1 Критические пары в $\mathbb{Z}_p$

Определение 1. Если $A, B \subset \mathbb{Z}_p$ таковы, что $A + B \neq \mathbb{Z}_p$, $|A + B| = |A| + |B| - 1$, то такая пара множеств называется критической.

Теорема 1. *Если A, B — критическая пара, то выполнено одно из следующих условий:*

- $\min\{|A|, |B|\} = 1$
- $|A + B| = p - 1, 2 \leqslant |A| \leqslant p - 1, B = \overline{c - A}, \{c\} = \mathbb{Z}_p \setminus (A + B)$
- *A, B — арифметические прогрессии с одинаковой разностью*

Доказательство.

Лемма. *Если (A, B) — критическая и $|A + B| = |A| + |B| - 1 < p - 1$, A — арифметическая прогрессия, то B — прогрессия с той же разностью.*

Лемма. *Если $\min\{|A|, |B|\} = 2$, (A, B) — критическая, то A, B — арифметические прогрессии с одинаковой разностью.*

Лемма. *Если $\min\{|A|, |B|\} \geqslant 2$, (A, B) — критическая, $|A + B| = |A| + |B| - 1 < p - 1$, тогда $(\overline{A + B}, -A)$ — критическая.*

Полагаем, что $\min\{|A|, |B|\} \geqslant 2$, $|A + B| = |A| + |B| - 1 < p - 1$.

Лемма. *В указанном предположении, если известно, что $A + B$ — арифметическая прогрессия, то A, B — арифметические прогрессии с одинаковой разностью.*

Доказательство. $A + B$ — арифметическая прогрессия, значит $\overline{A + B}$ тоже прогрессия с такой же разностью. Тогда по лемме $(\overline{A + B}, -A)$ — критическая и так как $\overline{A + B}$ — арифметическая прогрессия, то по другой лемме $-A$ и A — прогрессии с той же разностью (с точностью до знака). Еще одно применение леммы даёт нам то, что A и B — арифметические прогрессии с одинаковой разностью. □

Лемма. *Если (A, B) — критическая, $0 \in B, |A| = k \geqslant 2, |B| = l \geqslant 3, |A + B| = |A| + |B| - 1 < p - 1$. Тогда найдётся $e \in A$, такое что $(A_{(e)}, B_{(e)})$ — критическая пара, такая что $A_{(e)} + B_{(e)} = A + B$ и $2 \leqslant |B_{(e)}| < |B|$.*

Доказательство. Возьмём произвольное $e \in A$. $A_{(e)} + B_{(e)} \subset A + B$. По тоереме Коши-Давенпорта $|A_{(e)}| + |B_{(e)}| - 1 \leqslant |A_{(e)} + B_{(e)}| \leqslant |A + B| = |A| + |B| - 1 = |A_{(e)}| + |B_{(e)}| - 1 \Rightarrow |A_{(e)} + B_{(e)}| = |A + B| \Rightarrow A_{(e)} + B_{(e)} = A + B$.

$X = \{e \in A : |B_{(e)}| < |B|\}$. Покажем, что $|X| \geqslant 2$. Если $e \in X$, то $B \cap (A - e) \subsetneq B$. Рассмотрим $Y = A \setminus X$. Для $e \in Y$ выполнено $B \subset A - e$. Пусть $Y \neq \varnothing$, иначе все тривиально. Пусть $Y \neq \varnothing$, тогда $\forall e \in A : B + e \subset A$. По теореме Коши-Давенпорта $|Y| + |B| - 1 \leqslant |Y + B| \leqslant |A| = k$. $|Y| + l - 1 = k - |X| + l - 1 \leqslant k \Rightarrow |X| \geqslant l - 1 \geqslant 2$.

Пусть $\forall e \in X, B_{(e)} = 0$. $B' = B \setminus \{0\}$, тогда $\forall e \in X \to B' \cap (A - e) = \varnothing \Leftrightarrow$ $\forall e \in X \to (B' + e) \cap A = \varnothing$. Тогда $(B' + X) \cap A = \varnothing (X + B') \subset (A + B) \setminus A$.
□

□