Analytic and Combinatorial Number Theory (L1) 1

Analytic – continuous, analytic functions, derivatives, integrals, methods of mathematical analysis

Combinatorial – Applied to combinatorial, discrete objects, to the integers $\mathbb{Z}$.

Let us give some examples. $\mathbb{N} = \{1, 2, \dots\}$ – the natural numbers. We can partition it in (infinite) arithmetic progressions (AP) as $\mathbb{N} = \{1, 3, 5, 7, \dots\} \dot\cup \{2, 4, 6, 8, \dots\} = (1 + \underline{2}\mathbb{N}_0) \dot\cup (2 + \underline{2}\mathbb{N}_0)$ – partition into odd and even numbers [here $\mathbb{N}_0 := \mathbb{N} \cup \{0\} = \{0, 1, 2, \dots\}$], or also

$\mathbb{N} = (1 + \underline{4}\mathbb{N}_0) \dot\cup (3 + \underline{4}\mathbb{N}_0) \dot\cup (2 + \underline{2}\mathbb{N}_0)$ and other similar examples. Is there a partition of $\mathbb{N}$ into finitely many APs with distinct common differences? (Above underlined)

Proposition (on partitions of $\mathbb{N}$ into APs) There is no partition

$$(*) \quad \mathbb{N} = \dot{\bigcup_{i=1}^{k}} (a_i + d_i \mathbb{N}_0)$$

$k \geq 2$, $k \in \mathbb{N}$, $d_i \in \mathbb{N}$, such that $a_i \in \mathbb{N}$ and $1 \leq d_1 \leq d_2 \leq \dots \leq d_{k-1} < d_k$, i.e. with unique largest difference.

Proof Any partition $(*)$ translates in the identity

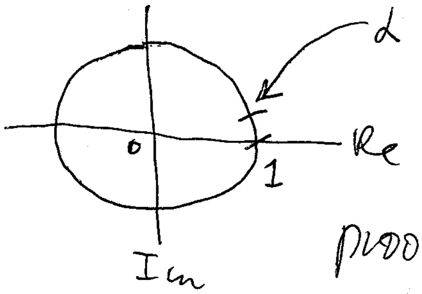
$$\sum_{n=1}^{\infty} z^n = \sum_{n=0}^{\infty} z^{a_1 + d_1 n} + \dots + \sum_{n=0}^{\infty} z^{a_k + d_k n}$$

which is the same as

$$\boxed{\frac{z}{1-z} = \frac{z^{a_1}}{1 - z^{d_1}} + \frac{z^{a_2}}{1 - z^{d_2}} + \dots + \frac{z^{a_k}}{1 - z^{d_k}}},$$

by summing the geometric series: $\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$, for $|z| < 1$ ($z \in \mathbb{R}, \mathbb{C}$)

We understand $\boxed{\dots}$ as an identity for functions defined on the unit complex disc $D = \{z \in \mathbb{C} \mid |z| < 1\}$. But considering the number $\alpha = e^{2\pi i/a_q}$ and substituting for z the numbers $(z_n) = (z_1, z_2, \dots) \subset D$ with $\lim_{n\to\infty} z_n = \alpha$, we see that the identity $\boxed{\cdots}$ is impossible: the last term goes in $|\cdot|$ to $+\infty$ but all other terms go to finite limits $\frac{z\alpha}{1-\alpha}, \frac{\alpha^{a_1}}{1-\alpha^{a_1}}, \dots, \frac{\alpha^{a_{q-1}}}{1-\alpha^{a_{q-1}}}$ $(\alpha, \alpha^{a_1}, \dots, \alpha^{a_{q-1}} \neq 1)$. $\boxtimes$



α is an a_q-th root of unity.

$\boxed{\text{Exercise}}$ Show that in the previous proof analysis can be in fact completely avoided by casting it in purely algebraic terms in the ring $\mathbb{C}[[z]]$ of formal power series.

Nice book: Donald J. Newman (1930, Brooklyn, NY – 2007, Philadelphia, Penns.), Analytic Number theory, Springer-Verlag, New York (1998). – wonderful book, but … of 76 pages! – in 1980 he found a short proof of the PNT (the prime number theorem (*), $\pi(x) := \#\{p \mid p \le x\} \sim \frac{x}{\log x}$ as $x \to +\infty$).

<u>Integer partitions</u> (above we considered <u>set</u> partitions of $\mathbb{N}$) An (i.) partition of $n \in \mathbb{N}$ is an expression $n = a_1 + a_2 + \dots + a_k$ where $a_i \in \mathbb{N}$ and the order of summands does not matter. Formally:

$\lambda = (a_1, a_2, \dots, a_k)$ where $a_i \in \mathbb{N}$, $a_1 \geq a_2 \geq \dots \geq a_k$ and $n = a_1 + a_2 + \dots + a_k$. We write $\lambda \vdash n$. Another format for partitions is $\lambda = 1^{m_1} 2^{m_2} \dots n^{m_n}$ where $m_i \in \mathbb{N}_0$ are the multiplicities of the parts $1, 2, \dots, n$ and $n = m_1 \cdot 1 + m_2 \cdot 2 + \dots + m_n \cdot n$. Partition function (to mathematician, not to physicist) is $p(n) := \#\{\text{partitions of } n\}$. For example, $p(0) := 1$ (definition), $p(1) = 1$, $p(2) = 2$ $(2, 1^2)$, $p(3) = 3$ $(3, 21, 1^3)$, $p(4) = 5$ $(4, 31, 2^2, 21^2, 1^4)$, $p(5) = 7$ $(5, 41, 32, 31^2, 2^2 1, 21^3, 1^5)$.

Besides the PNT another famous result of Analytic NT is the asymptotics for $p(n)$,

$$(*) \quad p(n) = (1 + o(1)) \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2/3} \cdot \sqrt{n}}, \quad n \to \infty,$$

found in 1918 by G. H. Hardy and S. Ramanujan. DJN gave ~~#~~ a short (analytic) proof for it in 1962 (Michigan J. Math.)

$\boxed{\text{Theorem (L. Euler, 18th century)}}$

$\forall n \in \mathbb{N}$ has as many partitions with distinct parts (all above $m_i \in \{0, 1\}$) as partitions with odd parts (all above a_i are odd numbers). Example for $n=5$:

$5, 41, 32, 31^2, 2^2 1, 21^3, 1^5$

DPs — OPs — both are three.

Proof. Let $p_d(n) = \#\{$partitions of n

with distinct parts and $p_o(n) = \#\{$the p-s of n with odd parts$\}$. It is easy to see (well, ~~not really~~) that

$$\sum_{n=0}^{\infty} p_d(n) z^n = 1+z+\cdots = \prod_{k=1}^{\infty}(1+z^k)$$ and

$$\sum_{n=0}^{\infty} p_o(n) z^n = 1+z+\cdots \prod_{k=1}^{\infty}\frac{1}{1-z^{2k-1}}$$ for $z \in \mathbb{C}$ with $|z|<1$.

But $$\prod_{k=1}^{\infty} 1+z^k = \prod_{k=1}^{\infty}\frac{1-z^{2k}}{1-z^k} = \frac{\cancel{(1-z^2)}\cancel{(1-z^4)}\cancel{(1-z^6)}\cancel{(1-z^8)}\cdots}{(1-z)\cancel{(1-z^2)}(1-z^3)\cancel{(1-z^4)}\cdots}$$

$$= \frac{1}{(1-z)(1-z^3)(1-z^5)\cdots} = \prod_{k=1}^{\infty}\frac{1}{1-z^{2k-1}},$$ thus indeed

$p_d(n) = p_o(n)$ for $\forall n \in \mathbb{N}$. $\boxtimes$

Exercise Again cast this proof formally, in the ring $\mathbb{C}[[z]]$ of formal power series.

In this course I will prove both results (*), the PNT and the asymptotics of $p(n)$.

The FTA - Fundamental Theorem of Algebra - Analysis (topology) proves the basic fact that

$$\boxed{\text{if } a_0, a_1, \ldots, a_n \in \mathbb{C},\ n \in \mathbb{N},\ a_n \neq 0 \text{ then } \exists \alpha \in \mathbb{C} \text{ s.t. } a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.}$$

That is, every non-constant $p \in \mathbb{C}[z]$ has a root, a number $\alpha \in \mathbb{C}$ with $p(\alpha) = 0$. We proceed in 2 steps.

Step 1 If every polynomial $z^k + a$, $k \in \mathbb{N}$, $a \in \mathbb{C}$, has a root, then the FTA holds.

Step 2 $\forall k \in \mathbb{N}\ \forall \alpha \in \mathbb{C}\ \exists \beta \in \mathbb{C}$: $\beta^k = \alpha$. That is, the field $\mathbb{C}$ is closed to taking any root.

$$S1 + S2 \Rightarrow \text{the FTA.}$$

Proof of Step 1. Let $p \in \mathbb{C}[z]$, $p(z) = a_0 + a_1 z + \dots + a_n z^n$ with $a_i \in \mathbb{C}$, $a_n \neq 0$, $n \in \mathbb{N}$, be a non-constant complex polynomial. First we show that the real-valued function $|p(z)| : \mathbb{C} \to [0, +\infty)$ attains a minimum value — not obvious, is continuous but is not compact. But (exercise for you) $\lim_{|z| \to +\infty} |p(z)| = +\infty$, so there is a $c > 0$ s.t. $|z| > c \Rightarrow |p(z)| > |p(0)|$. Thus, since the closed disc $\overline{D}_c = \{ z \in \mathbb{C} \mid |z| \leq c \}$ is compact and $0 \in \overline{D}_c$, we see that $|p(z)|$ attains on $\mathbb{C}$ a minimum value, at some $\alpha \in \overline{D}_c$. Using the substitution $z := z - \alpha$, we can assume wlog that $\alpha = 0$ (exercise). Thus **L2**