Множества Сидона

Задачу представляют: С.Берлов, К.Кохась, К.Куюмжиян

Условия задач

1 *Множества Сидона в* $\mathbb{N}$

1.1. Докажите, что если набор $\{a_1, a_2, \dots\}$ из n различных чисел имеет N различных сумм вида $a_i + a_j$, $i \leqslant j$, то $N \in [2n-1, C_{n+1}^2]$, причем все эти значения реализуются.

1.2. Имеется 20 различных натуральных чисел, множество попарных сумм которых (включая суммы каждого числа с самим собой) содержит ровно 201 элемент. Из какого наименьшего количества элементов может состоять множество (положительных) попарных разностей этих чисел?

1.3. Какое наибольшее количество чисел можно выбрать из множества $\{1, 2, \dots, 9\}$ так, чтобы все их попарные суммы $a_i + a_j$, $i < j$, были различны?

1.4. Существует ли такое конечное множество натуральных чисел, что все попарные суммы $a_i + a_j$, $i \leqslant j$, его элементов различны и при этом среди этих сумм имеется 100 последовательных натуральных чисел?

1.5. Существует ли такое множество натуральных чисел, что все его попарные суммы $a_i + a_j$, $i \leqslant j$, различны и при этом множество попарных сумм содержит отрезок натурального ряда $\mathbb{N} \cap [M, +\infty)$ при некотором M?

Множество A целых чисел называется *множеством Сидона*, если уравнение

$$x + y = u + v, \qquad x,\ y,\ u,\ v \in A$$

имеет только тривиальное решение $\{x, y\} = \{u, v\}$. Аналогичное множество остатков по модулю N будем называть множеством Сидона в $\mathbb{Z}_n$. Обозначим через f_n наибольшее количество элементов, которое может иметь множество Сидона, состоящее из натуральных чисел, не превосходящих n. Множество Сидона, состоящее из чисел, не превосходящих n, будем называть *максимальным*, если в него нельзя добавить ни одного числа, не превосходящего n, так, чтобы снова получилось множество Сидона. Вообще говоря, количество элементов в максимальном множестве Сидона может быть существенно меньше f_n. Обозначим через m_n наименьшее возможное количество элементов в максимальном множестве Сидона, в котором все числа не превосходят n. Наконец, есть еще третья постановка экстремальных задач о множествах Сидона. Для произвольного бесконечного множества Сидона A рассмотрим величину $g_n = |A \cap [1; n]|$. Насколько быстро может расти последовательность g_n? Очевидно, $g_n \leqslant f_n$. Оптимальные множества Сидона (например, из задачи 2.7) плохо согласованы друг с другом при разных n. Поэтому следует ожидать, что величина g_n существенно меньше f_n.

Некоторые из рассматриваемых неравенств имеют асимптотический характер. Будем говорить, что последовательность a_n асимптотически больше последовательности b_n (обозначается $a_n \gtrsim b_n$), если при любом $\varepsilon > 0$ при достаточно больших n выполнено неравенство $a_n \geqslant (1-\varepsilon) b_n$.

1.6. Докажите, что все попарные разности чисел из множества Сидона тоже различны.

1.7. Множество натуральных чисел от 1 до 100 разбито на 7 подмножеств. Докажите, что хотя бы одно из них — не множество Сидона.

1.8. Докажите, что существует множество Сидона из 100 натуральных чисел, не превосходящих 25 000.

1.9. A — множество Сидона из m чисел, B — произвольное множество из n чисел, $A + B$ — это множество всевозможных сумм вида $a + b$, где $a \in A$, $b \in B$. Докажите, что

$$|A + B| \geqslant \frac{m^2 n}{m + n - 1}\,.$$

1.10. Докажите, что $f_n \gtrsim \sqrt{n/2}$.

1.11. Докажите, что $f_n < \sqrt{2}\sqrt{n} + 1$.

1.12. Докажите, что $f_n < \sqrt{n} + \sqrt[4]{n} + 1$.

1.13. Докажите, что $f_n \gtrsim \sqrt{n}$.

1.14. Докажите, что $m_n \geqslant \sqrt[3]{n}$.

1.15. Докажите, что $m_n \leqslant C\sqrt[3]{n \log n}$.

1.16. Докажите, что существует бесконечное множество Сидона A, для которого $g_n \geqslant \sqrt[3]{n}$.

1.17. Докажите, что существует / постройте бесконечное множество Сидона, для которого последовательность g_n растет быстрее, чем в предыдущей задаче. В настоящее время рекорд имеет вид $g_n \gtrsim n^{\sqrt{2}-1}$.

2 *Множества Сидона в* $\mathbb{Z}_n$

2.1. Докажите, что множество Сидона в $\mathbb{Z}_N$ может иметь не менее $\sqrt[3]{N}$ элементов.

2.2. Дано множество A из n натуральных чисел, не превосходящих m, при этом $n \geqslant m/2$. Докажите, что

$$(A + A) \bmod m = \{0, 1, \dots, m-1\}.$$

2.3. Дано простое число p. Докажите, что количество различных по модулю p попарных сумм $a_i + a_j$, $i \leqslant j$, набора $\{a_1, a_2, \dots\}$ из n различных остатков по модулю p не меньше $\min(p, 2n-1)$.

2.4. Числа от 1 до $2n$ разбиты на две группы по n чисел в каждой. Докажите, что множества остатков попарных сумм чисел каждой группы при делении на $2n$ совпадают (в множество попарных сумм входят выражения вида $a + a$).

Рекордный пример “самого крупного” множества Сидона в $\mathbb{Z}_n$ принадлежит Зингеру. Одна из его реализаций описана в следующих двух задачах. Для конструкции требуется простое число p. Мы взяли $p = 5$.

2.5. Рассмотрим формальный элемент z, такой что

$$z^3 + 3z + 2 = 0.$$

Рассматривая многочлены от переменной z и пользуясь этим соотношением, мы сможем любой многочлен свести к многочлену степени не выше 2. Докажите, что множество многочленов вида $a + bz + cz^2$, где a, b, c — вычеты по модулю 5, состоит в точности из элементов 0, z, z^2, z^3, z^4, …, z^{124}.

2.6. Для каждого вычета s (по модулю 5) подберем такое натуральное k, что $z^k = z + s$. Добавим 0 к множеству из этих пяти чисел. Докажите, что получился пример множества Сидона из шести элементов в $\mathbb{Z}_{31}$.

2.7. Пусть p — простое число. Докажите, что можно указать $p-1$ натуральных чисел d_1, d_2, …, d_{p-1}, таких что их попарные суммы $d_i + d_j$, $i \leqslant j$, различны по модулю $p(p-1)$.

2.8. Если p — простое число, то можно указать p натуральных чисел d_1, d_2, …, d_p, таких что их попарные суммы $d_i + d_j$, $i \leqslant j$, различны по модулю $p^2 - 1$.

Решения

1.1. Задача предлагалась на ЛГТГ в 2002 г.

Докажем индукцией по n, что количество различных попарных сумм набора из $n \geqslant 2$ попарно различных чисел может быть любым натуральным числом из диапазона $[2n-1, C_{n+1}^2]$. База $n = 2$ очевидна.

Переход. Пусть утверждение верно для $n = k$. Докажем его при $n = k+1$. Пусть $a \in [2k-1, C_{k+1}^2]$. Рассмотрим два случая:

Случай 1. $2k-1 \leqslant a \leqslant 3k-3$. Искомым множеством является $A = [1,k] \cup \{a-k+2\}$. Очевидно, множество попарных сумм набора A есть $B = [3, a+2]$ и множество B состоит из a элементов.

Случай 2. $3k-2 \leqslant a \leqslant C_{k+1}^2$. По предположению индукции существует набор A такой, что множество попарных сумм этого набора состоит из $a-k$ элементов. Пусть $c > 2\max A$, $B = A \cup \{c\}$. Тогда множество попарных сумм набора B состоит из a элементов ($a-k$ сумм исходного набора и k сумм с участием c).

1.2. Ответ: 100. Задача предлагалась на Санкт-Петербургской математической олимпиаде в 1996 г. Автор — С. Иванов. Мы цитируем решение по [1].

Предположим, что количество не равных друг другу разностей меньше 100. Выпишем в произвольном порядке все выражения вида $a-b$, где a и b — числа из набора и $a > b$. Таких выражений столько же, сколько пар из 20 чисел, т. е. 190 штук. Поскольку они принимают меньше 100 различных значений, при выписывании более 90 раз оказывалось, что очередная разность равна какой-то из уже выписанных. Значит, имеется более 90 тождеств вида $a-b = c-d$, где a, b, c и d — числа из набора, $a > b$ и $c > d$. Каждому тождеству вида $a-b = c-d$ поставим в соответствие равенство между суммами: $a+d = b+c$. Заметим, что равенство $a+d = b+c$ сопоставлено таким образом не более чем двум тождествам с разностями, а именно тем из тождеств $a-b = c-d$, $b-a = d-c$, $a-c = b-d$ и $c-a = d-b$, в которых значения положительны. Значит, из тождеств между разностями (которых больше 90) получается больше 45 различных тождеств между суммами (мы считаем такие тождества различными, если они не получаются друг из друга перестановкой правой и левой части и перестановками слагаемых).

Докажем, что этого быть не может. Всего имеется ровно 210 попарных сумм (190 сумм различных чисел и 20 сумм, в которых число складывается с самим собой). По условию, они принимают 201 различных значений, т. е. разбиваются на 201 групп таких, что в каждой группе значения сумм одинаковы, а в разных группах — разные. Группа из k равных сумм дает $k(k-1)/2$ тождеств вида $a+b = c+d$ (столько, сколько можно составить пар из этих k сумм). Значит, общее количество тождеств между разностями равно $\sum_{i=1}^{201} k_i(k_i-1)/2$, где $k_1, \ldots, k_{201}$ — количества сумм в группах. Заметим, что максимальное значение этой суммы при условии, что k_i — натуральные числа и $\sum k_i = 210$, достигается тогда, когда все числа k_i, кроме одного, равны 1. Действительно, если $k_i \geqslant k_j > 1$, то сумму можно увеличить, заменив k_i и k_j на k_i+1 и k_j-1. Это следует из соотношения

$$\frac{(k_i+1)k_i}{2} + \frac{(k_j-1)(k_j-2)}{2} = \frac{k_i(k_i-1)}{2} + \frac{k_j(k_j-1)}{2} + k_i - k_j + 1.$$

Вычисляя сумму $\sum_{i=1}^{201} k_i(k_i-1)/2$ при $k_1 = \cdots = k_{200} = 1$ и $k_{201} = 10$, получаем 45, значит, имеется не более 45 равенств между суммами. Мы получили противоречие, чего и добивались.

Осталось привести пример набора из 20 чисел с 201 различными попарными суммами и 100 разностями. Положим $C = 10^{11}$ и рассмотрим набор чисел вида $C+10^k$ и $C-10^k$, где $k = 1, \ldots 10$. Этот набор имеет ровно 201 различных попарных сумм, а именно числа вида $2C$, $2C \pm 2\cdot 10^k$ и $2C \pm 10^k \pm 10^m$ ($k \neq m$). Попарными разностями являются числа вида $2\cdot 10^k$ (10 чисел), и $10^k - 10^m$ при $k > m$ (45 чисел) и $10^k + 10^m$ при $k \neq m$ (еще 45 чисел), итого ровно 100 различных чисел.

1.3. Задача с Канадской математической олимпиады 2002 г. Ответ: 5 чисел. Пример: 1, 2, 3, 5, 8. Если выбрать 6 чисел, то они дают 15 попарных сумм. При этом попарные суммы принимают значения от 3 до 17 — как раз 15 значений. Но 3 и 17 можно получить единственным способом: как $1+2$ и $8+9$. Следовательно, числа 1, 2, 8, 9 заведомо должны быть среди выбранных. Но это невозможно, поскольку $1+9 = 2+8$.

1.4. Задача предлагалась на 15 Уральском турнире юных математиков. Автор — С. Берлов. Ответ: такое множество существует.

Индукцией по n докажем, что существует множество Сидона, среди попарных сумм которого содержится n последовательных натуральных чисел. База очевидна. Переход от $n-1$ к n. Возьмем множество Сидона, удовлетворяющее индукционному предположению, пусть m — его максимальный элемент. Если прибавить ко всем элементам этого множества $2m$, оно по прежнему останется множеством Сидона, при этом все его попарные суммы увеличатся на $4m$ и среди них по прежнему будет $n-1$ последовательных натуральных чисел $2m+k, 2m+k+1, \ldots, 2m+k+n-2$. Теперь добавим к нашему множеству еще два числа: 1 и $2m+n-3$.

Мы построили множество, попарные суммы которого содержат n последовательных натуральных чисел. Оно является множеством Сидона, поскольку сдвинутые попарные суммы старого множества различны, попарные суммы с участием единицы меньше этих сумм, а суммы, с участием $2m+n-3$ — больше.

1.5. Ответ: такого множества не существует. Выберем большое n и пусть k — количество элементов нашего множества в интервале $[1;n]$. Тогда $k(k+1)/2 \geqslant n - \mathrm{const}$, т. е. $k \gtrsim \sqrt{2n}$, что противоречит оценке задачи 1.12.

1.6. Очевидно.

1.7. Это задача 4.7 из [3]. Какое-то из подмножеств содержит не менее 15 чисел. Для них можно составить не менее $15 \cdot 14/2 = 105$ разностей (где из большего числа вычитают меньшее). Значит, какие-то две разности совпадают, и тем самым это подмножество не является множеством Сидона.

1.8. Эта задача Ф. Петрова и Д. Джукича была включена в шортлист международной олимпиады по математике 2001 г. Приводим авторское решение.

Положим $p = 101$. Возьмем числа вида $2kp + (k^2 \bmod p)$, $k = 1, \ldots, p$. Проверим, что у этих чисел попарные суммы различны. Действительно, если случилось, что

$$2kp + (k^2 \bmod p) + 2\ell p + (\ell^2 \bmod p) = 2mp + (m^2 \bmod p) + 2np + (n^2 \bmod p)\,,$$

то обязательно $k+\ell = m+n$, и $k^2+\ell^2 \equiv m^2+n^2 \pmod p$. Отсюда $k+\ell \equiv m+n \pmod p$, $k\ell \equiv mn \pmod p$, и по теореме Виета $\{k,\ell\} = \{m,n\}$.

1.9. Это утверждение из [10]. Обозначим через $\sigma(k)$ количество решений уравнения

$$a+b=k, \qquad a \in A,\ b \in B\,.$$

Ясно, что $\sum_k \sigma(k) = |A|\cdot|B| = mn$. Тогда по неравенству о среднем арифметическом и среднем квадратичном

$$\sum_k \sigma(k)^2 \geqslant \frac{m^2n^2}{|A+B|}\,. \tag{1}$$

Сумма в левой части подсчитывает количество четверок чисел a, $a' \in A$, b, $b' \in B$, для которых $a+b = a'+b'$, или

$$a - a' = b' - b\,.$$

При $b = b'$ имеем $a = a'$, что дает нам mn различных решений уравнения, а при $b \neq b'$, в силу результата задачи 1.6, этому уравнению удовлетворяет не более одной пары чисел a, a', и мы получаем еще не более $n(n-1)$ решений. Итого

$$\sum_k \sigma(k)^2 \leqslant n(n-1) + mn\,.$$

Вместе с неравенством (1) это дает требуемое утверждение.

1.10. [6]. Аналогично задаче 1.8.

1.11. [6] Пусть $|A| = k$. Все разности вида $a-b$, $a > b$, a, $b \in A$ различны и лежат в интервале $[1, n-1]$. Их количество равно $k(k-1)/2$. Следовательно, $k(k-1)/2 \leqslant n-1$, откуда $k \leqslant \sqrt{2n - \frac{7}{4}} + \frac{1}{2} < \sqrt{2n} + 1$.

1.12. Мы приведем два решения этой задачи.

Решение 1 ([7]) . Пусть $1 \leqslant a_1 < a_2 < \cdots < a_r \leqslant n$ — данные числа. Тогда все разности вида $a_i - a_j$ различны. Величину $i-j$ назовем *порядком* разности $a_i - a_j$. Все разности порядка q могут быть разбиты на цепочки вида

$$a_\alpha - a_\beta,\ a_\beta - a_\gamma,\ \ldots, \qquad \alpha - \beta = \beta - \gamma = \ldots = q\,.$$

Сумма разностей из одной цепочки, очевидно, меньше n, следовательно, сумма всех разностей порядка q меньше qn. Тогда сумма всех разностей, порядок которых не превосходит некоторого числа m, меньше чем $\frac{1}{2}m(m+1)n$.

Количество разностей порядка k равно $r-k$, поскольку каждая такая разность имеет вид $a_{i+k} - a_i$, где $1 \leqslant i \leqslant r-k$. Следовательно, количество разностей, порядок которых не превосходит m, $1 \leqslant m < r$, равно $mr - \frac{1}{2}m(m+1) = ms$, где $s = r - \frac{1}{2}(m+1)$. Поскольку все разности попарно различны, сумма всех разностей, порядок которых не превосходит m, не меньше чем $\frac{1}{2}ms(ms+1) > \frac{1}{2}m^2s^2$. Таким образом,

$$\frac{1}{2}m^2s^2 < \frac{1}{2}m(m+1)n\,.$$

Сокращая, получаем
$$s < \sqrt{1+\frac{1}{m}}\,\sqrt{n} < \Big(1+\frac{1}{2m}\Big)\sqrt{n}\,.$$
Отсюда
$$r < \frac{1}{2}(m+1) + \Big(1+\frac{1}{2m}\Big)\sqrt{n}\,.$$
Выбирая $m = [\sqrt[4]{n}] + 1$, получаем требуемое.

Решение 2 ([10]). Пусть $A \subset [1, N]$ — множество Сидона из m чисел и пусть $B = \{1, 2, \ldots, n\}$. Тогда $A + B \subset [2, N+n]$ и по утверждению задачи 1.9
$$N + n - 1 \geqslant |A+B| \geqslant \frac{m^2 n}{m+n+1}\,.$$
Подставим $n = [m\sqrt{m}] - m + 1$:
$$N \geqslant \frac{m^2(m\sqrt{m} - m)}{m\sqrt{m}} - m\sqrt{m} + m = m^2 - 2m\sqrt{m} + m = (m - \sqrt{m})^2\,.$$
Решая это квадратичное неравенство относительно m, получаем
$$m \leqslant \sqrt{N} + \frac{1}{2} + \sqrt{\sqrt{N} + \frac{1}{4}} < \sqrt{N} + N^{1/4} + 1\,.$$

1.13. Следует из утверждения задачи 2.7.

1.14. Максимальность множества A означает, что для любого числа $d \leqslant n$, $d \notin A$ имеет место одно из представлений
$$d = a + b - c, \quad \text{где } a \neq b$$
$$2d = a + b,$$
$$d = 2a - c\,.$$
где a, b, $c \in A$. Сумм первого вида не более $m_n^2(m_n - 1)/2$, сумм второго — не более $m_n(m_n - 1)/2$, третьего — не более $m_n(m_n - 1)$. Количество чисел, которые мы пытаемся добавить, не может превосходить общее количество сумм. Следовательно,
$$n - m_n \leqslant \frac{m_n^2(m_n - 1)}{2} + \frac{m_n(m_n - 1)}{2} + m_n(m_n - 1)\,.$$
При $m_n \geqslant 3$ правая часть последнего неравенства, как нетрудно проверить, не превосходит $m_n^3 - m_n$.

1.15. Результат из [9].

1.16. Например, годится последовательность, построенная при помощи жадного алгоритма.

1.17. Рекордная конструкция описана в [8].

2.1. Возьмем какое-нибудь множество Сидона A в $\mathbb{Z}_N$ и будем добавлять в него новые элементы, пока это возможно. Невозможность добавить элемент означает, что любой элемент $d \in \mathbb{Z}_N \setminus A$ представим в виде $a + b - c$, где a, b, $c \in A$. Если множество A к этому моменту содержит k элементов, то в таком виде предствимо не более k^3 различных элементов $\mathbb{Z}_n$. Следовательно, $N \leqslant k^3 + k$.

2.2. Это задача 4.5 из [3]. Возьмем произвольный остаток k по модулю m. Рассмотрим $2n$ чисел
$$a_1,\ a_2,\ \ldots, a_n,\ \ldots, k - a_1,\ k - a_2,\ \ldots,\ k - a_n\,.$$
Первые n из них по условию имеют разные остатки по модулю m, следовательно, и остальные n чисел имеют разные остатки. Но всего здесь $2n > m$ чисел, поэтому для каких-то i и j число a_i имеет такой же остаток, как и число $k - a_j$. Тогда $a_i + a_j \equiv k \pmod{m}$.

2.3. Это частный случай теоремы Коши–Дэвенпорта: если p — простое число, то для любых двух множеств A и $B \subset \mathbb{Z}_p$

$$|A+B| \geqslant \min\{p, |A|+|B|-1\}.$$

Доказательство: Случай $|A|+|B| > p$ достаточно прост, мы его оставляем читателю. Будем рассматривать множества с дополнительных условием $|A|+|B| \leqslant p$. Допустим, что для некоторых множеств A и B верно противоположное неравенство

$$|A+B| \leqslant |A|+|B|-1. \qquad (*)$$

Среди всех таких пар множеств выберем пары с наименьшим возможным значением величины $|A+B|$, а среди таких пар — ту, у которой меньшее множество A содержит меньше всего элементов. Можно считать, что $|A| \geqslant 2$.

Заметим, что если сдвинуть одно из множеств, т.е., например, вместо множества A рассмотреть множество $A+c$ при некотором $c \in \mathbb{Z}_p$, то старое множество $A+B$ также сдвинется на c. В частности, количество элементов в множестве $A+B$ не изменится.

Сдвинем множество A таким образом, чтобы множества A и B пересекались, но при этом $A \not\subset B$. Это можно сделать по следующей причине. Допустим, что любой сдвиг A приводит к тому что если сдвинутое множество A пересекается с B, то оно содержится в B. Рассмотрим любой из таких случаев взаиморасположения множеств. Пусть a, $b \in A \cap B$ и $A \subset B$. Сдвинем множество A на $b-a$. Точка a перейдет в b, и следовательно, пресечение множеств не исчезнет. Если по-прежнему $A \subset B$, то образ точки b принадлежит обоим множествам. Рассмотрим еще один сдвиг на $b-a$ и т.д. Если каждый раз сдвинутое множество A будет содержаться в B, мы установим, что все точки

$$a,\ b,\ b+(b-a),\ b+2(b-a),\ b+3(b-a), \ldots$$

(все арифметические операции по модулю p) принадлежит множеству B. Это невозможно, покольку множество этих точек совпадает с $\mathbb{Z}_p$.

Итак, мы можем сдвинуть множество A таким образом, чтобы множества A и B пересекались, но при этом $A \not\subset B$. Заметим, что тогда для множеств $A_1 = A \cap B$ и $B_1 = A \cup B$ верно, что $A_1 + B_1 \subset A + B$, т.е. $|A_1 + B_1| \leqslant |A+B|$; кроме того $|A_1| + |B_1| = |A| + |B|$. Таким образом, пара множеств A_1, B_1 удовлетворяет неравенству $(*)$. Но при этом $|A_1| < |A|$, что противоречит минимальности множества A.

2.4. Задача предлагалась на Санкт-Петербургской математической олимпиаде в 1996 г. Автор — С. Иванов. Мы цитируем решение по книге [2].

В этой задаче, вычисляя остатки при делении на $2n$, всегда будем вместо остатка 0 брать число $2n$.

Пусть числа a и b (возможно, равные) принадлежат первой группе. Нам достаточно найти два числа из второй группы, сумма которых дает такой же остаток при делении на $2n$, что и $(a+b)$. Разобьем числа от 1 до $2n$ на пары следующим образом. Пусть $c = (a+b)/2$. Если c — число целое, то рассмотрим следующие пары чисел (всего $n+1$ пара):

$$(c,c),\ (c-1,c+1),\ \ldots,(c-n+1,c+n-1),\ (c-n,c+n).$$

Чтобы получились пары чисел из наших множеств, возьмем остатки чисел из этих пар при делении на $2n$. Построенное множество пар обладает тем свойством, что сумма чисел в каждой паре имеет такой же остаток при делении на $2n$, что и $(a+b)$, и никакие две пары не содержат одного и того же числа. Заметим, что среди этих пар встретится и наша исходная пара

$$(a,b) = \left(c + \frac{a-b}{2}, c - \frac{a-b}{2}\right).$$

Кроме чисел a и b в первой группе имеется еще $(n-2)$ числа, а кроме пары (a,b) в построенном множестве имеется еще n пар, значит, обязательно в какой-то из пар нет ни одного числа из первой группы, и, таким образом, эта пара содержит два требуемых числа из второй группы (возможно, совпадающие). Случай полуцелого c разбирается аналогично.

2.5.

2.6.

2.7. Это утверждение из [10]. Пусть g — первообразный корень по модулю p. Для $i = 1, 2, \ldots, p$ обозначим через a_i решение системы сравнений

$$a_i \equiv i \pmod{p-1}, \qquad a_i \equiv g^i \pmod{p}.$$

Это и есть требуемый набор чисел. Чтобы убедиться в этом, достаточно проверить, что сравнение

$$a_i + a_j \equiv r \pmod{p(p-1)}$$

имеет при каждом r не более одного решения (i, j) с точностью до перестановки. Это сравнение эквивалентно системе из двух сравнений

$$a_i + a_j \equiv r \pmod{p-1}, \qquad a_i + a_j \equiv r \pmod{p},$$

т.е.

$$i + j \equiv r \pmod{p-1}, \qquad g^i + g^j \equiv r \pmod{p},$$

Тогда числа $x_1 = g^i$, $x_2 = g^j$ удовлетворяют сравнениям

$$x_1 + x_2 \equiv r \pmod{p}, \qquad x_1 x_2 \equiv g^r \pmod{p}$$

и поэтому $\pmod{p}$ определены однозначно. Таким образом, пара (i, j) определена однозначно.

2.8. Это результат из [4]. Пусть c — первообразный корень F_{p^2}. Элементы поля F_p будем обозначать $1, \ldots, (p-1)$, p. Пусть d_i — натуральные число, удовлетворяющие соотношениям

$$c^{d_i} = c + i \quad (i = 1, 2, \ldots, p).$$

Тогда числа d_i образуют то множество, которое нам требуется. Действительно, предположим, что $d_i + d_j = d_k + d_\ell \pmod{p^2 - 1}$. Тогда в F_{p^2} мы имеем равенство $c^{d_i} c^{d_j} = c^{d_l} c^{d_\ell}$, т. е.

$$(c + i)(c + j) = (c + k)(c + \ell)$$

или

$$c(i + j - k - \ell) = k\ell - ij\,.$$

Так как $c \notin F_p$, мы вынуждены заключить, что $i + j - k - l = 0$ и $k\ell - ij = 0$. Но тогда $\{i, j\} = \{k, \ell\}$.

Литература

[1] *Берлов С., Иванов С., Карпов Д., Кохась К., Петров Ф., Храбров А.* Задачи Санкт-Петербургской олимпиады школьников по математике. 2000. СПб.: изд-во СПбГУ, 2000.

[2] *Берлов С., Иванов С., Кохась К.* Петербургские математичкские олимпиады. СПб.: Лань, 2003.

[3] *Конягин С. В., Тоноян Г. А. и др.* Зарубежные математические олимпиады. М.: Наука, 1987.

[4] *Bose R.C., Chowla S.* Theorems in the additive theory of numbers. // Comment. Math. Helv. 1962/63. Vol. 37. P. 141–147.

[5] *Katz N.H., Nao T.* A new bound on partial sum-sets and difference-sets, and applications to the Kakeya conjecture // arxiv.org

[6] *Kolountzakis M.* Problems in the additive number theory of general sets, I. Sets with didstinct sums. // http://www.math.uiuc.edu/˜ kolount/surveys.html

[7] *Lindsröm B.* An inequality for B_2-sequences. Journ. of Comb. Theory, V. 6. P. 211–212.

[8] *Ruzsa I.* An infinite Sidon sequence. // J. Number Theory. 1998. Vol. 68. P. 63–71.

[9] *Ruzsa I.* A small maximal Sidon set // Ramanujan J. 1998. Vol. 2. P. 55–58.

[10] *Ruzsa I.* Solving of linear equation in a set of integers, I. Acta Arithmetica. 1993. Vol. LXV. N. 3. P. 259–282.

[11] Singer J. A theorem in finite projective geometry and some applications to number theory // Trans. Amer. Math. Soc. 1938. Vol. 43 P. 377–385.