Lecture 2

M. Klazar

October 14, 2025

In this lecture we present the resolution of the equation $x^m - y^2 = 1$, $m \in \mathbb{N}$ with $m \geq 3$, due to V. Lebesgue. We begin by introducing two tools for the proof: p-adic order of fractions and the ring of Gaussian integers on $\mathbb{Z}[i]$.

p-adic order

For a prime p and nonzero $\alpha \in \mathbb{Q}$ we define $\mathrm{ord}_p(\alpha)$ $(\in \mathbb{Z})$ as the unique integer k such that

$$\alpha = p^k \beta$$

where β is a fractions with neither the numerator nor the denominator divisible by p. We set $\mathrm{ord}_p(0) := +\infty$. We compute with $+\infty$ as follows: $+\infty + c = c + (+\infty) := +\infty$ for any $c \in \mathbb{R} \cup \{+\infty\}$, and $c < +\infty$ for any $c \in \mathbb{R}$. We prove the next lemma in the next lecture as Corollary 2.

Lemma 1. *If p is a prime and $\alpha_1, \alpha_2, \ldots, \alpha_n$ are $n \geq 2$ fractions such that the minimum*

$$\min(\{\mathrm{ord}_p(\alpha_i)\colon\ i = 1, 2, \ldots, n\})$$

is attained for a unique index i, then $\sum_{j=1}^n \alpha_j \neq 0$.

Gaussian integers

By *Gaussian integers* we mean the integral domain

$$\mathbb{Z}[i]_{\mathrm{do}} = \langle \mathbb{Z}[i], 0, 1, +, \cdot \rangle$$

in which

$$\mathbb{Z}[i] = \{a + bi\colon\ a, b \in \mathbb{Z}\} \ \ (\subset \mathbb{C})\,,$$

$0 = 0 + 0i$, $1 = 1 + 0i$, and $+$ and $\cdot$ are addition and multiplication of complex numbers.

The theorem of V. Lebesgue on $x^m - y^2 = 1$

Resolution of the equation $x^m - y^2 = 1$ for $m \in \mathbb{N}$ with $m \geq 2$ is easy for even $m = 2n$. Then

$$x^m - y^2 = (x^n - y)(x^n + y) = 1$$

and we see that the only solutions are $\pm 1, 0$. The case when $m \geq 3$ is odd is harder and was resolved by V. Lebesgue in [1].

Theorem 2 (V. Lebesgue, 1850). *Let $m \in \mathbb{N}$ with $m \geq 3$ and odd. Then*

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

has only the trivial solution $1, 0$.

Proof. Let $m \geq 3$ be an odd integer and $a, b \in \mathbb{Z}$ with $b \neq 0$ be such that $a^m - b^2 = 1$. We derive a contradiction. If b is odd then $a^m \equiv 2$ modulo 4, which is impossible. Thus b is even and nonzero, and a is odd. We consider the factorization

$$a^m = (1 + bi)(1 - bi)$$

in Gaussian integers.

It is easy to see that $1 + bi$ and $1 - bi$ are coprime in $\mathbb{Z}[i]_{\mathrm{dom}}$. Indeed, if $\alpha \in \mathbb{Z}[i]$ divides both $1 + bi$ and $1 - bi$, then $n = \alpha\overline{\alpha}$ $(\in \mathbb{N})$ divides, in $\mathbb{Z}$, the number $2 \cdot \overline{2} = 4$ and the odd number $(1 + bi)(1 - bi) = a^m$. Thus $n = 1$, α is a unit in $\mathbb{Z}[i]_{\mathrm{dom}}$, and $1 + bi$ and $1 - bi$ are coprime. Since $\mathbb{Z}[i]_{\mathrm{dom}}$ is UFD (see Theorem 9 in the next lecture), using item 2 of Proposition 4 in the next lecture we get $\alpha \in \mathbb{Z}[i]$, $\epsilon, \epsilon' \in \mathbb{Z}[i]^\times$ and $u, v \in \mathbb{Z}$ such that

$$1 + bi = \epsilon\alpha^m = (\epsilon'\alpha)^m = (u + vi)^m \text{ and } 1 - bi = \overline{\epsilon}(\overline{\alpha})^m = (\overline{\epsilon'\alpha})^m = (u - vi)^m$$

— every unit ± 1 and $\pm i$ in $\mathbb{Z}[i]^\times$ (see Proposition 6 in the next lecture) is an m-th power. Since m is odd, we have

$$2 = (u + vi)^m + (u - vi)^m = 2u \cdot \beta,\ \beta \in \mathbb{Z}[i]\,,$$

and deduce that $u = \pm 1$. We exclude the possibility $u = -1$. Since $(1 + v^2)^m = (u^2 + v^2)^m = 1 + b^2$ is odd, the number v is even. From

$$1 + bi = (u + vi)^m = \textstyle\sum_{j=0}^{m} \binom{m}{j} u^{m-j}(vi)^j \equiv u^m + mu^{m-1}vi \pmod 4$$

(congruence in $\mathbb{Z}[i]_{\mathrm{dom}}$) we deduce that $u^m \equiv 1$ modulo 4 (congruence in $\mathbb{Z}$), which excludes $u = -1$.

Thus $u + vi = 1 + vi$ with even and nonzero v (since $b \neq 0$). Comparing the real parts in $1 + bi = (1 + vi)^m$ we get an identity in $\mathbb{Z}$,

$$1 = \textstyle\sum_{j=0}^{(m-1)/2} (-1)^j \binom{m}{2j} v^{2j},\ \text{ or } \ -\binom{m}{2}v^2 + \sum_{j=2}^{(m-1)/2} (-1)^j \binom{m}{2j} v^{2j} = 0\,.$$

For $m = 3$ the last sum is empty (zero) and the equality is impossible as $v \neq 0$. For odd $m \geq 5$ we show that the equality does not hold by means of Lemma 1 and prime $p = 2$. We set $A = \binom{m}{2}v^2$ and $B_j = \binom{m}{2j} \cdot v^{2j}$ for $j = 2, 3, \ldots, \frac{m-1}{2}$, and show that $\mathrm{ord}_2(A) < \mathrm{ord}_2(B_j)$ for every j. Indeed,

$$B_j = A \cdot \tfrac{1}{j(2j-1)} \binom{m-2}{2j-2} v^{2j-2} =: A \cdot C_j$$

and $\mathrm{ord}_2(C_j) \geq 2j - 2 - \lfloor \log_2(j) \rfloor > 0$, so that by the additivity of $\mathrm{ord}_2(\cdot)$ (item 1 of Proposition 1 in the next lecture) we have $\mathrm{ord}_2(A) = \mathrm{ord}_2(B_j) - \mathrm{ord}_2(C_j) < \mathrm{ord}_2(B_j)$. We get a contradiction $\square$

The previous proof is taken from [2, Chapter 2].

References

[1] V. Lebesgue, Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$, *Nouv. Ann. Math.* **9** (1850), 178–181

[2] R. Schoof, *Catalan's Conjecture*, Springer-Verlag, London 2008