Lecture 4 | Part 2 - Diophantine equations

Three ex-problems

(A) $P \in \mathbb{Z}[t_1, t_2, \dots, t_n]$, ? $\exists (a_1, a_2, \dots, a_n) \in \mathbb{Z}^n$ s.t. $P(a_1, a_2, \dots, a_n) = 0$? That is, is solvability of the equation $P = 0$ in integers decidable by an algorithm?

A related problem (algorithms were not known then) was posed by D. Hilbert in 1900 and is known as Hilbert's tenth problem. He asked for a procedure deciding solvability in integers of a given Diophantine equation.

A set $X \subset \mathbb{Z}^n$ is Diophantine: $\exists Q \in \mathbb{Z}[x_1, \dots, x_n, y_1, \dots, y_m]$ s.t. $(x_1, \dots, x_n) \in X \Leftrightarrow \exists \bar{b} \in \mathbb{Z}^m : Q(\bar{x}, \bar{b}) = 0$.

($\bar{x}$ = $(x_1, \dots, x_n)$)

A set $X \subset \mathbb{Z}^n$ is decidable (recursive): $\exists$ an algorithm $\mathcal{A} : \mathbb{Z}^n \to \{0, 1\}$ s.t. $\mathcal{A}$ terminates on each input and $\bar{x} \in X \Leftrightarrow \mathcal{A}(\bar{x}) = 1$, $\bar{x} \notin X \Leftrightarrow \mathcal{A}(\bar{x}) = 0$.

A set $X \subset \mathbb{Z}^n$ is listable (recursively enumerable): $\exists$ an algorithm $\mathcal{A}: \mathbb{N} \to \mathbb{Z}^n$ (allowing $X = \emptyset$ or $X = \mathbb{Z}^n$) s.t. $\mathcal{A}$ terminates on each input and (as a map) $\mathcal{A}(\mathbb{N}) = X$.

It is not obvious how to use the $\mathcal{A}$ showing that X is listable to show that X is decidable and indeed in 1936 Alonzo A. Turing (1912–1954) proved that $\exists X \subset \mathbb{Z}^n$ that is listable but not decidable. *)

The DPRM theorem (1970)

Every listable set is Diophantine.

Corollary

$\exists Q \in \mathbb{Z}[x_1, \dots, x_n, y_1, \dots, y_m]$ s.t. the question: for given $\bar{x} \in \mathbb{Z}^n$, is there a $\bar{y} \in \mathbb{Z}^m$ s.t. $Q(\bar{x}, \bar{y}) = 0$? is not algorithmically decidable.

*) Obviously, decidable $\subset$ listable and Diophantine $\subset$ listable.

③ In fact, the polynomial Q can be presented explicitly.

D: Martin Davis (1928)
P: Hilary Putnam (1926-2016)
R: Julia Robinson (1919-1985)
M: Yuri V. Matiyasevich (1947)

(B) **Theorem (Wiles-Taylor) 1995** = Fermat's Last Theorem, FLT

$x,y,z,n \in \mathbb{Z}, n \geq 3, x^n + y^n = z^n \Rightarrow xyz = 0.$

(that is, $x^n + y^n = z^n$ has for $n \in \mathbb{N}, n \geq 3$, no solution $x,y,z \in \mathbb{N}$.)

Andrew Wiles (1953) Sir!
Richard Taylor (1962)

(C) **Catalan's Conjecture**

④ Named after

• Eugène Ch. Catalan (1814–1894)

$n \in \mathbb{N}$ is a pure power if $n = a^b$ for some $a, b \in \mathbb{N} \setminus \{1\}$. For example, $8 = 2^3$ and $9 = 3^2$ are p. powers.

Conjecture (E. Catalan, 1844)

8 and 9 are the only consecutive pure powers

In other words, $x^a - y^b = 1$ has no solution $x, y, a, b \in \mathbb{N} \setminus \{1\}$ other than $3^2 - 2^3 = 1$.

If $x^a - y^b = 2$ has other solution in than $3^3 - 5^2 = 2$ is not known.

Catalan's conjecture was proven in 2002 by • Preda Mihăilescu (1955).

Pythagorean triples, **Theorem** $\nexists\, x, y, z \in \mathbb{Z}$ satisfy that $x^2 + y^2 = z^2$ $\Leftrightarrow$ $\exists\, a, b, c \in \mathbb{Z}$ s.t. $z = a(b^2 + c^2)$ and (i) $x = 2abc$, $y = a(b^2 - c^2)$ or

(5) (ii) $x = a(b^2 - c^2)$, $y = 2abc$.

~~Lemma Let $a \in \mathbb{N}$. If $x, y \in \mathbb{Z}$ are s.t. $xy = a^2$, then $x = bc^2$, $y = d^2$ for some~~

Proof. $\Leftarrow$ is trivial. Let us prove $\Rightarrow$.

We may assume that $x, y, z \in \mathbb{N}$ and are such that $x^2 + y^2 = z^2$ and $(x, y) = (x, z) = (y, z) = 1$.

$\rightsquigarrow$ x is even, y and z are odd.

$\rightsquigarrow \left(\frac{x}{2}\right)^2 = \frac{z-y}{2} \cdot \frac{z+y}{2} \rightsquigarrow \left(\frac{z-y}{2}, \frac{z+y}{2}\right) = 1$ ($\in \mathbb{N}$, $\in \mathbb{N}$)

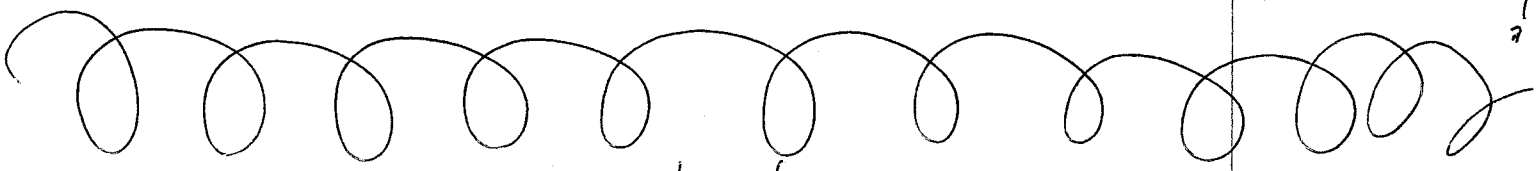
and their product is a $\square$ $\rightsquigarrow \frac{z+y}{2} = b^2$ and $\frac{z-y}{2} = c^2$ for some $b, c \in \mathbb{N}$. Summing a subtracting we get: $z = b^2 + c^2$, $y = b^2 - c^2$ and $x = 2bc$. For every y and odd x we get case (ii) ☒

Exercise Check that in the general case (if $x, y, z \in \mathbb{Z}$ and not coprime) we really get the above parametric expressions.

(6) **Theorem (P. de Fermat, 17th century)**

$x^4+y^4=z^2$ has no solution $x,y,z \in \mathbb{Z}$ with $xyz \neq 0$.

Proof: In the next lecture!



Not the end of the lecture yes: a nice problem on Pyth. Δ triples solved by a SAT-solver.

M. J. Heule, O. Kullmann, V. W. Marek:

$$\neg\exists f : \mathbb{N}=\{1,2,\dots\} \to \{0,1\} \text{ s.t.}$$

$$a,b,c \in \mathbb{N},\ f(a)=f(b)=f(c) \Rightarrow a^2+b^2 \neq c^2$$

that is, it is impossible to 2-color the natural numbers $\mathbb{N}$ so that there is no monochromatic Pyth. triple.

Proof: By a SAT-solver, needs 200 TB of memory & they prove it for $\{1,2,\dots,7825\}$ in place of $\mathbb{N}$, and 7825 is minimum with the property.