Chapter 3

Congruences

Definition (Congruence)**.** Let $m \in \mathbb{N}$. We say that integers a and b **are congruent modulo** m if m divides $a - b$. We write $a \equiv b \mod m$.

The integer m is called the **modulus**.

If $a \equiv b \mod m$, then b is a **residue** of a modulo m.

Example.

- $5 \equiv 25 \mod 10$ since $10 \mid (5 - 25)$;
- $3 \equiv 113 \mod 10$;
- $3 \not\equiv -113 \mod 10$ since $10 \nmid (3 - (-113))$ as $10 \nmid 116$.

Remark (Can we manipulate congruences the way we manipulate equations?)**.** We often manipulate statements of the form "$a = b$", using properties of $=$ (is equal to) without particular comment. We would like to understand whether statements of the form "a is congruent to b mod m" can be manipulated in the same way. The following rules for equality, $=$, are considered obvious: $a = a$ is true for all a; if $a = b$ then $b = a$; if $a = b$ and $b = c$ then $a = c$. It turns out that congruence mod m obeys the same rules. In the next Proposition we formally prove this fact and also learn the special names these three rules are given in abstract algebra and formal logic.

Proposition 3.1 (Congruence is reflexive, symmetric and transitive)**.** Let $m \in \mathbb{N}$. Congruence modulo m is

i) **Reflexive:** $\forall a \in \mathbb{Z}$, $a \equiv a \mod m$.

Proof. $a - a = 0 \implies m \mid (a - a) \implies a \equiv a \mod m$.

ii) **Symmetric:** $\forall a, b \in \mathbb{Z}$, $(a \equiv b \mod m) \implies (b \equiv a \mod m)$.

Proof. $m \mid (a-b) \implies a - b = mk,\ k \in \mathbb{Z} \implies b - a = m(-k),\ -k \in \mathbb{Z} \implies m \mid (b-a)$.

iii) **Transitive:** $\forall a, b, c \in \mathbb{Z}$, $(a \equiv b \mod m) \wedge (b \equiv c \mod m) \implies (a \equiv c \mod m)$.

Proof. $m \mid (a-b)$ and $m \mid (b-c) \implies a - b = mk,\ b - c = m\ell,\ k, \ell \in \mathbb{Z} \implies a - c = m(k+\ell),\ k + \ell \in \mathbb{Z} \implies m \mid (a-c)$. □

Remark (Can we add and multiply congruences?)**.** It turns out that the analogy between equations and congruences goes further, namely, we can add congruences termwise and we can also multiply congruences termwise.

Proposition 3.2 (Modular arithmetic)**.** Let a_1, a_2, b_1 and b_2 be integers such that $a_1 \equiv a_2 \mod m$ and $b_1 \equiv b_2 \mod m$. Then

- $a_1 + b_1 \equiv a_2 + b_2 \mod m$;
- $a_1 b_1 \equiv a_2 b_2 \mod m$.

Proof. Let $a_1 - a_2 = mk$, $b_1 - b_2 = m\ell$ with $k, \ell \in \mathbb{Z}$. Then

- $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = m(k + \ell)$;
- $a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 = a_1(b_1 - b_2) + b_2(a_1 - a_2) = m(a_1 \ell + b_2 k)$

(note how we subtracted $a_1 b_2$ then added it back). In each case the result is divisible by m so the required congruences follow. □

Question. The *Modular Arithmetic* shows that we can add, subtract and multiply congruences mod m, just as we can do with equations. Can we *divide* both sides of a congruence by the same integer?

The general answer is **no** but in the following important special case the answer is positive:

Proposition 3.3 (Both sides of a congruence can be divided by an integer coprime to the modulus)**.** If $\gcd(a, m) = 1$ then $(ab_1 \equiv ab_2 \mod m) \implies (b_1 \equiv b_2 \mod m)$.

Proof. Assume $ab_1 \equiv ab_2 \mod m$, so by definition $m \mid (ab_1 - ab_2)$, so $m \mid a(b_1 - b_2)$. We are given that m is coprime to a so by the Coprime factor Lemma 2.4, $m \mid (b_1 - b_2)$. Hence by definition $b_1 \equiv b_2 \mod m$. □

Remark (The 'most convenient' residue)**.** The preceding results show that we may replace an integer with any of its residues modulo m when doing arithmetic modulo m. Recall that a residue of a modulo m is *any* integer b such that $a \equiv b \mod m$. It is easy to see that each integer has infinitely many residues modulo m: indeed, the residues of a are a, $a-m$, $a+m$, $a-2m$, $a+2m$ and so on. Is there a 'most convenient' residue?

In many ways, the *least non-negative* residue of a is the best choice. The next Proposition reveals what it is.

Proposition 3.4 (Residues and remainders)**.** Let a, b be integers and m be a positive integer.

(i) The **least non-negative residue** of an integer a modulo m **is the remainder** of a on division by m.

(ii) $a \equiv b \mod m$ if and only if a and b leave the **same remainder** when divided by m.

Proof. (i) By definition, a residue of a modulo m is an integer c such that $m \mid (a-c)$, that is, $a - c = mp$ for some $p \in \mathbb{Z}$, equivalently $c = a - mp$. Hence $R = \{a - mp : a - mp \geq 0, p \in \mathbb{Z}\}$ is the set of all non-negative residues of a. So the least non-negative residue of a mod m is the the least element, $r = \min R$, of this set. But it was shown in the proof of Division Theorem 2.1 that r is the remainder of a when divided by m.

(ii) Assume that a and b leave the same remainder r when divided by m. Then by part (i) $a \equiv r \mod m$ and $b \equiv r \mod m$ so $r \equiv b \mod m$ because congruence is symmetric, and finally $a \equiv b \mod m$ since congruence is transitive.

Now assume that $a \equiv b \mod m$, and let r, s be the remainders of a, b, respectively, when divided by m. We aim to show that $r = s$. By part (i), r is the **least** non-negative residue of a mod m. Also by pat (i), s is a residue of b mod m so $a \equiv b \equiv s \mod m$ so s is also a residue of a mod m. Moreover, s is a non-negative residue of a, since remainders are always non-negative. Therefore, $r \leq s$ (least non-negative residue of $a \leq$ some non-negative residue of a).

We now swap a and b and do the same. Namely, by part (i) s is the least non-negative residue of b mod m, but $b \equiv a \equiv r \mod m$ so r is some non-negative residue of b mod m. So $s \leq r$. The two inequalities imply that $r = s$ as required. □

Example (Arithmetic of remainders)**.** We give examples of modular arithmetic allowing us to find remainders in various situations.

(i) The remainder of n when divided by 7 is 3. What is the remainder of $n + 5$ when divided by 7? What is the remainder of $5n$ when divided by 7?

Solution. Since 3 is the remainder of n, 3 is also a residue of n mod 7, that is,

$$n \equiv 3 \mod 7.$$

By Modular Arithmetic, we can add 5 to both sides of this congruence (formally: take the sum of this congruence and the congruence $5 \equiv 5 \mod 7$ which is true by reflexivity) to obtain

$$n + 5 \equiv 8 \mod 7.$$

Note that 8 is **not** the remainder as 8 is not less than 7; still, 8 is a residue of $n + 5$ mod 7. By Proposition 3.4(ii), $n + 5$ and 8 have the same remainder when divided by 7. Since 8 leaves remainder 1, it follows that $n + 5$ *leaves remainder* 1 *when divided by* 7.

To find the remainder of $5n$, multiply both sides of the congruence $n \equiv 3 \mod 7$ by 5 (formally: multiply this congruence by the congruence $5 \equiv 5 \mod 7$), obtaining $5n \equiv 15 \mod 7$. Hence $5n$ and 15 leave the same remainder when divided by 7. We conclude that *the remainder of* $5n$ *on division by* 7 *is* 1.

(ii) The remainder of $2k$ when divided by 7 is 6, what is the remainder of k?

Solution. $2k \equiv 6 \mod 7$; since 2 is coprime to the modulus, 7, by Proposition 3.3 we can divide both sides of the congruence by 2, obtaining $k \equiv 3 \mod 7$. So the remainder of k when divided by 7 is equal to the remainder of 3, which is 3.

(iii) The remainder of $2k$ when divided by 16 is 6. The remainder of 3ℓ when divided by 16 is 1. What are the remainders of k, ℓ?

Solution. We cannot divide both sides of the congruence $2k \equiv 6 \mod 16$ by 2 without touching the modulus, because 2 is not coprime to 16. It is not obvious how to "divide by 3" both sides of $3\ell \equiv 1 \mod 16$. We will be able to solve these congruences after we introduce more techniques below.

Solving linear congruences

We will learn to solve equations of the form

$$ax \equiv c \mod m,$$

where x is an unknown integer. Here $m \in \mathbb{N}$ is the modulus, and $a \in \mathbb{Z}$.

General method: observe that $ax \equiv c \mod m$ by definition means that $m \mid (ax - c)$, that is, there exists $y \in \mathbb{Z}$ such that $ax - c = my$, equivalently $ax - my = c$. In other words, x is the first component of a solution (x, y) to the linear Diophantine equation

$$ax - my = c.$$

Solve the Diophantine equation to find x.

We illustrate this method by examples.

Example (Solving a linear congruence)**.** Find **all** integers x for which $5x \equiv 12 \mod 19$.

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

$$5x - 19k = 12.$$

A pair $(x, k) \in \mathbb{Z}^2$ satisfying this equation can be found by Euclid's Algorithm. Since $\gcd(5, 19) = 1$ which divides 12, this method **will** give a solution. Start with

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

and work back up to get

$$1 = 5 - 4 \times 1 = 5 - (19 - 5 \times 3) \times 1 = 5 \times 4 - 19 \times 1.$$

Multiply through by 12 to get

$$5 \times 48 - 19 \times 12 = 12,$$

so a **particular** solution to $5x - 19k = 12$ is $(x_0, k_0) = (48, 12)$.

To find the general solution, we continue to follow the method of solving linear Diophantine equations developed in the previous Chapter. Subtract $5 \times 48 - 19 \times 12 = 12$ from $5x - 19k = 12$ to obtain $5(x - 48) - 19(k - 12) = 0$, equivalently $5(x - 48) = 19(k - 12)$. Thus $19 \mid 5(x - 48)$, and as 19 is coprime to 5, we conclude that $19 \mid (x - 48)$ so $x - 48 = 19\ell$, $\ell \in \mathbb{Z}$.

We do not need to keep track of k because we only want to solve for x. Thus all solutions to $5x \equiv 12 \mod 19$ are given by

$$x = 48 + 19\ell, \quad \ell \in \mathbb{Z}.$$

We usually want to present the answer in the form of a congruence for x:

$$x \equiv 48 \mod 19.$$

Moreover, it is customary to choose the least non-negative residue for the answer: 48 leaves remainder 10 when divided by 19 so

$$x \equiv 10 \mod 19.$$

Question. Is it true that every linear congruence of the form $ax \equiv c \mod m$ has a solution expressed by a unique remainder mod m?

Answer. No. The following situations are also possible:

- The solution is expressed by more than one remainder mod m.
- There are no solutions.

We illustrate both situations by examples.

Example (A linear congruence with more than one solution in the given modulus)**.** Find all solutions in integers x to $15x \equiv 36 \mod 57$.

Solution. First, check there are solutions. The congruence $15x \equiv 36 \mod 57$ is equivalent to the Diophantine equation $15x - 36 = 57k$, i.e.

$$15x - 57k = 36$$

for $x, k \in \mathbb{Z}$. Apply Euclid's Algorithm to find $\gcd(15, 57)$:

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

hence $\gcd(15, 57) = 3$. Since $3 \mid 36$ the equation $15x - 57k = 36$ and thus the congruence **will** have solutions.

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

$$3 = 15 - 12 \times 1 = 15 - (57 - 15 \times 3) \times 1 = 15 \times 4 - 57 \times 1.$$

As $3 \times 12 = 36$ we must multiply through by 12 to get

$$15 \times 48 - 57 \times 12 = 36. \qquad (\dagger)$$

So $(x_0, k_0) = (48, 12)$ is a particular solution of $15x - 57k = 36$. Looking at (†) modulo 57 we see that $15 \times 48 \equiv 12 \mod 57$ so **a** solution of $15x \equiv 36 \mod 57$ is $x_0 = 48$.

Thirdly, find the general solution. From $15x - 57k = 36$ we subtract $15 \times 48 - 57 \times 12 = 36$ and rearrange to get

$$15(x - 48) = 57(k - 12).$$

Here, 57 is not coprime to 15 so we cannot deduce that 57 divides $x - 48$. Instead, we divide the equation through by 3 to obtain

$$5(x - 48) = 19(k - 12).$$

So $19 \mid 5(x - 48)$ and, since 19 is coprime to 5, we conclude that $19 \mid (x - 48)$ so that

$$x = 48 + 19\ell, \qquad \ell \in \mathbb{Z}.$$

Note that we do not need to keep track of k as we are only looking for x.

Finally express your answer as a congruence with the original modulus. The solution $x = 48 + 19\ell$, $\ell \in \mathbb{Z}$, could be written as $x \equiv 48 \mod 19$. But it is more usual to express the answer in the *same* modulus, 57, as the question. Varying $\ell (= \ldots, -2, -1, 0, 1, \ldots)$ we find solutions $\ldots, 10, 29, 48, 67, \ldots$. But $67 \equiv 10 \mod 57$ and so after 10, 29 and 48 we get no new solutions mod 57; whereas 10, 29 and 48 are *incongruent* mod 57. So we give the solutions to $15x \equiv 36 \mod 57$ as

$$x \equiv 10,\ 29, \text{ or } 48 \mod 57.$$

Remark (Advice for exam)**.** Students are advised to follow the procedure 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. This may be an explicit requirement in the exam, for example: *Given that* $15x \equiv 36 \mod 57$*, find all possible remainders of* x *on division by* 57*.*

Remark (Number of incongruent solutions to a linear congruence)**.** Note that that in the above example, the number of incongruent solutions of $15x \equiv 36$ mod 57 (or, the same, the number of distinct remainders left by solutions on dividing by 57) equals 3, which is the same as $\gcd(15, 57)$. This is not a coincidence, as can be seen in the following

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

This result will not be proved in the course but interested students can find the ideas for the proof in P. J. Eccles, *Introduction to Mathematical Reasoning*, around p.244.

Example (A linear congruence with no solutions)**.** Solve $598x \equiv 1 \mod 455$.

Solution. If x satisfies the congruence, then x, together with some integer k, satisfies the Diophantine equation

$$598x - 455k = 1.$$

Yet we found in an earlier Example that $\gcd(598, 455) = 13$, and since $13 \nmid 1$, this Diophantine equation has **no** integer solutions. Hence the congruence has **no** integer solutions.

Multiplicative inverses

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

Since the inverse of a modulo m is a solution of a congruence, it can be found using Euclid's Algorithm.

Example. Find an inverse of 56 modulo 93.

Solution. Starting with $a = 93$ and $b = 56$ we use Euclid's Algorithm to show that

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

Modulo 93 this gives $56 \times 5 \equiv 1 \mod 93$. Hence $x = 5$ is a solution. That is, 5 is an inverse of 56 mod 93.

Remark (Advice)**.** Don't forget to CHECK your answer by multiplying 56 by 5 and finding the remainder on division by 93.

Proposition 3.5 (Invertible residues)**.** a is invertible mod $m \iff \gcd(a, m) = 1$.

Proof. The congruence $ax \equiv 1 \mod m$ is soluble, if and only if the equation $ax - my = 1$ is. The criterion for solubility of $ax - my = 1$ is $\gcd(a, m) \mid 1$ which is equivalent to $\gcd(a, m) = 1$. □

If we found a multiplicative inverse a' to a modulo m we can then quickly solve many congruences of the form $ax \equiv c \mod m$ for various c by multiplying both sides by a':

$$x \equiv (a'a)x \equiv a'(ax) \equiv a'c \mod m.$$

Example. Solve $56x \equiv 23 \mod 93$.

Solution. We already found an inverse of $56 \mod 93$ which was 5. Multiply both sides of the congruence by 5 to get $280x \equiv 115 \mod 93$, where $280 = 56 \times 5 \equiv 1 \mod 93$. Hence the solution is

$$x \equiv 115 \mod 93$$

which is better written, using the least non-negative residue, as

$$x \equiv 22 \mod 93.$$

Pairs of congruences. The Chinese Remainder Theorem

We will consider pairs of linear congruences of the form

$$x \equiv c_1 \mod m_1 \quad \text{and} \quad x \equiv c_2 \mod m_2. \tag{*}$$

Here $m_1, m_2 \in \mathbb{N}$ are two moduli, c_1, c_2 are integers, and x is the unknown. Solutions to (*) are all integers x which satisfy **both** congruences.

Remark (Pairs of more general linear congruences)**.** One can consider pairs of more general linear congruences such as $a_1x \equiv b_1 \mod m_1$ and $a_2x \equiv b_2 \mod m_2$. However, in such a pair each congruence can be solved individually and, if both congruences have solutions, we are reduced to a simpler pair of congruences of the form (*). Hence we will not consider the more general case.

Example (A naive attempt to solve a pair of congruences)**.** Consider the two simultaneous linear congruences

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

Integers satisfying the first congruence include

$$\ldots -8, -3, 2, 7, 12, 17, 22, 27, 32, \ldots$$

Those satisfying the second include

$$\ldots -8, -5, -2, 1, 4, 7, 10, 13, 16, 19, 22, \ldots$$

We notice that -8, 7 and 22 satisfy both congruences simultaneously. But there may be other integers satisfying both congruences simultaneously... How do we find them?

Students should realise that there is no need to attempt to solve congruences in such a naive way. Follow the procedure below.

Example (The correct way to solve a pair of congruences)**.** Find all $x \in \mathbb{Z}$ such that

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

Solution. The congruence $x \equiv 2 \mod 5$ is equivalently written as the equation $x = 2 + 5k$, $k \in \mathbb{Z}$. The congruence $x \equiv 1 \mod 3$ is equivalently written as $x = 1 + 3\ell$, $\ell \in \mathbb{Z}$. (Note that k and ℓ are not equal so we must use two different letters.) Both expressions are equal to x, so we equate them to obtain

$$2 + 5k = 1 + 3\ell,$$

equivalently (after rearranging)

$$3\ell - 5k = 1.$$

This is a linear Diophantine equation in k and ℓ. We could solve it using Euclid's Algorithm, though here it is easy to see that $\ell = 2, k = 1$ is *a* solution. The general solution of the Diophantine equation is

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

Thus the x that satisfy both congruences are

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

equivalently written as

$$x \equiv 7 \mod 15.$$

Answer: $x \equiv 7 \mod 15$.

Example (A pair of congruences with no solutions)**.** Solve $(x \equiv 2 \mod 6) \wedge (x \equiv 1 \mod 4)$.

Solution. Informally, we observe that integers satisfying the first congruence include

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

while

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

satisfy the second. It looks as if 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.

Now let us apply the formal method above: $x \equiv 2 \mod 6$ becomes $x = 2 + 6k$ while $x \equiv 1 \mod 4$ becomes $x = 1 + 4\ell$ where $k, \ell \in \mathbb{Z}$. Equate to get $2 + 6k = 1 + 4\ell$, i.e.

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

This Diophantine equation has **no solutions** because the left hand side is even, the right hand side odd. (In other words, $\gcd(4,2) \nmid 1$.)

An exact criterion for two congruences to have simultaneous solutions may be complicated, but a very reasonable assumption turns out to **guarantee** that the solutions exist: assume that the two moduli, m_1 and m_2, are coprime. See the following famous result.

Theorem 3.6 (Chinese Remainder Theorem)**.** Let m_1 and m_2 be coprime natural numbers, and c_1, c_2 integers. Then the simultaneous congruences

$$x \equiv c_1 \mod m_1 \quad \text{and} \quad x \equiv c_2 \mod m_2$$

have solutions. There is exactly one solution x_0 with $0 \leq x_0 < m_1 m_2$, and the general solution is $x \equiv x_0 \mod m_1 m_2$.

Proof. *The proof of the Chinese Remainder Theorem is not given in lectures and is not examinable. Students are expected to master the method of solving two simultaneous congruences and hence be able to find* x_0.

We rewrite the simultaneous congruences as the equation

$$x = c_1 + m_1 k = c_2 + m_2 \ell, \qquad k, \ell \in \mathbb{Z}.$$

After rearranging, this is equivalent to the equation

$$m_1 k - m_2 \ell = c_2 - c_1$$

which **has** solutions $(k, \ell) \in \mathbb{Z}^2$ because $\gcd(m_1, m_2) = 1$ divides $c_2 - c_1$. So by Theorem 2.6 the general solution has the form $(k, \ell) = (k_0 + m_2 t,\ \ell_0 + m_1 t)$, $t \in \mathbb{Z}$, for some k_0 and ℓ_0. We obtain the general solution for x which is

$$x = c_1 + m_1 k = (c_1 + m_1 k_0) + m_1 m_2 t,\ t \in \mathbb{Z} \quad \Longleftrightarrow \quad x \equiv (c_1 + m_1 k_0) \mod m_1 m_2.$$

Hence the Theorem holds with x_0 being the least non-negative residue of $c_1 + m_1 k_0 \mod m_1 m_2$. By Proposition 3.4 this x_0 is the remainder on dividing by $m_1 m_2$, hence one has $0 \leq x_0 < m_1 m_2$. □

Example (illustrating simultaneous congruences)**.** There are between 200 and 300 students in a mathematics course. If the students are divided into groups of 11, there are 6 students left over. If the students are divided into groups of 12, there are 9 students left over. How many students are there?

Solution. Let x be the number of students, then x leaves remainder 6 on division by 11 and remainder 9 on division by 12. Write this as a pair of congruences:

$$x \equiv 6 \mod 11 \quad \text{and} \quad x \equiv 9 \mod 12.$$

To solve, write $x = 6 + 11k = 9 + 12\ell$, $k, \ell \in \mathbb{Z}$. Rearrange to get $11k - 12\ell = 3$. Instead of doing Euclid's algorithm, notice that $11 \times 1 - 12 \times 1 = -1$ and multiply through by -3 to obtain

$$11(-3) - 12(-3) = 3.$$

Hence $(k_0, \ell_0) = (-3, -3)$ is a particular solution of the Diophantine equation. The general solution is $(k, \ell) = (-3 + 12t,\ -3 + 11t)$, $t \in \mathbb{Z}$ so $x = 6 + 11k = 6 + 11(-3 + 12t) = -27 + 132t$, equivalently $x \equiv -27 \mod 132$. This answer is better written using *the least non-negative residue mod* 132, i.e. the remainder of -27 which is $-27 + 132 = 105$:

$$x \equiv 105 \mod 132.$$

We remark that 105 plays the role of x_0 in the Chinese Remainder Theorem, as $x_0 = 105$ is the unique solution of the congruence which satisfies $0 \leq x_0 < 11 \times 12$.

However, 105 is not between 200 and 300. The only solution between 200 and 300 is

$$x = 105 + 132 = 237$$

since it is easy to see that all the other solutions are either less than 200 or greater than 300. Answer: 237 students.

Method of Successive Squaring

Remark (motivation)**.** In modern times, congruences modulo m have many practical applications, for example in cryptography. To decipher data, one often needs to calculate the remainder of a^N when divided by m. Here $m \in \mathbb{N}$ is the modulus, a is a given integer representing a piece of data, and $N \in \mathbb{N}$ is a large number. Usually a^N is so astronomically large that it cannot be calculated directly. We will consider a method which will allow us to find the remainder without finding a^N itself.

The Modular Arithmetic proposition implies that if $a \equiv b \mod m$ then $a \times a \equiv b \times b \mod m$, that is, $a^2 \equiv b^2 \mod m$. This leads us to the following method of **finding a residue of** a^2 **mod** m:

- Find a residue r of a mod m. This can be the remainder of a when divided by m in which case $0 \leq r < m$. We have $a \equiv r \mod m \implies a^2 \equiv r^2 \mod m$.
- Calculate r^2 and find a residue r_1 (usually the remainder) of r^2 mod m.
- We have $a^2 \equiv r_1 \mod m$.

This idea can be repeated and the resulting method of **finding a residue of a^N mod m** is best illustrated by an example.

Example (Method of Successive Squaring)**.** What is the remainder of 4^{100} when divided by 13?

Solution.
- $4^2 = 16 \equiv 3 \mod 13$, so
- $4^4 \equiv 3^2 \equiv 9 \mod 13$, so
- $4^8 \equiv 9^2 = 81 \equiv 3 \mod 13$, so
- $4^{16} \equiv 3^2 \equiv 9 \mod 13$, so
- $4^{32} \equiv 9^2 \equiv 3 \mod 13$, so
- $4^{64} \equiv 3^2 \equiv 9 \mod 13$.

Then

$$\begin{aligned} 4^{100} &= 4^{64+32+4} \\ &= 4^{64} \times 4^{32} \times 4^4 \\ &\equiv 9 \times 3 \times 9 = 27 \times 9 \equiv 1 \times 9 \\ &\equiv 9 \mod 13. \end{aligned}$$

Hence 9 is a residue of 4^{100} mod 13 and, as $0 \leq 9 < 13$, we conclude that 9 is the remainder of 4^{100} when divided by 13.

Remark (writing N as a sum of powers of 2)**.** Clearly successive squaring gives us residues of $a^{(2^k)}$ mod m so in order to find a residue of a^N mod m we write N as a sum of powers of 2. This is the same as *writing the exponent in binary notation*. So, in this example

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

and $64, 32$ and 4 are the exponents seen above.

Question. How to write a number N as a sum of distinct powers of 2?

Answer.
- Find the highest power 2^k of 2 such that $2^k \leq N$;
- write $N = 2^k + N_1$; here $N_1 < 2^k$ (otherwise we would have found at least 2^{k+1} in the previous step);
- repeat the process to write N_1 as a sum of powers of 2.

Example. Find the last 2 digits of 1913^{99}.

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

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

So the two digits of the remainder of $1913^{99} \mod 100$ will be the last two digits of 1913^{99}.

		$\mod 100$
$1913^2 \equiv 13^2$		$\equiv 69$
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

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

So the last two digits of 1913^{99} are 7 and 7.

Exercise (for students to attempt in their own time)**.** What are the last *three* digits of 13^{99}? What are the last two digits of 13^{1010}?

Non-linear Diophantine Equations

As an example of the use of congruences we can use them to show when some Diophantine equations do *not* have integer solutions. This is quite a negative application — we do **not** prove that the equations have solutions, if they do!

Idea. 1) Given a Diophantine Equation first *assume* it has integer solutions.

2) Then look at the equation modulo an appropriate modulus.

3) Find a contradiction.

Example. Prove that there are **no** integral solutions to

$$15x^2 - 7y^2 = 1.$$

Solution. Assume there **is** a solution $(x_0, y_0) \in \mathbb{Z}^2$, so $15x_0^2 - 7y_0^2 = 1$. Look at the equation modulo 5 to get

$$0x^2 - 7y_0^2 \equiv 1 \mod 5 \qquad \Longleftrightarrow \qquad 3y_0^2 \equiv 1 \mod 5.$$

Our logic in choosing modulus 5 here is that the term $15x^2$ becomes zero mod 5. Indeed, $5 \mid 15$ and

$$a \equiv 0 \mod m \qquad \Longleftrightarrow \qquad m \mid a.$$

Multiplying both sides of the congruence by 2 we get

$$6y_0^2 \equiv 2 \mod 5 \qquad \text{i.e.} \qquad y_0^2 \equiv 2 \mod 5.$$

We see if this is possible or not by testing each possible remainder of y modulo 5:

$y \mod 5$	$y^2 \mod 5$
0	0
1	1
2	4
3	4
4	1

We can see that a square can be congruent only to 0, 1 or 4 modulo 5. In **no** case do we get $y^2 \equiv 2 \mod 5$, there being no 2 in the right hand column. So our assumption that $15x^2 - 7y^2 = 1$ has a solution has led to a *contradiction modulo* 5. Hence the original equation has no integer solutions.

Remark (A chosen module is not guaranteed to work)**.** If we look at the equation modulo 7, we get

$$15x_0^2 \equiv 1 \mod 7 \quad \iff \quad x_0^2 \equiv 1 \mod 7.$$

Unfortunately there is a solution to this, namely $x_0 = 1$. Thus we have **not** found a contradiction. This does not mean that there is anything wrong with the method, just that this modulus has not led to a contradiction.

Solution (Alternative Solution)**.** We could have looked at the equation **modulo** 3, to get $-7y_0^2 \equiv 1 \mod 3$, equivalently $2y_0^2 \equiv 1 \mod 3$. Multiply both sides by 2 to get $4y_0^2 \equiv 2 \mod 3$, i.e. $y_0^2 \equiv 2 \mod 3$. We see if this is possible or not by testing each possible value for y.

$y \mod 3$	$y^2 \mod 3$
0	0
1	1
2	1

In **no** case do we get $y^2 \equiv 2 \mod 3$. So our assumption that $15x^2 - 7y^2 = 1$ has a solution has led to a *contradiction modulo 3*. Hence the original equation has no integer solutions.

Remark (Benefit of a smaller modulus)**.** The lesson from this is that the smaller you take the modulus the smaller the table, i.e. the less work you have to do.

Example. Show that for any $n \equiv 1 \mod 7$ no integers a, b can be found satisfying

$$n = 2a^3 - 5b^3.$$

Solution. The information concerning n is given modulo 7 so we look at the Diophantine equation modulo 7, and try to find integer solutions of

$$2a^3 - 5b^3 \equiv 1 \mod 7 \qquad \text{which is equivalent to} \quad 2a^3 + 2b^3 = 2(a^3 + b^3) \equiv 1 \mod 7.$$

Observe that 4 is the inverse of $2 \mod 7$, i.e., $4 \times 2 \equiv 1 \mod 7$. Multiply both sides of the congruence by 4:

$$2(a^3 + b^3) \equiv 1 \mod 7 \iff 4 \times 2(a^3 + b^3) \equiv 4 \times 1 \mod 7 \iff a^3 + b^3 \equiv 4 \mod 7.$$

We search all possible values of $\left(a^3, b^3\right) \mod 7$.

$a \mod 7$	$a^3 \mod 7$
0	0
1	1
2	1
3	$3^3 = 27 \equiv 6$
4	$4^3 \equiv (-3)^3 \equiv -3^3 \equiv -6 \equiv 1$
5	6
6	6

Hence a^3 takes only 3 different values modulo 7, i.e.

$$a^3 \equiv 0, 1 \text{ or } 6 \mod 7.$$

Thus there are only 9 different possibilities for the pair $\left(a^3, b^3\right) \mod 7$:

$\left(a^3, b^3\right) \mod 7$	$a^3 + b^3 \mod 7$
$(0, 0)$	0
$(0, 1)$	1
$(0, 6)$	6
$(1, 0)$	1
$(1, 1)$	2
$(1, 6)$	0
$(6, 0)$	6
$(6, 1)$	$7 \equiv 0$
$(6, 6)$	$12 \equiv 5$

In no row do we see a final result of 4, hence $a^3 + b^3$ is never $\equiv 4 \mod 7$, hence no $n \equiv 1 \mod 7$ can be written as $2a^3 - 5b^3$ for integers a and b.

Question. How do we find the appropriate modulus?

Answer. There is no method for finding the right modulus, we have to look at the original equation with different moduli, trying to find a case that has no solutions. If, for all moduli we choose, the resulting congruence has a solution, there is a chance that the original equation has solutions, but if so these have to be found by other means.

Exercise. Other examples students may wish to try in their own time:

Show that $7x^4 + 2y^3 = 3$ has no integer solutions.

Show that 5 does not divide $a^3 + a^2 + 1$ for any $a \in \mathbb{Z}$.

Show that $2x^3 + 27y^4 = 21$ has no integer solutions.

Show that $7x^5 + 3y^4 = 2$ has no integer solutions.