Теорема Эрдёша-Гинзбурга-Зива.

1. а) Докажите, что среди n целых чисел найдется несколько, сумма которых делится на n.

б) Докажите, что существуют такие $2n-2$ целых числа, что среди них не найдется ровно n чисел, сумма которых делится на n.

Теорема (Эрдёш, Гинзбург, Зив, 1961). Среди любых $2n-1$ целого числа найдется ровно n чисел, сумма которых делится на n.

2. Докажите, что теорема ЭГЗ верна для $n=a$ и для $n=b$, то она верна и для $n=ab$.

Итак, достаточно доказать теорему только для простого числа p.

Доказательство I (идейное, суммирование через МТФ). Чем отличается число, кратное p, от числа, не кратного p? Тем, что a^{p-1} сравнимо с 0 или с 1. То есть нужно привести к противоречию предположение $(a_{i_1}+\dots+a_{i_p})^{p-1}\equiv 1$ для всех $\{i_1,\dots,i_p\}\subset\{1,2,\dots,2p-1\}$.

Опр. Если $A,B\subseteq M$, то $A+B=\{a+b|a\in A, b\in B\}$, $2A=\{2a|a\in A\}$ и т.п. Здесь M – множество, на котором определена операция «+», «·2» и т.п.

Доказательство II (мощное, через теорему Коши-Дэвенпорта). Выведите из нижеследующей теоремы ее аналог для суммы нескольких подмножеств, а из этого – теорему ЭГЗ.

Теорема (Коши (1813), Дэвенпорт(1935)). Если p – простое, и $A,B\subseteq\mathbb{Z}_p$ – непустые подмножества, то $|A+B|\geqslant\min\{p,|A|+|B|-1\}$.

Пример. По модулю простого p уравнение $x^2+y^2\equiv k$ имеет решение для каждого целого k.

Схема доказательства. 1) Случай $|A|+|B|>p$ достаточно прост.

2) Пусть выполнено $|A+B|<|A|+|B|-1$. Идея состоит в том, что заменять «контрпримерную» пару множеств (A,B) на пару (A',B'), с уменьшением чего-нибудь (чтобы вести индукцию по этому чему-нибудь).

3) Заведем операцию *сдвига (по кругу)* множества, то есть замены A на $A+\{c\}$. Докажите, что если $|A|\geqslant 2$, то можно сдвинуть A так, чтобы A и B пересекались, но при этом $A\not\subset B$ (трюк Коши).

4) $(A,B)\to(A\cap B, A\cup B)$.

Доказательство III (поправки и подкрутки). Рассмотрим произвольную сумму $a_1+\dots+a_p\equiv r \pmod p$, и кажому числу a_i сопоставим в пару отсутствующее в этой сумме число b_i. Теперь будем подправлять сумму, заменяя некоторые a_i на b_i. То есть прибавлять к обеим частям по $(b_{i_1}-a_{i_1})+\dots+(b_{i_s}-a_{i_s})$. Такими поправками мы хотим превратить r в 0, но s уже не фиксировано!

3. Есть $p-1$ ненулевое число по модулю p. Тогда можно сложить несколько из них так, чтобы получить любое ненулевое по модулю p число.

Доказательство IV (безыдейная демонстрация силы правильной индукции). Пусть $k\leqslant p$. Допустим, что среди целых чисел $x_1,\dots,x_{2k-1}$ нет $k+1$ числа, сравнимых по модулю p. Тогда из этих чисел можно составить такие k сумм из k слагаемых каждая, что все суммы будут различными по модулю p.

Для самостоятельного решения

4. Докажите, что уравнение $ax^3+by^3+cz^3\equiv d \pmod p$ при $a,b,c\not\equiv 0 \pmod p$ имеет решение.

5. Абелева группа A *не имеет кручения*, если из условия $na=a+a+\dots+a=0$ следует, что $a=0$ (например, $\mathbb{Z}_3$ или группа поворотов относительно точки имеют кручение, а $\mathbb{Z}$ – нет. В частности, A бесконечна). Докажите, что если группа A не имеет кручения, то для любых конечных $B,C\subseteq A$ выполнено $|B+C|\geqslant|B|+|C|-1$.

6. Имеется n чисел, взаимно простых с n. Докажите, что любой остаток по модулю n равен сумме некоторых из этих чисел.