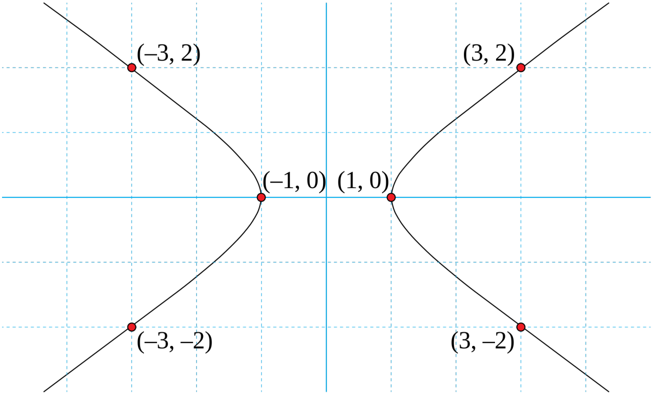
What is...Matiyasevich's theorem?

Or: I can't decide...

Pell's equation: $x^2 - n \cdot y^2 = 1$

A polynomial equation has infinitely many solutions in an appropriate field:

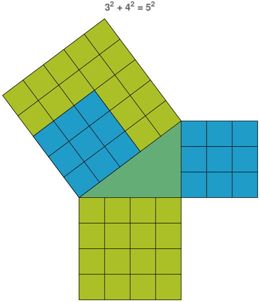


$$x^2 - 2y^2 = 1$$

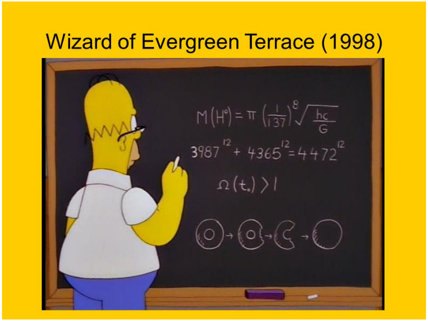
Diophantus and others. Are there solutions in the integers $\mathbb{Z}$?

These are (very) classical questions!

Pythagorean triples $x^2 + y^2 = z^2$:



Fermat's last theorem $x^n + y^n = z^n$:



Find an algorithm

If $x^2 - n \cdot y^2 - 1 = 0$ has a solution, then we can find it by brute force:

```
In[92]:= Table[Solve[x^2 - 2*y^2 - 1 == 0, x], {y, 0, 10}]
```

$$\text{Out[92]=}\ \{\{\{x \to -1\}, \{x \to 1\}\}, \{\{x \to -\sqrt{3}\}, \{x \to \sqrt{3}\}\}, \{\{x \to -3\}, \{x \to 3\}\}, \{\{x \to -\sqrt{19}\}, \{x \to \sqrt{19}\}\}, \{\{x \to -\sqrt{33}\}, \{x \to \sqrt{33}\}\}, \{\{x \to -\sqrt{51}\}, \{x \to \sqrt{51}\}\}, \{\{x \to -\sqrt{73}\}, \{x \to \sqrt{73}\}\}, \{\{x \to -3\sqrt{11}\}, \{x \to 3\sqrt{11}\}\}, \{\{x \to -\sqrt{129}\}, \{x \to \sqrt{129}\}\}, \{\{x \to -\sqrt{163}\}, \{x \to \sqrt{163}\}\}, \{\{x \to -\sqrt{201}\}, \{x \to \sqrt{201}\}\}\}$$

Main problem. Can we do anything in general if there are no solutions?

I am not asking:

- To find all solutions
- To have an efficient algorithm
- To have an algorithm that works in practice

Enter, the theorem!

Listable if and only Diophantine

- Listable. There is an algorithm that enumerates the members of D.
- Diophantine. $D \subset \mathbb{N}^j$ such that, for some $P(x_1, ..., x_j, y_1, ..., y_k)$ we have

$$(x_1, ..., x_j) \in D \Leftrightarrow \left(\exists (y_1, ..., y_k) \in \mathbb{N}^k\right) : \left(P(x_1, ..., x_j, y_1, ..., y_k) = 0\right)$$

- I showed you that every Diophantine is listable – the converse is the main meat

Crucial implication. There is no algorithmic decision procedure for determining whether an arbitrary Diophantine equation has a solution

- This was Hilbert's tenth problem
- There are non-decidable sets; examples come from statements that are not provable is Peano arithmetic

A fun application

(Listable if and only if Diophantine) $\Rightarrow$ (Primes is a Diophantine set)

Here is an example:

DIOPHANTINE REPRESENTATION OF THE SET OF PRIME NUMBERS

JAMES P. JONES, DAIHACHIRO SATO, HIDEO WADA AND DOUGLAS WIENS

1. Introduction. Martin Davis, Yuri Matijasevič, Hilary Putnam and Julia Robinson [4] [8] have proven that every recursively enumerable set is Diophantine, and hence that the set of prime numbers is Diophantine. From this, and work of Putnam [12], it follows that the set of prime numbers is representable by a polynomial formula. In this article such a prime representing polynomial will be exhibited in explicit form. We prove (in Section 2)

THEOREM 1. *The set of prime numbers is identical with the set of positive values taken on by the polynomial*

$$
\begin{aligned}
\text{(1)}\quad & (k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)\cdot(h+j)+h-z]^2-[2n+p+q+z-e]^2\\
&-[16(k+1)^3\cdot(k+2)\cdot(n+1)^2+1-f^2]^2-[e^3\cdot(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2\\
&-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)\cdot(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2\\
&-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2\\
&-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}
\end{aligned}
$$

as the variables range over the nonnegative integers.

Thank you for your attention!

I hope that was of some help.