Introduction to Number Theory
Úvod do teorie čísel | lecture ①

← my LNs.

Avi Wigderson: Mathematics & Computation
A Theory Revolutionizing Technology and Science
(Princeton Un. Press, 2019) | p. 1:

"Here is just one tip of the iceberg we'll explore in this book: How much time does it take to find the prime factors of a 1,000-digit integer?"

---

chapters of this course: ① Diophantine appr. ② Diophantine equations ③ Geometry of numbers ④ Prime numbers ⑤ Congruences ⑥ Partitions

---

① Diophantine approximation $\alpha \in \mathbb{R}$, $q \in \mathbb{N} := \{1, 2, \dots\}$. Then $\exists \frac{p}{q} \in \mathbb{Q}$ (rational #s) s.t. $|\alpha - \frac{p}{q}| \leq \frac{1}{q}$ (in fact, even $\leq \frac{1}{2q}$). Can we do better? Yes, we can, in Dirichlet's theorem.

Theorem (P. Dirichlet, 1842) ① $\forall \alpha \in \mathbb{R}\ \forall Q \in \mathbb{N}, Q \geq 2$ $\exists p, q \in \mathbb{Z}$ (the integers) s.t. $1 \leq q < Q$ and

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ}.$$

② $\forall \alpha \in \mathbb{R} \setminus \mathbb{Q}$, the inequality $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$ has infinitely many solutions $\frac{p}{q} \in \mathbb{Q}$.

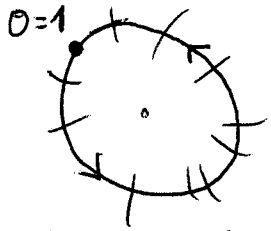
Proof.

① ⇒ ②: If $\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}$ are solutions, set $Q \in \mathbb{N}$ s.t. $\frac{1}{Q} < \min_{i=1\dots n} \left|\alpha - \frac{p_i}{q_i}\right|$ ≠ 0! (α is irr.) and take the fraction $\frac{p_{n+1}}{q_{n+1}} := \frac{p}{q}$ guaranteed by ①. Then $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ} < \frac{1}{q^2}$ and also $\dots \leq \frac{1}{Q}$, thus by the choice of Q we have that $\frac{p}{q} \neq \frac{p_i}{q_i}$, $i = 1\dots n$.

① Recall that for $\beta \in \mathbb{R}$, the fractional part of β, $\{\beta\} \in [0,1)$, is defined by $\beta = \lfloor \beta \rfloor + \{\beta\}$. One also writes that $\{\beta\} := \beta \bmod \mathbb{Z}$.

($\lfloor \beta \rfloor \in \mathbb{Z}$ integer part of β; $\{\beta\} \in [0,1)$)

Consider the Q numbers $\{0\alpha\}, \{1\alpha\}, \{2\alpha\}, \dots, \{(Q-1)\alpha\}$ in the interval $[0,1)$, which is useful to view as



Q (not nec. distinct) points on a circle with length 1. Some two neighbouring ones have distance $\leq \frac{1}{Q}$:
$\exists \ell, k \in \mathbb{N}_0 := \{0,1,2,\dots\}$ s.t. $0 \leq k < \ell < Q$ and $|\{\ell\alpha\} - \{k\alpha\}| \leq \frac{1}{Q}$. Thus $|\underbrace{(\ell-k)}_{=:q\in\mathbb{N}}\alpha - p| \leq \frac{1}{Q}$ for some $p \in \mathbb{Z}$, and $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ}$. ☒

Application: the **Fermat–Euler thm.** that if $p = 1+4n$ is a prime number, then $p = a^2+b^2$ for some $a,b \in \mathbb{N}$. For example, $97 = 9^2+4^2$. Also $2 = 1^2+1^2$, but always $p = 3+4n \neq \square+\square$ because $\square \equiv 0,1 \pmod 4$.

Lemma $\forall\, p = 1+4n$ (a prime) $\exists\, c \in \mathbb{N}$ s.t. $c^2 \equiv -1 \pmod p$.

Proof. Let's say that we know that $\mathbb{Z}_p$, the integers taken modulo p, form a field. We denote $\mathbb{Z}_p^\times := \mathbb{Z}_p \setminus \{0\}$. For $x \in \mathbb{Z}_p^\times$ let

$\Box x := \{x, -x, x^{-1}, -x^{-1}\}$. It is easy to see

that $x, y \in \mathbb{Z}_p^\times \Rightarrow \Pi_x = \Pi_y$ or $\Pi_x \cap \Pi_y = \emptyset$ and so (since $x \in \Pi_x$) $\{\Pi_x \mid x \in \mathbb{Z}_p^\times\}$ is a set partition of $\mathbb{Z}_p^\times$. For example $\mathbb{Z}_{13}^\times = \{1, 2, \dots, 12\}$ is partitioned in the sets $\{2, 11, 7, 6\}$, $\{3, 10, 9, 4\}$, $\{1, 12\}$ and $\{5, 8\}$. It follows that $|\Pi_x| = 4$ or 2. the latter

the # of elements

happens iff $x = x^{-1}$ or $x = -x^{-1}$ (since $p > 2$, always $x \neq -x$). $\Leftrightarrow x^2 = 1 \Leftrightarrow x = \pm 1$. But $\Leftrightarrow$ $\Rightarrow \Pi_x = \{1, -1\} = \{1, p-1\}$ $\Leftrightarrow x^2 \equiv -1$. Since $|\mathbb{Z}_p^\times| = 4n$ and the 2-element block $\{1, p-1\} = \Pi_x$ is present, there must be present also the other 2-element block and $x^2 \equiv -1$ has a solution in $\mathbb{Z}_p$. That is $c^2 \equiv -1 \pmod p$ for some $c \in \mathbb{N}$. ☒

Theorem (L. Euler, 1747) $\forall$ prime $p = 4n+1$ $\exists a, b \in \mathbb{N}$ s.t. $p = a^2 + b^2$.

Proof. For $p = 1 + 4n$ we take a $c \in \mathbb{N}$ by the Lemma, so $c^2 \equiv -1 \pmod p$.

Let $\alpha := \frac{c}{p}$, $Q := \underbrace{\lceil \sqrt{p} \rceil}_{\text{upper int. part}}$. By ① of Dirichlet's theorem we take $a, b \in \mathbb{Z}$ s.t. $1 \leq b < \sqrt{p}$ and $\left| \frac{c}{p} - \frac{a}{b} \right| < \frac{1}{b\sqrt{p}}$. $\rightsquigarrow 0 \leq |cb - pa| < \sqrt{p}$

$\rightsquigarrow 0 < \underbrace{(cb-pa)^2 + b^2}_{= (c^2+1)b^2 + p(\cdots) \equiv 0 \pmod p} < 2p. \rightsquigarrow (cb-pa)^2 + b^2 = p.$ ☒

Another two methods to prove Dirichlet's theorem are based on continued fractions (of real #s) and on the Farey fractions. We briefly define both.

Let us expand $\sqrt{2} = 1.414\ldots$ in continued fraction [Větězový zlomek]:

$\sqrt{2} = \lfloor \sqrt{2} \rfloor + \{\sqrt{2}\} =: \underbrace{1}_{a_0} + \alpha_0 = 1 + \frac{1}{1/\alpha_0} =$

$= 1 + \frac{1}{\underbrace{\lfloor 1/\alpha_0 \rfloor}_{=a_1} + \underbrace{\{1/\alpha_0\}}_{=\alpha_1}}$. $\frac{1}{\alpha_0} = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1 =$

$= a_1 + \alpha_1 := 2 + \alpha_1$. So $\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{1/\alpha_1}}$.

We continue in this way: $\frac{1}{a_1} = \frac{1}{\sqrt{2}+1-2} = \frac{1}{\sqrt{2}-1} =$
$= \sqrt{2}+1 = [1/a_1] + \{1/a_1\} =: a_2 + a_2 = 2 + a_2$. Thus
$a_n = 2$ for $\forall n$ and

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}}.$$

We write $\sqrt{2} = [1,2,2,2,2,\ldots]$ - this is the cont. fraction for $\sqrt{2}$. For general $\alpha \in \mathbb{R}$ we proceed in a similar way.

The Farey fractions $\mathcal{F}_n$, for $n \in \mathbb{N}$, is the ordered list of all fractions $\frac{p}{q} \in [0,1]$ s.t. $(p,q) = 1$ and $1 \leq q \leq n$. For example,

p and q are coprime
i.e. $\frac{p}{q}$ is in lowest terms

$$\mathcal{F}_5 = \left\{ \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1} \right\}.$$

In the next lecture I will show you, in the case of cont. fractions without details, how to prove Dirichlet's theorem by these fractions.