3^2 \equiv 9 \equiv -4 \quad \bmod 13, \\
4^8 &\equiv (-4)^2 \equiv 3 \quad \bmod 13, \\
4^{16} &\equiv 3^2 \equiv 9 \equiv -4 \quad \bmod 13, \\
4^{32} &\equiv (-4)^2 \equiv 3 \quad \bmod 13, \\
4^{64} &\equiv 3^2 \equiv 9 \equiv -4 \quad \bmod 13.
\end{aligned}
$$

Then

$$
\begin{aligned}
4^{100} &= 4^{64+32+4} \qquad (9)\\
&= 4^{64} \times 4^{32} \times 4^4 \\
&\equiv (-4) \times 3 \times -4 \\
&\equiv 9 \bmod 13.
\end{aligned}
$$

■

Note What becomes important in this method is how to *write the exponent as a sum of powers of 2.* This is the same as *writing the exponent in binary notation.* So, in this example

$$\begin{aligned} 100_{10} &= 1100100_2 \\ &= 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^2 \\ &= 1 \times 64 + 1 \times 32 + 1 \times 4 \end{aligned}$$

and $64, 32$ and 4 are the exponents seen in (9) above.

Example 3.6.2 *Find the last 2 digits of* 13^{99}.

Solution An integer with $r \geq 2$ digits, $a_r a_{r-1} \ldots a_2 a_1 a_0$ $(r \geq 2)$ in decimal notation, represents

$$\begin{aligned} & a_r 10^r + a_{r-1} 10^{r-1} + \ldots + a_2 10^2 + a_1 10 + a_0 \\ = & \left(a_r 10^{r-2} + a_{r-1} 10^{r-3} + \ldots + a_2\right) 100 + (a_1 10 + a_0) \\ \equiv & (a_1 10 + a_0) \bmod 100. \end{aligned}$$

So the two digits of $13^{99} \bmod 100$ will be the last two digits of 13^{99}.

		$\bmod 100$
13^2		$\equiv 69$
13^4	$\equiv 69^2$	$\equiv 61$
13^8	$\equiv 61^2$	$\equiv 21$
13^{16}	$\equiv 21^2$	$\equiv 41$
13^{32}	$\equiv 41^2$	$\equiv 81$
13^{64}	$\equiv 81^2$	$\equiv 61.$

Then, because $99 = 64 + 32 + 2 + 1$ when written as a sum of powers of 2, we find that

$$\begin{aligned} 13^{99} &= 13^{64} \times 13^{32} \times 13^2 \times 13 \\ &\equiv 61 \times 81 \times 69 \times 13 \bmod 100 \\ &\equiv 77 \bmod 100. \end{aligned}$$

So the last two digits of 13^{99} are 7 and 7. ■

Questions for students. What are the last *three* digits of 13^{99}. What are the last two digits of 13^{1010}?