Diophantine equations.

How hard can they be?

In 1900, the German mathematician David Hilbert proposed a list of 23 mathematical problems. He gave a talk on these problems at the 1900 International Congress of Mathematicians. (Wikipedia link to Hilbert's problems.) Hibert's problems were interesting and profound, and work on them led to a lot of interesting mathematical ideas in the 20th century. It's interesting to note that, as far as I know, no computer program has ever come up with an interesting and profound mathematical question. Finding the right question is an *art*. It's like level design.

Click on the link above to see all of Hilbert's problems on Wikipedia. I am just going to talk about Hilbert's tenth problem.

Hilbert's tenth problem.

"Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers."

A formalisation of what Hilbert is asking: he challenges us to give an *algorithm*, like Euclid's Algorithm. He wants an algorithm which takes an arbitrary Diophantine equation, such as $x^7 + y^7 = z^7 + 12345$, as input, and outputs "yes" if the Diophantine equation has a solution in integers x and y, and "no" otherwise.

Hilbert's tenth problem is one of the Hilbert problems which has been completely solved. It is generally believed that in 1900 Hilbert would have been extremely surprised by the solution.

Hilbert's tenth problem: devise an algorithm which takes as input a Diophantine equation and outputs "yes" if the equation has a solution with all of the variables integers and "no" if it does not.

Theorem (Matiyasevich–Robinson–Davis–Putnam, 1970). No such algorithm exists.

Diophantine equations take us to the *boundaries of what is possible in mathematics.* That's why they're hard.

Let's try and solve some Diophantine equations!

Find all integers x and y such that

$$3478x^7 + 3473464x^2y^8 + 32874y^{2018} = 38y^2(x+1)^{53} + 12345.$$

There are no solutions to this equation! If x and y are any integers, then one can see easily that the left hand side is even and the right hand side is odd.

Later on in this lecture we'll see a generalisation of this trick. Methods like this are called "local methods". I want to show you one global method first though.

I told you last time that finding all integer solutions to $x^3 - x = y^5 - y$ was beyond human capabilities. But that's degree 5 in two variables! For degree 3 equations in two variables, we are getting quite good. If we could solve the Birch and Swinnerton-Dyer conjecture, we would be in even better shape.

Here is a cool result.
Theorem. The only integer solutions to $y^2 - x^3 = 17$ with $x, y \in \mathbb{Z}_{\geq 1}$ are: $17 = 5^2 - 2^3 = 9^2 - 4^3 = 23^2 - 8^3 = 282^2 - 43^3 = 375^2 - 52^3 = 378661^2 - 5234^3$ and that's it. There are however infinitely many rational solutions, and we have a "formula" for them.

As far as I know, all known proofs of this theorem use extensive computer calculations. We won't be proving this theorem in M1F.

Exercise. Assuming the theorem above, find all solutions to $y^2 - x^3 = 17$ with $x, y \in \mathbb{Z}$.

Here is another cubic example, which we can solve completely.

Example. The only solutions to $4y^2 = x^3 + 1$ with $x, y \in \mathbb{Z}$ are $(x, y) = (-1, 0)$.

Proof. If $x, y \in \mathbb{Z}$ satisfy this equation, then because the left hand side is non-negative we must have $x^3 \geq -1$ and hence $x \geq -1$. We can see that for $x = -1$ the only possibility is $y = 0$, and that for $x = 0$ there are no possibilities for y.

I claim there are no solutions with $x \geq 1$. We prove this by contradiction. Say $x \geq 1$ and $y \in \mathbb{Z}$ satisfy $x^3 + 1 = 4y^2$. By changing the sign of y, we can assume $y \geq 0$. Now $y = 0$ doesn't work because $x \geq 1$, so we must have $y > 0$ and hence $y \geq 1$.

We've reduced the question to

Hypotheses: $x, y \in \mathbb{Z}_{\geq 1}$ and $4y^2 = x^3 + 1$. Goal: get a contradiction.

Rewrite the equation as $4y^2 - 1 = x^3$, and factor the left hand side as $(2y-1)(2y+1)$. We know $y \geq 1$, so $2y-1$ and $2y+1$ are both positive integers. I claim that $\text{hcf}(2y-1, 2y+1) = 1$. Indeed, if e divides $2y-1$ and $2y+1$ then it divides their difference, which is 2. So $e = 1$ or $e = 2$. But $e = 2$ doesn't work because $2y+1$ is odd. So the only common factor of $2y-1$ and $2y+1$ is 1.

So far: if $x, y \in \mathbb{Z}_{\geq 1}$ and $4y^2 = x^3 + 1$ then $(2y-1)(2y+1) = x^3$ and $\text{hcf}(2y-1, 2y+1) = 1$.

Now recall

Proposition 7.15. If $a, b, c, n \in \mathbb{Z}_{\geq 1}$ with $\text{hcf}(a, b) = 1$, and if $ab = c^n$, then both a and b are nth powers of positive integers.

By Proposition 7.15 we can deduce that $2y - 1$ and $2y + 1$ are both positive cubes. However the positive cubes are $1, 8, 27, 64, \ldots$ and clearly no two can differ by 2 – consecutive differences are easily checked to be greater than 2. This is a contradiction, which finishes the proof of the example.

Congruences.
Say $a, b, \in \mathbb{Z}$ and $m \in \mathbb{Z}_{\geq 1}$. We say "$a$ is congruent to b mod m" if $a - b$ is a multiple of m.
There is some very cool notation for this:

$$a \equiv b \bmod m.$$

Unfolding the definition of "is a multiple of", we see that
$\forall a, b \in \mathbb{Z}, \forall m \in \mathbb{Z}_{\geq 1}$,

$$a \equiv b \bmod m \iff \exists k \in \mathbb{Z}, a - b = m * k.$$

That $\equiv$ notation (`\equiv` in LaTeX, `\==` in Lean) looks very like the notation for equality! This is not a coincidence. In fact $\equiv$ satisfies a whole bunch of basic properties that $=$ also satisfies. We will see some of these later. But first let's do examples.

$$a, b \in \mathbb{Z}, m \in \mathbb{Z}_{\geq 1}.$$

We say *a is congruent to b mod m* if $a - b$ is a multiple of m.

$$a \equiv b \bmod m \iff m \mid (a - b).$$

[What does "if" mean in a *definition*?] [It means if and only if!]

Examples.

$$31 \equiv 81 \equiv 1234321 \bmod 10.$$

Why? All of 31, 81, 1234321 end in 1, so the difference of two such numbers will end in zero and will hence be a multiple of 10. Is $31 \equiv -51 \bmod 10$? No! What should the units digit of -51 be to make it work? $31 \equiv -59 \bmod 10$.

$$a, b \in \mathbb{Z}, m \in \mathbb{Z}_{\geq 1}.$$

We say *a is congruent to b mod m* if $a - b$ is a multiple of m.

$$a \equiv b \bmod m \iff m \mid (a - b).$$

Examples.

If $a \in \mathbb{Z}$ then $a \equiv 0 \bmod m$ is just another way of saying that a is a multiple of m.

For example, an integer n is even if and only if $n \equiv 0 \bmod 2$. And n is odd if and only if $n \equiv 1 \bmod 2$. Every integer is exactly one of even or odd, so every integer is congruent to either 0 or 1 modulo 2, but not both.

Why is every integer exactly one of even or odd?

We proved this!

Lemma 7.1 (division with remainder.) Say $a \in \mathbb{Z}$ and $m \in \mathbb{Z}_{\geq 1}$ are integers. Then
(i) we can write $a = qm + r$ with q ("quotient") an integer, and r ("remainder") an integer satisfying $0 \leq r < m$.
(ii) If $a = qb + r = q'b + r'$ with $q, q' \in \mathbb{Z}$ and $0 \leq r, r' < b$, then $q = q'$ and $r = r'$.

Applying Lemma 7.1 with $m = 2$, we deduce that any integer a can be written as $a = 2q + r$ with $0 \leq r \leq 1$, and that the quotient and the remainder were *unique*.
So every integer either leaves remainder 0 or remainder 1 when you divide it by 2, and no integer leaves both! Hence every integer is either of the form $2q$ or of the form $2q + 1$ (and never both), and hence every integer is exactly one of even or odd.

How does this even/odd trick generalise to a general congruence mod m?

Lemma 7.16. If $a \in \mathbb{Z}$ and $m \in \mathbb{Z}_{\geq 1}$ then there exists a unique integer r (depending on a), with $0 \leq r \leq m-1$ and $a \equiv r \bmod m$.

Lemma 7.1 (division with remainder.) Say $a \in \mathbb{Z}$ and $m \in \mathbb{Z}_{\geq 1}$ are integers. Then
(i) we can write $a = qm + r$ with q ("quotient") an integer, and r ("remainder") an integer satisfying $0 \leq r < m$.
(ii) If $a = qb + r = q'b + r'$ with $q, q' \in \mathbb{Z}$ and $0 \leq r, r' < b$, then $q = q'$ and $r = r'$.

Proof of 7.16. Existence of r: We can write $a = qm + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r \leq m-1$, by Lemma 7.1(i). Then $a - r$ is a multiple of m, and hence $a \equiv r \bmod m$.

Uniqueness of r: Say $a = qm + r$ as above, with $0 \leq r \leq m-1$. if r' is an integer with $0 \leq r' \leq m-1$ and $a \equiv r' \bmod m$, then by definition of $\equiv$ there exists an integer q' such that $a - r' = q'm$. Hence $a = q'm + r'$ and by Lemma 7.1(ii) we must have $q = q'$ and $r = r'$. So r is unique.

Exercise: every integer a is congruent to exactly one of 0,1,2,3 mod 4. Which ones are the even ones and which ones are the odd ones?

Exercise: every integer a is congruent to exactly one of 0,1,2 mod 3. Which ones are the even ones and which ones are the odd ones?

Let's go back to why the notation $\equiv$ for congruence looks a bit like $=$.

Euclid's Elements are a series of 13 mathematical volumes, written 2300 years ago. It is said to be the most successful and influential textbook ever written. (Wikipedia link.) Euclid introduced axiomatic reasoning into mathematics, with "postulates" and some "common notions".

Common notion 4: Things that coincide with one another are equal to one another

Formalisation of common notion 4: $\forall x,\ x = x$.

Common notion 1: Things that are equal to the same thing are also equal to one another.

Formalisation of common notion 1:
$\forall x\ y\ z,\ x = z \wedge y = z \implies x = y$.

Things we all believe about equals:
1) $x = x$;
2) If $x = y$ then $y = x$;
3) If $x = y$ and $y = z$ then $x = z$.

Here are some theorems about congruence mod m.

Theorem 7.17. Say $m \in \mathbb{Z}_{\geq 1}$ and $a, b, c \in \mathbb{Z}$.
1) $a \equiv a \bmod m$;
2) If $a \equiv b \bmod m$ then $b \equiv a \bmod m$;
3) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$.

That's why I mean by "congruence mod m behaves in a similar way to equality".