28.09.2018
Arithmetic
Seminar-3
H. Göral

Theorem (van der Waerden) (1927)

Suppose that the positive integers are colored with finitely many colors. Then there are arbitrarily long arithmetic progression in positive integers all have the same color.

In other words,

If $f: \mathbb{Z}^+ \longrightarrow S$, S is finite, then for any $k \geq 3$ we can find a, b $(b \geq 1)$ so that

$$f(a) = f(a+b) = f(a+2b) = \cdots = f(a+kb)$$

Example: $A = \{n^3 : n \geq 1\}$ does not contain 3-term arithmetic progression.

Definition: (p-adic valuation)

Let n be a nonzero positive integer and p be an arbitrary prime.

If $n = p^m k$ and $p \nmid k$, then $V_p(n) := m$.

Properties of p-adic valuation:

- $V_p(0) = \infty$
- $V_p(a.b) = V_p(a) + V_p(b)$
- $V_p(a+b) \geq \min\{V_p(a), V_p(b)\}$

  If $V_p(a) \neq V_p(b)$, then $V_p(a+b) = \min\{V_p(a), V_p(b)\}$

Theorem: There are infinitely many primes.

proof: (Alpoge, 2017)

Suppose that there are finitely many primes.

If $\mathcal{P}$ is the finite set of primes, then

$$f: \mathbb{Z}^+ \longrightarrow \left(\{0,1\} \times \{0,1\}\right)^{\mathcal{P}}$$

$$f(n) = \left(\begin{array}{l} 1 \text{ if } p \mid n \\ 0 \text{ if } p \nmid n \end{array}, V_p(n) \pmod 2 \right)_p$$

is a coloring. By van der Waerden's theorem there are arbitrarily long A.P.

Let r be larger than the square of any prime.

Choose a monochromatic A.P:

$$a,\ a+d,\ a+2d,\ \ldots,\ a+rd. \qquad (d \geq 1)$$

Let p be a prime that divides. Then p must divide all terms in A.P which implies $p \mid d$.

We claim that $V_p(a) < V_p(d)$. Suppose that it does not hold. We have two cases.

Case 1: $V_p(a) > V_p(d)$.

$$V_p(d) = V_p(a+d) \leq V_p(a) - 2.$$

$$V_p(a+pd) = V_p(a+d) + 1 \not\equiv V_p(a+d) \pmod 2,$$

a contradiction.

Case 2: $V_p(a) = V_p(d)$.

Suppose that $a = p^m a_1$ and $d = p^m d_1$. Then $p \nmid a_1 \cdot d_1$.

$\varphi: \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z}$ is 1-1 and onto.

$\bar{k} \longmapsto \overline{a_1 + kd_1}$

That is, for $1 \leq k \leq p^2 < r$ $a_1 + kd_1 \equiv p \pmod{p^2}$ and $V_p(a_1 + kd_1) = 1$.

$V_p(a + kd) = V_p(a) + 1 \Rightarrow V_p(a) \neq V_p(a+kd) \pmod 2$, a contradiction.

Hence, we have the claim.

$V_p(a) < V(d)$ implies that $V_p(a) = V_p(a+d)$ which means that a and $a+d$ have the same factorization, a contradiction.

Thus, there are infimitely many primes. ∎

Fermat's theorem: There are no 4-term AP in squares. In other words, n^2, n^2+d, n^2+2d, n^2+3d can not be all squares.

- 3-term AP in squares: 1, 25, 49.

Theorem: There are infinitely many primes.

proof: (Granville)

Suppose that there are finitely many primes, $p_1, \dots, p_k$. All positive integers are of the form:

$A = p_1^{e_1} \cdots p_k^{e_k}$, $e_i = 2q_i + r_i$, where $r_i \in \{0, 1\}$.

Then, $R = p_1^{r_1} \cdots p_k^{r_k}$ is the square-free part.

$f(A) = (r_1, \dots, r_k)$ is a coloring. That is, the positive integers whose square-free part is same are colored with game color. By van der Warden's theorem, $\underbrace{A, A+D, A+2D, A+3D}_{4\text{-term AP}}$ have the game color. $R \mid A$, $R \mid A+D$, $R \mid A+2D$, $R \mid A+3D$ $\Rightarrow R \mid D$. Let $a = \frac{A}{R}$, $d = \frac{D}{R}$. Then,

$a, a+d, a+2d, a+3d$ is a 4-term AP in squares which contraclicts with Fermat's theorem. ■

Szemerédi's theorem: (1975)

Fix $\delta > 0$ in $\mathbb{R}^+$, $k \geq 3$ in $\mathbb{Z}^+$. If N is large enough then any subset A of $\{1, 2, \ldots, N\}$ with at least δN elements must contain a k-term AP.

Green - Tao theorem: (2004)

The set of primes contains arbitrarily long AP.

Future Topics:

- $\pi(x) = \#\{p \leq x : p \text{ is prime}\}$

  $\lim_{x \to \infty} \frac{\pi(x)}{x} = 0$ (This is a probability of choosing a prime in the set of positive integers)

- Prime Number Theorem:

$$\pi(x) \sim \frac{x}{\log x}$$

- $Li(x) = \int_2^x \frac{dt}{\log t}$, $\pi(x) = Li(x) + O_\varepsilon\left(x^{\frac{1}{2}+\varepsilon}\right) \Leftrightarrow$ Riemann Hypothesis

- Dirichlet's theorem: $(a, q) = 1 \Rightarrow a, a+q, a+2q, \ldots$ contains infinitely many primes.

- Erdös - Turan Conjecture: Let $A \subseteq \{1, 2, \ldots\}$.

$$\sum_{a \in A} \frac{1}{a} = \infty \Rightarrow A \text{ contains arbitrarily long AP.}$$