Lecture 5

Thm. (P. de Fermat, 17^{th} century) (1607–1665)

$\neg\exists\, x,y,z\in\mathbb{N}:$ $\boxed{x^4+y^4=z^2.}$

• P. de Fermat

<u>Proof.</u> Let $x,y,z\in\mathbb{N}$ be a sol. $\rightsquigarrow (x,y)=(x,z)=(y,z)=1 \rightsquigarrow$ x and y have different parity. Let $x\equiv 1\,(2),\ y\equiv 0\,(2)$. $\rightsquigarrow \underline{y^4=(z-x^2)(z+x^2).}$

$z,x\equiv 1\,(2),\ (z,x)=1 \rightsquigarrow (z-x^2,z+x^2)=2$

$\overset{FA}{\rightsquigarrow} \underbrace{z-x^2=2a^4}\ \&\ \underbrace{z+x^2=8b^4}$ for some $a,b\in\mathbb{N}$

or

s.t. $(a,b)=1$ and $a\equiv 1\,(2)$.

$\rightsquigarrow$ (subtracting) $x^2=4b^4-a^4$ – not possible modulo 4.

$\rightsquigarrow z-x^2=8b^4\ \&\ z+x^2=2a^4.$

$\rightsquigarrow \underbrace{x^2=a^4-4b^4}\ \&\ z=a^4+4b^4.$

$\Updownarrow$

$4b^4=(a^2-x)(a^2+x). \rightsquigarrow (a^2-x,a^2+x)=2.$

$\overset{FA}{\rightsquigarrow} a^2-x=2c^4\ \&\ a^2+x=2d^4$ for some $c,d\in\mathbb{N}$.

$\underset{\text{(adding)}}{\rightsquigarrow} \boxed{c^4+d^4=a^2.}$

But $a < z$ — infinite descend, i.e. ↯ (contradiction) ② ⊠

The Pell equation

• John Pell (1611–1685): "an English mathematician and political agent abroad."

— Euler's error (in attribution of the eq. to)

---

why

P. eq. is $\boxed{x^2 - dy^2 = 1}$ where $d \in \mathbb{N}$, $d \neq \square^2$.

~~Attt~~ $\boxed{\text{Example.}}$ $x^2 - 3y^2 = 1$

$x = \pm 1$, $y = 0$ ... trivi sol.; for all P. eq-s.

$x = 2$, $y = 1$ ... nontriv. sol.; also $x = \pm 2$, $y = \pm 1$

important $(2 + 1\cdot\sqrt{3})^2 = (2+\sqrt{3})^2 = 7 + 4\sqrt{3}$

gives another solution $x = 7$, $y = 4$. Indeed

$7^2 - 3\cdot 4^2 = (7 + \sqrt{3}\,4)(7 - \sqrt{3}\,4) =$

$= (2+\sqrt{3})^2 (2-\sqrt{3})^2 = (2^2 - 3\cdot 1^2)^2 =$ we know $1^2 = 1$.

Similarly, $(7 + 4\sqrt{3})(2+\sqrt{3}) = 26 + 15\sqrt{3}$ gives

Sol. $x = 26$, $y = 15$; $26^2 - 3\cdot 15^2 = 676 - 3\cdot 225 = 1$. ⊠

For a given P. equation $x^2-dy^2=1$ we define

$$A_d = A := \{a+b\sqrt{d} \mid a,b\in\mathbb{Z},\ a^2-db^2=1\} \subset \mathbb{R}$$

and

$$B_d = B := \{a+b\sqrt{d}\in A \mid a+b\sqrt{d}>0\} \subset \mathbb{R}.$$
$$\subset A$$

$\boxed{\text{Theorem}}$ We have the isomorphisms of infinite Abelian groups

$$\cancel{(A,1,\cdot)}\ (A,1,\cdot) \cong (\mathbb{Z},0,+) \oplus \mathbb{Z}_2$$

and $$(B,1,\cdot) \cong (\mathbb{Z},0,+)$$

where $\cdot$ is (usual) multiplication of real numbers and $+$ is usual addition of integers.

$\boxed{\text{Theorem (J. L. Lagrange, 1770)}}$ Every Pell eq. has a nontrivial solution, i.e.

$$\forall d\in\mathbb{N}, d\neq\square\ \exists a,b\in\mathbb{N}=\{1,2,\dots\}: a^2-db^2=1.$$

$\boxed{\text{Proof.}}$ An application of Dirichlet's thm.! We apply it on $\sqrt{d}\in\mathbb{R}\setminus\mathbb{Q}$.

$\xrightarrow[\text{Dir. thm.}]{}$ $\exists$ ∞ many $\frac{p}{q} \in \mathbb{Q}$ s.t.

$$0 < \frac{p}{q} < \sqrt{d} + 1 \Leftarrow \left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}.$$

$$|p^2 - dq^2| = q^2 \left|\sqrt{d} - \frac{p}{q}\right| \cdot \left|\sqrt{d} + \frac{p}{q}\right| <$$

$< q^2 \cdot \frac{1}{q^2}(\sqrt{d} + \sqrt{d} + 1) = 2\sqrt{d} + 1$ – constant independent of p and q. / Pigeon-hole, Schubfach Prinzip, Dirichlet's principle:

$\exists\, c \in \mathbb{Z},\ c \neq 0$ (and $|c| < 2\sqrt{d}+1$)

$\exists\, p_i, q_i \in \mathbb{N},\ i = 1,2$ s.t.

$$p_1^2 - dq_1^2 = p_2^2 - dq_2^2 = c$$

and $p_1 \equiv p_2 \pmod{|c|}$
$q_1 \equiv q_2$ (—"—), and $\frac{p_1}{q_1} \neq \frac{p_2}{q_2}$.

Let $a, b \in \mathbb{R}$ be given by

$$a + b\sqrt{d} = \frac{p_1 + q_1\sqrt{d}}{p_2 + q_2\sqrt{d}} = \frac{(p_1 + q_1\sqrt{d})(p_2 - q_2\sqrt{d})}{(p_2 + q_2\sqrt{d})(p_2 - q_2\sqrt{d})} =$$

$$= \frac{\text{—"—}}{c} =$$

(5)

$$= \underbrace{\frac{p_1p_2 - d q_1 q_2}{c}}_{\in \mathbb{Z}} + \underbrace{\frac{p_2 q_1 - p_1 q_2}{c}}_{\in \mathbb{Z}} \sqrt{d}.$$

$\in \mathbb{Z}$ and $\in \mathbb{Z}$, by the above congruences. Now

$$a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d})$$

$$= \frac{p_1 + q_1\sqrt{d}}{p_2 + q_2\sqrt{d}} \cdot \frac{p_1 - q_1\sqrt{d}}{p_2 - q_2\sqrt{d}}$$ because ...

$$= \frac{p_1^2 - d q_1^2}{p_2^2 - d q_2^2} = \frac{c}{c} = 1.$$ So $x = a$, $y = b$

is a sol. of the P. equation, but is it nontrivial? $b = 0 \Leftrightarrow p_2 q_1 - p_1 q_2 = 0$ (!) $\Leftrightarrow$

$\Leftrightarrow \frac{p_2}{q_2} = \frac{p_1}{q_2}$ which was forbidden. $\boxtimes$

- <u>Joseph-Louis Lagrange (1736 - 1813)</u>

With the help of the previous Lagrange's theorem we prove the thm. on groups.

~~Proof~~ To show that $A=(A,1,\cdot)$ is an Ab. group (6)
it suffices to show that $x,y\in A \Rightarrow xy\in A$ and $x\in A \Rightarrow \frac{1}{x}\in A$.

$\underbrace{a+b\sqrt{d}}_{\alpha}, \underbrace{c+e\sqrt{d}}_{\beta} \in A \rightsquigarrow \gamma=\alpha\beta=(ac+bed)+(ae+bc)\sqrt{d}$

$\bar\gamma=\bar\alpha\bar\beta= \text{—''—} - \text{—''—}$

$\bar\alpha=a-b\sqrt{d},\ \bar\beta=c-e\sqrt{d}$ $\qquad \gamma\bar\gamma=\alpha\beta\bar\alpha\bar\beta=\alpha\bar\alpha\beta\bar\beta$
$=(a^2-db^2)(c^2-de^2)=1\cdot 1=1.$

$\frac{1}{\alpha}=\frac{1}{a+b\sqrt{d}}=\frac{a-b\sqrt{d}}{\underbrace{a^2-b^2d}_{=1}}=$
$=a-b\sqrt{d}$

$\rightsquigarrow$ also $B=(B,1,\cdot)\subset A$ is an Ab. group.

$\varepsilon:=\min(\underbrace{\{\alpha\in A \mid \alpha>1\}}_{\neq\emptyset \text{ by Lagrange's thm.}})$ Why ε exists?

$\alpha=a+b\sqrt{d}>1$
$\alpha'=a'+b'\sqrt{d}>1$ $\rightsquigarrow a,a',b,b'\in\mathbb{N}$ and $\alpha<\alpha' \iff$
$\iff a<a' \iff b<b'.$

We claim that $B=\{\varepsilon^n \mid n\in\mathbb{Z}\}$, in fact $n\mapsto\varepsilon^n$ is a group isomorphism between $(\mathbb{Z},0,+)$ and $(B,1,\cdot)$.
Let $\alpha\in B$, $\alpha\neq 1$, wlog $\alpha>1$ (else take $\frac{1}{\alpha}$), and let $m\in\mathbb{N}_0$ be minimum with

$\varepsilon^m\leq\alpha<\varepsilon^{m+1}$. If $\leq$ is $<$, then $\varepsilon^m<\alpha<\varepsilon^{m+1}$,

So $1<\beta:=\alpha\varepsilon^{-m}<\varepsilon$, but $\beta\in B$ contradicts the choice of ε. So $(B,1,\cdot)\cong(\mathbb{Z},0,+)$. As for A, the $\oplus\mathbb{Z}_2$ is just the sign flipping $\pm\alpha$, $\alpha\in B$. $\boxtimes$

Generalized Pell eq. is $x^2 - dy^2 = m$ where $d \in \mathbb{N}, d \neq \square$ and $m \in \mathbb{Z}, m \neq 0$ are parameters. (For $m = 0$ exactly 1 sol. $x = y = 0$.)

$\boxed{\text{Theorem}}$ The ~~a~~ gen. Pell equation has either no solution $x, y \in \mathbb{Z}$ or infinitely many.

Proof. Exercise for you (might be an exam question...) $\boxtimes$

Importance of the Pell eq.:
- can be explicitly solved
- other DE reduce to it
- relation to the 10^{th} HP

Exercise for you: how to determine the generators ε by an algorithm.

Here is a table of ε: Wikipedia article on Pell eq.

$\boxed{\text{Thank you!}}$