# The Local-Global Principle

Sebastiano Tronto

28 March 2019

Figure: Diophantus of Alexandria (III century)

# Diophantine Equations

# Diophantine Equations

- Very old problem

# Diophantine Equations

- Very old problem
- Very simple in their formulation, but...

# Diophantine Equations

- Very old problem
- Very simple in their formulation, but...
- ... very hard to solve!

# Diophantine Equations

- Very old problem
- Very simple in their formulation, but...
- ... very hard to solve!
- "Fermat's Last Theorem" took centuries to be proved (stated in 1637 - proved to be true in 1995)

# Diophantine Equations

# Diophantine Equations

$X^2 + Y^2 = Z^2$ Pythagora's Triples

# Diophantine Equations

| | |
|---|---|
| $X^2 + Y^2 = Z^2$ | Pythagora's Triples |
| $X^n + Y^n = Z^n$ | Fermat's Equation |

# Diophantine Equations

| | |
|---|---|
| $X^2 + Y^2 = Z^2$ | Pythagora's Triples |
| $X^n + Y^n = Z^n$ | Fermat's Equation |
| $X^2 - nY^2 = 1$ | Pell's Equation |

# Diophantine Equations

| | |
|---|---|
| $X^2 + Y^2 = Z^2$ | Pythagora's Triples |
| $X^n + Y^n = Z^n$ | Fermat's Equation |
| $X^2 - nY^2 = 1$ | Pell's Equation |

In general, we have a **polynomial** with **integer coefficients**

$$F(X_1, \ldots, X_n)$$

# Diophantine Equations

| | |
|---|---|
| $X^2 + Y^2 = Z^2$ | Pythagora's Triples |
| $X^n + Y^n = Z^n$ | Fermat's Equation |
| $X^2 - nY^2 = 1$ | Pell's Equation |

In general, we have a **polynomial** with **integer coefficients**

$$F(X_1, \dots, X_n)$$

and we want to find **integer** solutions of

$$F(X_1, \dots, X_n) = 0.$$

# Modular Arithmetic

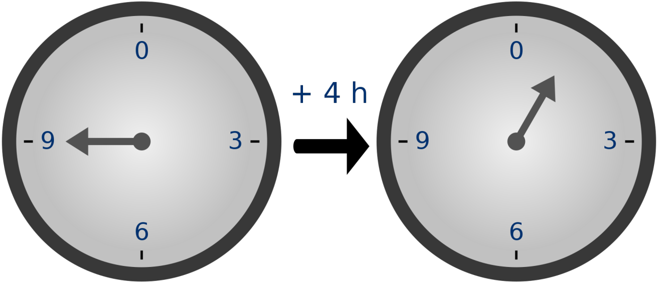



Figure: $9 + 4 = 1!$

# Modular Arithmetic

# Modular Arithmetic

- Fix an integer number $N > 1$ (say $N = 12$).

# Modular Arithmetic

- Fix an integer number $N > 1$ (say $N = 12$).
- For every other integer $m$, consider the **remainder** $[m]_N$ of the division of $m$ by $N$.

# Modular Arithmetic

- Fix an integer number $N > 1$ (say $N = 12$).
- For every other integer $m$, consider the **remainder** $[m]_N$ of the division of $m$ by $N$.
- For example $[23]_{12} = [11]_{12}$.

- Fix an integer number $N > 1$ (say $N = 12$).
- For every other integer $m$, consider the **remainder** $[m]_N$ of the division of $m$ by $N$.
- For example $[23]_{12} = [11]_{12}$.

**Notation:** $$23 \equiv 11 \pmod{12}$$

# Modular Arithmetic

On the set $\{[0]_N, [1]_N, \dots, [N-1]_N\}$ we define operations:

$$[x]_N + [y]_N = [x+y]_N \qquad [x]_N \cdot [y]_N = [x \cdot y]_N$$

# Modular Arithmetic

On the set $\{[0]_N, [1]_N, \dots, [N-1]_N\}$ we define operations:

$$[x]_N + [y]_N = [x+y]_N \qquad [x]_N \cdot [y]_N = [x \cdot y]_N$$

These operations behave well (associativity, commutativity...) and the set $\mathbb{Z}/N = \{[0]_N, [1]_N, \dots, [N-1]_N\}$ is a **ring**.

- **Example 1.** (12-hour clock) If it is 9h00, what time is it going to be in 4 hours from now?

- **Example 1.** (12-hour clock) If it is 9h00, what time is it going to be in 4 hours from now?

$$[9]_{12} + [4]_{12} = [9+4]_{12} = [13]_{12} = 1$$

Answer: 1h00!

- **Example 1.** (12-hour clock) If it is 9h00, what time is it going to be in 4 hours from now?

$$[9]_{12} + [4]_{12} = [9 + 4]_{12} = [13]_{12} = 1$$

  Answer: 1h00!

- **Example 2.** (24-hour clock) If it is 17:00, what time was it 72 hours ago?

- **Example 1.** (12-hour clock) If it is 9h00, what time is it going to be in 4 hours from now?

$$[9]_{12} + [4]_{12} = [9+4]_{12} = [13]_{12} = 1$$

Answer: 1h00!

- **Example 2.** (24-hour clock) If it is 17:00, what time was it 72 hours ago?

$$[17]_{24} - [72]_{24} = [17]_{24} - [0]_{24} = [17]_{24}$$

Answer: again 17:00!

# Reducing Equations Modulo $N$

# Reducing Equations Modulo $N$

- Consider the equation $X^2 + 5Y^2 = 10Z^3 + 3$.

# Reducing Equations Modulo $N$

- Consider the equation $X^2 + 5Y^2 = 10Z^3 + 3$.
- If the two sides are equal, then certainly:

$$[X^2 + 5Y^2]_N = [10Z^3 + 3]_N$$

# Reducing Equations Modulo $N$

- Consider the equation $X^2 + 5Y^2 = 10Z^3 + 3$.
- If the two sides are equal, then certainly:

$$[X^2 + 5Y^2]_N = [10Z^3 + 3]_N$$

- But we can rewrite:

$$[X]_N^2 + [5]_N \cdot [Y]_N^2 = [10]_N \cdot [Z]_N^3 + [3]_N$$

And get an equation to be solved in $\mathbb{Z}/N$.

# Reducing Equations Modulo $N$

- For example with $N = 5$, the equation

$$X^2 + 5Y^2 = 10Z^3 + 3$$

# Reducing Equations Modulo $N$

- For example with $N = 5$, the equation

$$X^2 + 5Y^2 = 10Z^3 + 3$$

becomes:

$$X^2 \equiv 3 \pmod 5$$

which is much easier to deal with!

# Reducing Equations Modulo $N$

- For example with $N = 5$, the equation

$$X^2 + 5Y^2 = 10Z^3 + 3$$

becomes:

$$X^2 \equiv 3 \pmod{5}$$

which is much easier to deal with!

- Since $\mathbb{Z}/5$ is a **finite set**, we can try all its elements to check if there is a solution.

# Reducing Equations Modulo $N$

$$[0]_5^2 = [0]_5 \neq [3]_5$$

# Reducing Equations Modulo $N$

$$[0]_5^2 = [0]_5 \neq [3]_5$$
$$[1]_5^2 = [1]_5 \neq [3]_5$$

$$[0]_5^2 = [0]_5 \neq [3]_5$$
$$[1]_5^2 = [1]_5 \neq [3]_5$$
$$[2]_5^2 = [4]_5 \neq [3]_5$$

$$
\begin{aligned}
[0]_5^2 &= [0]_5 \neq [3]_5 \\
[1]_5^2 &= [1]_5 \neq [3]_5 \\
[2]_5^2 &= [4]_5 \neq [3]_5 \\
[3]_5^2 &= [9]_5 = [4]_5 \neq [3]_5
\end{aligned}
$$

# Reducing Equations Modulo $N$

$$[0]_5^2 = [0]_5 \neq [3]_5$$
$$[1]_5^2 = [1]_5 \neq [3]_5$$
$$[2]_5^2 = [4]_5 \neq [3]_5$$
$$[3]_5^2 = [9]_5 = [4]_5 \neq [3]_5$$
$$[4]_5^2 = [16]_5 = [1]_5 \neq [3]_5$$

$$[0]_5^2 = [0]_5 \neq [3]_5$$
$$[1]_5^2 = [1]_5 \neq [3]_5$$
$$[2]_5^2 = [4]_5 \neq [3]_5$$
$$[3]_5^2 = [9]_5 = [4]_5 \neq [3]_5$$
$$[4]_5^2 = [16]_5 = [1]_5 \neq [3]_5$$

**No solution modulo 5!**

$$[0]_5^2 = [0]_5 \neq [3]_5$$
$$[1]_5^2 = [1]_5 \neq [3]_5$$
$$[2]_5^2 = [4]_5 \neq [3]_5$$
$$[3]_5^2 = [9]_5 = [4]_5 \neq [3]_5$$
$$[4]_5^2 = [16]_5 = [1]_5 \neq [3]_5$$

**No solution modulo 5!**

This means that there is no solution for the original equation!

- Consider a Diophantine Equation $F(X_1, \ldots, X_n) = 0$.

# The Local-Global Principle

- Consider a Diophantine Equation $F(X_1, \dots, X_n) = 0$.
- Assume that it has no solution.

- Consider a Diophantine Equation $F(X_1, \dots, X_n) = 0$.
- Assume that it has no solution.
- Can we always find an $N$ such that the equation has no solution **modulo** $N$?

- Consider a Diophantine Equation $F(X_1, \dots, X_n) = 0$.
- Assume that it has no solution.
- Can we always find an $N$ such that the equation has no solution **modulo** $N$?
- **Example:** $X^2 + 1 = 0$ has no integer solution, but it has a solution modulo 5:

$$[2]_5^2 + [1]_5 = [4]_5 + [1]_5 = [5]_0 = 0$$

# The Local-Global Principle

- Consider a Diophantine Equation $F(X_1, \dots, X_n) = 0$.
- Assume that it has no solution.
- Can we always find an $N$ such that the equation has no solution **modulo** $N$?
- **Example:** $X^2 + 1 = 0$ has no integer solution, but it has a solution modulo 5:

$$[2]_5^2 + [1]_5 = [4]_5 + [1]_5 = [5]_0 = 0$$

But one can check that it has no solution modulo 3.

- **In other words:** if an equation has solutions modulo $N$ for every $N$ **(*)**, does it actually have an integer solution?

# The Local-Global Principle

- **In other words:** if an equation has solutions modulo $N$ for every $N$ **(*)**, does it actually have an integer solution?
- This is called the **Local-Global Principle**, or **Hasse Principle** (after Helmut Hasse, 1898-1979).

- **In other words:** if an equation has solutions modulo $N$ for every $N$ **(*)**, does it actually have an integer solution?
- This is called the **Local-Global Principle**, or **Hasse Principle** (after Helmut Hasse, 1898-1979).
- **Remark:** The condition **(*)** is equivalent to the existence of a solution modulo every power of every prime number (**Chinese Remainder Theorem**).

- **In other words:** if an equation has solutions modulo $N$ for every $N$ **(*)**, does it actually have an integer solution?
- This is called the **Local-Global Principle**, or **Hasse Principle** (after Helmut Hasse, 1898-1979).
- **Remark:** The condition **(*)** is equivalent to the existence of a solution modulo every power of every prime number (**Chinese Remainder Theorem**).
- *Nitpicking note: together with* **(*)** *one should also assumes that the equation has solutions in the real numbers* $\mathbb{R}$.

- **Answer:**

- **Answer:** in general, **no**!

- **Answer:** in general, **no**!
- **Counterexample:** the equation

$$2Y^2 = X^4 - 17Z^4$$

has solutions modulo every $N$, but no integer solution.

- **Answer:** in general, **no**!
- **Counterexample:** the equation

$$2Y^2 = X^4 - 17Z^4$$

  has solutions modulo every $N$, but no integer solution.
- But in some cases this idea works...

**Theorem (Hasse-Minkowski)**

*Let* $F(X_1, \ldots, X_n)$ *be a* **homogeneous** *polynomial of* **degree 2**. *If* $F(X_1, \ldots, X_n) = 0$ *has a solution modulo* $N$ *for every* $N$ *and it has a solution in* $\mathbb{R}$, *then it has an integer solution.*

**Theorem (Hasse-Minkowski)**

*Let* $F(X_1, \ldots, X_n)$ *be a* **homogeneous** *polynomial of* **degree 2**. *If* $F(X_1, \ldots, X_n) = 0$ *has a solution modulo* $N$ *for every* $N$ *and it has a solution in* $\mathbb{R}$, *then it has an integer solution.*

That is, **quadratic forms satisfy the local-global principle**.

# Open Questions

# Open Questions

- What other classes of equations satisfy this principle?

# Open Questions

- What other classes of equations satisfy this principle?
  **Example:** cubic forms **do not** satisfy it.

# Open Questions

- What other classes of equations satisfy this principle?
  **Example:** cubic forms **do not** satisfy it.
- Study **cohomological obstructions** to the principle (Brauer-Manin, descent).

# Open Questions

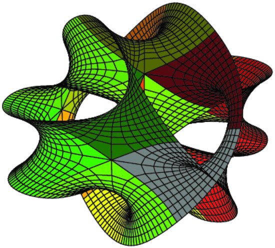
- What other classes of equations satisfy this principle?
  **Example:** cubic forms **do not** satisfy it.
- Study **cohomological obstructions** to the principle (Brauer-Manin, descent).
- Apply the principle to study other number-theoretic problems.

# Open Questions

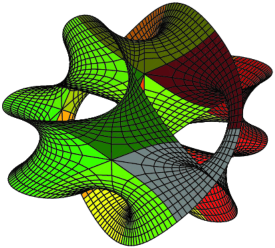
- What other classes of equations satisfy this principle?
  **Example:** cubic forms **do not** satisfy it.
- Study **cohomological obstructions** to the principle (Brauer-Manin, descent).
- Apply the principle to study other number-theoretic problems.
- In my master thesis, I explained the lack of primitive solutions to quadratic equations with a Brauer-Manin obstruction to the local-global principle applied to “strong approximation”.

# More pictures

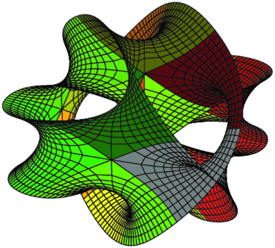
# More pictures

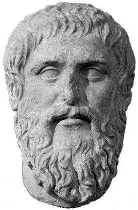


# More pictures

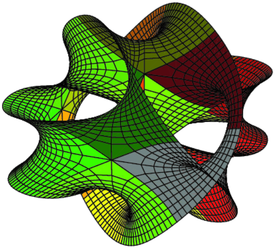


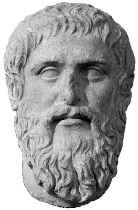
# More pictures



# More pictures



# Thank you for your attention!