Lec 8/28

Monday, August 28, 2017 14:17

question: If f, g are injective and $f \sim g$, under what conditions is $f^{-1} \sim g^{-1}$

question: If $A \subseteq \mathbb{N}$, $A = \{a_1, \dots, a_n, \dots\}$ and $a_n \sim \phi(n)$ where $|\phi(n)| \leq P(n)$ (P is a polynomial)

Is it true that $AA^{-1} = \{\frac{a_i}{a_j} \mid a_i, a_j \in A\}$ dense in $\mathbb{R}^+$?

Sárközy's Theorem:

Let $A \subseteq \mathbb{N}$, assume that $\bar{d}(A) = \limsup \frac{|A \cap \{1, \dots, n\}|}{n} > 0$.

then $(A - A) \cap \{n^2 \mid n \in \mathbb{N}\} \neq \emptyset$

(i.e. $\exists\, x, y \in A$, $n \in \mathbb{N}$ s.t. $x - y = n^2$) (i.e. $\exists n \in \mathbb{N}$ s.t. $A \cap (A - n^2) \neq \emptyset$)

exercise: show this is equiv

why n^2 can't be n^2+1

$A = \{3n+2, n \in \mathbb{N}\}$. $(3n_1+2) - (3n_2+2) = 3(n_1 + n_2) = n^2+1$

but $3m \neq n^2+1$ since if $n \bmod 3 = 0$ obvi

$= 1$

$= 2$ something about residues.

What is n&s condition for a polynomial to replace n^2?

Exercise Theorem if $n_1 < n_2 < \dots < \dots$ is such that

$\frac{n_{i+1}}{n_i} > \lambda > 1$ $\forall i > 1$ (or eventually (bonus bonus)) then $\{n_i\}_1^\infty$ is "not good" for Sárközy thm.

Counterexample for primes: $A = 4\mathbb{N}$.

but $p \pm 1$ works (Dirichlet's theorem) (exercise) ex Prove that $P-17$ is not good for Sárközy (use Dirichlet's theorem)

The following sets are "good for Sárközy":

$\mathbb{P}+1$, $\mathbb{P}-1$, $\{n^2-1, n \in \mathbb{N}, n \geq 2\}$

$\{(p-1)^2, p \in \mathbb{P}\}$, $\{\lfloor p^c \rfloor, p \in \mathbb{P}, c>0, c \notin \mathbb{N}\}$.

N&S condition for polynomials in Sárközy thm:

Theorem Let $f(n)$ be a polynomial, $\deg(f) \geq 1$, then

$B = \{|f(n)|, n \in \mathbb{Z}\}$ is "good for Sárközy" iff $\forall a \in \mathbb{N}$ $B \cap a\mathbb{N} \neq \emptyset$

(we call such f "divisible")

Exercise If f not divisible, f not good

Hint: Consider A an infinite progression.

Equiv. form of Sárközy: (prove this equivalent)

- $\forall A \subset \mathbb{N}$ w/ $\bar{d}(A) > 0$, $\exists n \in \mathbb{N}$ s.t. $\bar{d}(A \cap (A - n^2)) > 0$ ($x \in A - n^2$ iff $x + n^2 \in A$)

$\bar{d}(A_1), \bar{d}(A_2) > 0$. $(A_1 - A_1) \cap (A_2 - A_2) \ni n^2$

Challenge why is $e \notin \mathbb{Q}$. why is $e^2 \notin \mathbb{Q}$. (modify Fourier proof)

Theorem $e^x \notin \mathbb{Q}$ $\forall x \in \mathbb{Q} \setminus \{0\}$

Finite field: a field of finite cardinality obviously.

Ex: Let $\mathbb{Z} = \bigcup_{i=0}^{4} (5\mathbb{Z}+i)$. denote $5\mathbb{Z}+i = C_i$ for $i = 0,1,2,3,4$.

$C_i + C_j = C_{(i+j) \bmod 5}$

$C_i \cdot C_j = C_{(ij) \bmod 5}$

These C_i are a field (exercise)

This is a field for prime 5. (exercise)

Theorem $\forall p \in \mathbb{P}$ and every $n \in \mathbb{N}$, there exists a unique up to isomorphism finite field having p^n elements

$\Gamma = \{a+bi \ , \ a,b \in \mathbb{Z}\} \approx \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \ a,b \in \mathbb{Z} \right\}$

(exercise) show this isomorphism

The only invertible elements of Γ are $\pm 1, \pm i$

$\Gamma = \mathbb{Z}[i]$, also consider $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[-\sqrt{2}]$.

ex: give an example of a number theoretical ring w/ infinitely many units

$\mathbb{Z}_5$ (does it have quadratic irrationalities?) $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, $4^2 = 1$. so $\sqrt{2}$, $\sqrt{3}$ are not in $\mathbb{Z}_5$.

So now $\{a + b\sqrt{2}, \ a,b \in \mathbb{Z}_5\} \approx \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}, \ a,b \in \mathbb{Z}_5 \right\}$ Exercise. → or nah (show this is a field w/ 25 elements)

$\{a + b\sqrt{3}, \ a,b \in \mathbb{Z}_5\}$

$(a+b\sqrt{2})(c+d\sqrt{2}) = ac + 2bd + (ad+bc)\sqrt{2}$

$\det \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} = a^2 - 2b^2 = 0 \Rightarrow (ab^{-1})^2 = 2$ so if $b \neq 0$ then nothing, so $b = a = 0$.

$\|$

$\left\{ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix}, \ a,b \in \mathbb{Z}_5 \right\}$ $\det(\ ) = a^2 - 3b^2 = 0$ iff $a = b = 0$

$\cong$

$\left\{ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix}, a,b \in \mathbb{Z}_5 \right\}$ det ( ) $= a^2 - 3b^2 = 0$ iff $a, b = 0$.

Exercise prove these 2 are isomorphic.

Exercise: for any $p \in \mathbb{P}$, $\exists$ finite field w/ p^2 elements

Hint: squares of a finite field don't cover all of it.