Московский физико-технический институт
Физтех-школа прикладной математики и информатики

ОСНОВЫ КОМБИНАТОРИКИ И ТЕОРИИ ЧИСЕЛ

I СЕМЕСТР

Лекторы: *Райгородский Андрей Михайлович*
Мусатов Даниил Владимирович

Авторы: *Даниил Максимов*
Проект на Github

осень 2021

Содержание

1 Наивная теория множеств

1.1 Множество

Определение 1.1. *Множеством* называется совокупность каких-либо объектов.

Замечание. Если говорить чуть точнее, то множество считается неопределяемым понятием, так как его определение даётся через синонимичные слова, что является замкнутым кругом.

Замечание. В рамках стандартной модели (так мы будем называть наивную теорию множеств, ибо будем работать по большому счёту только с ней) объектом может быть что угодно, в том числе и множество.

Свойства множества

1. Каждый объект входит в множество ровно один раз, то есть множество хранит *уникальные* объекты. Если мы рассматриваем множества без этого свойства, то они называются *мультимножествами*.
2. Множество не обладает порядком. Если порядок объектов в множестве важен, то такое множество называется *кортежом*, или же *упорядоченным множеством*.
3. Запись $x \in Y$ означает, что объект x принадлежит множеству Y.

Замечание. Еще вводится обозначение $x \notin Y$, что по определению означает $\neg(x \in Y)$.

Определение 1.2. *Элементом* множества называется объект, который принадлежит этому множеству.

Определение 1.3. Выражение $X \subset Y$ означает, что множество X является *подмножеством* Y. Формально записывается так:

$$X \subset Y \Rightarrow (\forall x \in X \Rightarrow x \in Y).$$

1.2 Равенство множеств

Определение 1.4. $X = Y$, если $(X \subset Y) \wedge (Y \subset X)$, или же $\forall z \in X \Rightarrow z \in Y$ и $\forall z \in Y \Rightarrow z \in X$.

Свойства равенства множеств

1. $X \subset X$ (рефлексивность).
2. $(X \subset Y) \wedge (Y \subset X) \Rightarrow (X = Y)$ (антисимметричность).
3. $(X \subset Y) \wedge (Y \subset Z) \Rightarrow (X \subset Z)$ (транзитивность).

Замечание. При этом стоит отметить, что принадлежность не обладает транзитивностью. Контрпримером служит выражение:

$$1 \in \{1\} \in \{2, 3, \{1\}\},$$

но при этом $1 \notin \{2, 3, \{1\}\}$.

1.3 Способы описания множеств

1. Прямое перечисление элементов: $X = \{1, 2, 3\}$.
2. Генератор множества (set builder notation) $X = \{x \mid x = 2k, k \in \mathbb{N}\}$.

1.4 Парадокс Рассела

Если множество может быть элементом множества, то существует ли множество всех множеств? С этим вопросом мы приходим быстро к противоречию.

Утверждение 1.1. *Рассмотрим $M = \{x \mid x \notin x\}$. Верно ли утверждение $M \in M$?*

Доказательство. Имеем 2 случая:

1. $M \in M$. Но из определения $\forall x \in M \Rightarrow x \notin x$, мы получаем противоречие.
2. $M \notin M$. Но из определения $x \notin x \Rightarrow x \in M$. Снова противоречие.

Таким образом, множества всех множеств не существует. □

Замечание. Выше мы говорили о равенстве множеств. Как известно, мы определяем равенство как отношение эквивалентности на некотором множестве, но так как мы показали, что множества всех множеств не существует, то мы не можем назвать равенство между множествами отношением эквивалентности.

1.5 Пустое множество

Определение 1.5. *Пустым множеством* называется такое множество, в котором нету элементов. Обозначается обычно так: $\varnothing$.

Свойства пустого множества

1. Пустое множество единственно.
2. Пустое множество вложено в любое другое множество: $\forall X \Rightarrow \varnothing \subset X$.

1.6 Различие между принадлежностью и подмножеством

Рассмотрим X - некоторое конечное множество, содержащее n элементов.
Сколько подмножеств у такого множества? Ответ: 2^n.

▷ $n = 0 \Rightarrow \varnothing$ — 1 подмножество, 0 элементов.

▷ $n = 1 \Rightarrow \varnothing, \{a\}$ — 2 подмножества, 1 элемент.

▷ $n = 2 \Rightarrow \varnothing, \{a\}, \{b\}, \{a, b\}$ — 4 подмножества, 2 элемента.

1.7 Универсальное множество

Определение 1.6. *Универсальным множеством* называется такое множество, для которого в конкретно задаче считается верным, что для любого множества A выполнены два свойства:

- $A \cap U = A$,
- $A \cup U = U$.

1.8 Операции над множествами

1. Объединение: $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$.
2. Пересечение: $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$.
3. Разность: $A \backslash B = \{x \mid (x \in A) \wedge (x \notin B)\}$.
4. Симметрическая разность: $A \triangle B = \{x \mid (x \in A \cup B) \wedge (x \notin A \cap B)\}$.
5. Отрицание (дополнение): $\overline{A} = \{x \mid x \notin A\}$.

Дистрибутивность

Утверждение 1.2. *Для любых множеств A, B и C верно, что*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Доказательство. Пусть $x \in A \cap (B \cup C)$, тогда:

$$(x \in A) \wedge (x \in (B \cup C)).$$

Имеем 2 случая:

1. $(x \in A) \wedge (x \in B) \Rightarrow x \in (A \cap B)$.
2. $(x \in A) \wedge (x \in C) \Rightarrow x \in (A \cap C)$.

Фактически означает, что $x \in (A \cap B) \cup (A \cap C) \Rightarrow A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$. Теперь покажем обратное. Рассмотрим $x \in (A \cap B) \cup (A \cap C)$. Возникает снова 2 случая:

1. $x \in (A \cap B) \Rightarrow (x \in A) \wedge (x \in B) \Rightarrow (x \in A) \wedge (x \in (B \cup C)) \Rightarrow x \in A \cap (B \cup C)$.
2. $x \in (A \cap C) \Rightarrow (x \in A) \wedge (x \in C) \Rightarrow (x \in A) \wedge (x \in (B \cup C)) \Rightarrow x \in A \cap (B \cup C)$.

Отсюда по определению равенства $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. □

Законы де Моргана

Законы де Моргана на множествах имеют ровно такие же аналоги, как и в логике:

$$\overline{A \cap B} = \overline{A} \cup \overline{B},$$
$$\overline{A \cup B} = \overline{A} \cap \overline{B}.$$

1.9 Упорядоченные пары и кортежи

Определение 1.7. *Неупорядоченной парой* называется мультимножество из 2х элементов. Обозначается как и просто множество: $\{a, b\}$.

Определение 1.8. *Упорядоченной парой* называется неупорядоченная пара, у которой зафиксирован первый элемент. Обозначается через круглые скобки: (a, b). Упорядоченная пара может быть выражена через мультимножество по определению Куратовского:

- ▷ упрощенное определение Куратовского $\{a, \{a, b\}\}$,
- ▷ полное определение Куратовского $\{\{a\}, \{a, b\}\}$.

Определение 1.9. Неформально *кортеж* — это упорядоченное мультимножество $(x_1, \ldots, x_n)$. Если формально, то определение рекурсивно:

1. Кортеж длины 0 — это $\varnothing$.
2. Кортеж длины $n + 1$ — это упорядоченная пара (h, T), где T — кортеж длины n, а h — элемент, который мы ставим на первое место в кортеже.

Пример. $(x_1, x_2, \ldots, x_n) = (h, T)$, где $h = x_1$, $T = (x_2, \ldots, x_n)$.

1.10 Декартово произведение

Определение 1.10. *Декартовым произведением* множеств A и B называется множество

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Замечание. Такое множество называется декартовым из-за близости с декартовой системой координат. Первый элемент даст координату по оси x, а второй по оси y.

1.11 Декартова степень

Определение 1.11. *Декартовой степенью* n множества A называется множество

$$A^n = \{(a_1, \ldots, a_n) \mid a_i \in A\}$$

Ассоциативность декартового произведения

Утверждение 1.3. *Если положить кортежи* $(a, (b, c))$ *и* $((a, b), c)$ *естественно равными для любых* a, b, c*, то декартово произведение ассоциативно:*

$$\forall A, B, C \quad A \times (B \times C) = (A \times B) \times C$$

1.12 Отображения и соответствия

Определение 1.12. *Соответствием* между A и B называется произвольное подмножество $A \times B$.

$$F \subset A \times B.$$

Принадлежность пары (a, b) данному соответствию F принято обозначать как

$$\big((a, b) \in F\big) := \big(b \in F(a)\big).$$

Само соответствие порой обозначают так

$$F \colon A \rightrightarrows B.$$

Определение 1.13. *Отображением* или же *функцией* между множествами A и B называется однозначное соответствие на этих же множествах, то есть

$$\forall a \in A \; \exists! b \in B \colon b = F(a).$$

Или же пишут, что

$$F \colon A \to B.$$

Определение 1.14. *Аргументом* функции называется $a \in A$.

Определение 1.15. *Значением функции* называется $b \in B$.

Определение 1.16. Функция называется *частично определенной*, если допускается отсутствие значения у какого-либо аргумента, то есть

$$\forall a \in A \Rightarrow |F(a)| \leqslant 1.$$

Свойства соответствий и отображений

Соответствие называется

- ▷ *инъективным*, если $\forall a_1, a_2 \in A \colon a_1 \neq a_2 \Rightarrow F(a_1) \cap F(a_2) = \varnothing$;
- ▷ *сюръективным*, если $\forall b \in B \;\; \exists a \in A \colon b \in F(a)$;
- ▷ *биективным*, если оно является одновременно и инъективным, и сюръективным.

Для отображений все определяется примерно так же. Отображение называется

- ▷ *инъекцией*, если $\forall a_1, a_2 \in A \colon a_1 \neq a_2 \Rightarrow F(a_1) \neq F(a_2)$;
- ▷ *сюръекцией*, если $\forall b \in B \;\; \exists a \in A \colon b = F(a)$;
- ▷ *биекцией*, если оно является одновременно и инъекцией, и сюръекцией.

Определение 1.17. F^{-1} называется *обратным соответствием* к F, если

$$(a, b) \in F \Leftrightarrow (b, a) \in F^{-1}.$$

Определение 1.18. F^{-1} называется *обратным отображением* к F, если

$$b = F(a) \Leftrightarrow a = F^{-1}(b).$$

1.13 Образ и прообраз

Замечание. Определения ниже даны в предположении, что задано соответствие $F\colon A \rightrightarrows B$.

Определение 1.19. Если $S \subset A$, то $F(S) := \bigcup\limits_{a \in S} F(a)$ называется *образом* множества S.

Определение 1.20. Пусть $T \subset B$. Тогда $F^{-1}(T) := \bigcup\limits_{b \in T} F^{-1}(b)$ называется *прообразом* множества T.

Определение 1.21. *Областью определения* F называется прообраз множества B. Обозначается как $Dom\ F$ (от слова *domain*).

Определение 1.22. *Областью значений* F называется образ множества A. Обозначается как $Ran\ F$ (от слова *range*).

Определение 1.23. Пусть $S \subset A$. Тогда $F|_S : S \to B$ называется *сужением* $F : A \to B$ на подмножество S, то есть $x \in S \Rightarrow F|_S(x) = F(x)$.

При этом F по отношению к $F|_S$ называется *продолжением*.

Утверждение 1.4. *Если F — частично определенная функция, то $F|_{Dom\ F}$ — отображение.*

1.14 Композиция

Определение 1.24. Пусть $F\colon A \rightrightarrows B$, $G\colon B \rightrightarrows C$. Тогда соответствие $G \circ F$ называется *композицией* соответствий F и G, если

$$G \circ F\colon A \rightrightarrows C,$$
$$(x, z) \in G \circ F \Leftrightarrow \exists y \mid \big((x, y) \in F\big) \wedge \big((y, z) \in G\big).$$

Определение 1.25. Пусть $F\colon A \to B$, $G\colon B \to C$. Тогда отображение $G \circ F$ называется *композицией* отображений F и G, если

$$G \circ F\colon A \to C,$$
$$(x, z) \in G \circ F \Leftrightarrow \exists y \mid \big(y = F(x)\big) \wedge \big(z = G(y)\big).$$

Принято обозначать $G \circ F := G(F(x))$.

Свойства композиции

Рассматриваются такие соответствия/отображения, что композиция существует.

1. $H \circ (G \circ F) = (H \circ G) \circ F$ (ассоциативность).
2. Коммутативность **необязательно** выполнена.

   Пример. Пусть $F : A \rightrightarrows B$, $G : B \rightrightarrows A$. Тогда $G \circ F : A \rightrightarrows A$, но при этом $F \circ G : B \rightrightarrows B$.
3. $\exists id_A\colon A \to A$, $id_B\colon B \to B \mid F \circ id_A = id_B \circ F = F$ (существование отображения множества в себя, т.е. $a = id_A(a)\ \forall a \in A$).
4. $F^{-1} \circ F = id_A$, если $F\colon A \to B$.
5. $F \circ F^{-1} = id_B$, если $F\colon A \to B$.

1.15 Степень соответствия

Определение 1.26. Пусть задано соответствие $F\colon A \rightrightarrows A$. Тогда

$$F^n = \underbrace{F \circ \cdots \circ F}_{n \text{ раз}}, \quad n \in \mathbb{N}.$$

Свойства степени

- $F^{n+m} = F^n \circ F^m$.
- $(F^n)^m = F^{n \cdot m}$.

1.16 Возведение множества в степень другого множества

Пусть есть A и B такие, что $|A| = n$, $|B| = k$.
Вопрос: сколько существует *различных* отображений из A в B?
Ответ: k^n.

Определение 1.27. Степенью A множества B называется множество всевозможных отображений из множества A в множество B:

$$|B^A| = |B|^{|A|}.$$

Случай с $k = 2$

Заметим, что для полного определения $F : A \to B$ нам необходимо и достаточно задать $F^{-1}(b_0)$ или $F^{-1}(b_1)$. Тогда $F(x)$ можно определить очень просто:

$$F(x) = \begin{cases} b_0, & \text{если } x \in F^{-1}(b_0), \\ b_1, & \text{иначе.} \end{cases}$$

Таким образом, получается вывод: любое подмножество *однозначно* сопоставляется функции с двумя значениями.

Определение 1.28. *Булеаном* называют множество всех подмножеств множества A. Обозначается как 2^A.

Случай с $n = 0$

Пусть $A = \varnothing$. Тогда посмотрим на произвольное отображение $F\colon A \to B$. Как известно, F представляет собой подмножество $A \times B = \varnothing \times B = \varnothing$. То есть $F = \varnothing$, при этом данное соответствие является отображением, так как любому элементу множества A соответствует ровно один элемент множества B. Отсюда следствие:

$$B^{\varnothing} = \{\varnothing\}.$$

Причём это верно для любого B, даже для $B = \varnothing$.

Случай с $n \neq 0, k = 0$

$F \subset A \times \varnothing = \varnothing$, но если $A \neq \varnothing$, то такое соответствие не является отображением, так как любому элементу из A ничего не соответствует (частично определенная функция).

Свойства множества в степени множества

1. $(A \times B)^C \cong A^C \times B^C$.
2. $B \cap C = \varnothing \Rightarrow A^{B \cup C} \cong A^B \times A^C$.
3. $A^{B \times C} \cong (A^B)^C$.

Замечание. Писать знак $=$ вместо $\cong$ — слишком сильное утверждение. Выражение справа и слева не являются эквивалентными, но между ними существует «естественное» отображение (равномощность).

1.17 Мощность множества

Определение 1.29. Наивно определим мощность через рекурсию:

1. $|\varnothing| = 0$,
2. $|A| = |A \backslash \{a_1\}| + 1$.

Замечание. Так, вообще говоря, нельзя делать. Из-за такого определения мы зацикливаем определение натуральных чисел, если задавать их через аксиомы Пеано.

Теорема 1.1. *Мощность множества не зависит от того, какой конкретно элемент из него исключили, то есть* $\forall a, b \in A \Rightarrow |A \backslash \{a\}| = |A \backslash \{b\}|$.

Доказательство.

$$|A \backslash \{a\}| = |A \backslash \{a\} \backslash \{b\}| + 1 = |A \backslash \{b\}|.$$

□

Теорема 1.2. *Если множества A и B конечны, то в них поровну элементов тогда и только тогда, когда между ними есть биекция.*

Доказательство. Докажем, что если $|A| = |B|$, то между множествами существует биекция. Сделаем это по индукции:

База: $A = B = \varnothing$. Тогда, отображение $F\colon A \to B$ — биекция (несложно проверить).

Ход индукции: теперь $A \neq \varnothing$ и $B \neq \varnothing$. Выберем $a \in A$ и $b \in B$. Согласно предположению индукции, то существует биекция $F\colon A \backslash \{a\} \to B \backslash \{b\}$. Если мы добавим к данной биекции новую пару $b = F(a)$, то она всё ещё будет биекцией. Что и требовалось доказать.

Теперь докажем в обратную сторону: если есть биекция, то в множествах поровну элементов.

Пусть $A = \varnothing$. Тогда, $B = \varnothing$, иначе мы нарушим сюръективность $\Rightarrow |A| = |B| = 0$.

Рассмотрим $A \neq \varnothing$. Выберем $a \in A$. Тогда, так как у нас есть биекция, то найдётся $b = F(a)$. Заметим, что $F|_{A \backslash \{a\}}$ — тоже биекция, а значит $|A \backslash \{a\}| = |B \backslash \{b\}|$. Следовательно, $|A| = |B| = |A \backslash \{a\}| + 1 = |B \backslash \{b\}| + 1$. □

1.18 Равномощность

Определение 1.30. Множества A и B называются *равномощными*, если существует биекция $F\colon A \to B$. Обозначается как $A \cong B$.

Замечание. Отношение равномощности обладает всеми свойствами отношения эквивалентности, **но не является им из-за несуществования всеобъемлющего множества**.

Порядок на равномощности

Определение 1.31. Говорят, что $A \lesssim B$, если $\exists B' \subset B \mid A \cong B$.

Определение 1.32. $A \lesssim B$, если $A \lesssim B$ и при этом $A \ncong B$.

Теорема 1.3. *(Кантора-Бернштейна) Отношение порядка на равномощности антисимметрично, то есть*

$$(A \lesssim B) \wedge (B \lesssim A) \Rightarrow A \cong B.$$

Доказательство. Пусть выполнено $A \lesssim B$ и $B \lesssim A$. Это означает, что есть биекции $f\colon A \to B_1$ и $g\colon B \to A_1$, где $A_1 \subset A$ и $B_1 \subset B$.

Так как f и g - отображения, то можно посмотреть на образы $f(A_1) = B_2$ и $g(B_1) = A_2$. При этом верны утверждения:

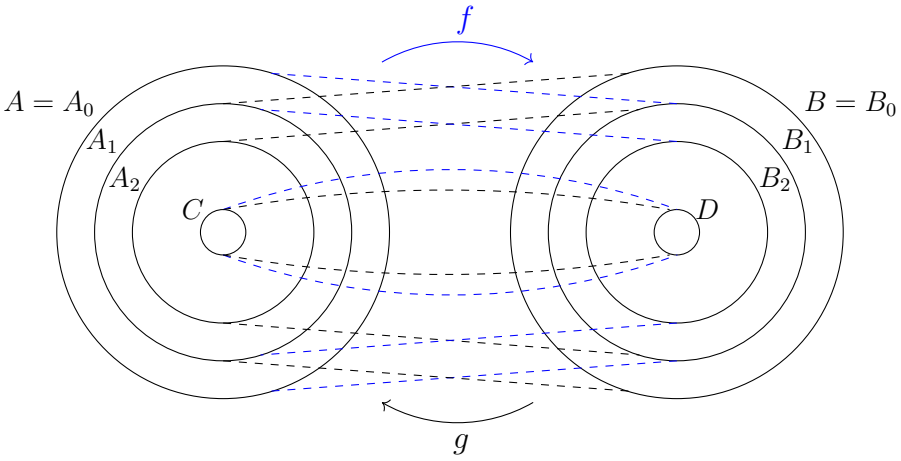
$$B \supset B_1 \Rightarrow g(B) \supset g(B_1)$$
$$A \supset A_1 \Rightarrow f(A) \supset f(A_1)$$

То есть $B_1 \supset B_2$ и $A_1 \supset A_2$. Так можно продолжать итеративно и, положив за $A_0 = A$, $B_0 = B$, получить последовательности вложенных множеств:

$$A_0 \supset A_1 \supset A_2 \supset \dots$$
$$B_0 \supset B_1 \supset B_2 \supset \dots$$

При этом имеются равенства:

$$f(A_k) = B_{k+1}$$
$$g(B_k) = A_{k+1}$$



Из всего вышесказанного возникают 2 утверждения, которые мы положим в основу биекции $h\colon A \to B$:

$$f(A_k \backslash A_{k+1}) = B_{k+1} \backslash B_{k+2}$$
$$g(B_k \backslash B_{k+1}) = A_{k+1} \backslash A_{k+2}$$

Но этого недостаточно. Ещё могут быть такие элементы, которые не попадут ни в одно кольцо: они принадлежат множествам $C = \bigcap\limits_{i=0}^{\infty} A_i$ и $D = \bigcap\limits_{i=0}^{\infty} B_i$. Однако при этом заметим, что $f(C) = D$, $g(D) = C$. Если $c \in C$, то $\forall i \ \{c\} \subset A_i$, а из этого следует, что $\forall i \ \{f(c)\} \subset f(A_i)$. Аналогично для $d \in D$. Если же элемент $a \notin C$, то он лежит в каком-то кольце и про этот случай уже всё известно. В итоге получаем следующую биекцию:

$$h(x) = \begin{cases} f(x),\ x \in A_{2k} \backslash A_{2k+1} \\ g^{-1}(x),\ x \in A_{2k+1} \backslash A_{2k+2} \\ f(x),\ x \in C \end{cases}$$

□

1.19 Бинарные отношения

Определение 1.33. Подмножество $R \subset A \times A$ называется *бинарным отношением*, $(x, y) \in R$ принято обозначать как xRy.

Свойства бинарных отношений

- ▷ Рефлексивность: $\forall a \in A \ aRa$.
- ▷ Антирефлексивность: $\forall a \in A \ \neg aRa$.
- ▷ Симметричность: $\forall a, b \in A \ aRb \Rightarrow bRa$.
- ▷ Антисимметричность: $\forall a, b \in A \ (aRb \wedge bRa) \Rightarrow (a = b)$.
- ▷ Транзитивность: $\forall a, b, c \in A \ (aRb \wedge bRc) \Rightarrow aRc$.
- ▷ Антитранзитивность: $\forall a, b, c \in A \ (aRb \wedge bRc) \Rightarrow \neg aRc$.
- ▷ Евклидовость: $\forall a, b, c \in A (aRc \wedge bRc) \Rightarrow aRb$.
- ▷ Полнота: $\forall a, b \in A (aRb \vee bRa)$.

1.20 Отношение эквивалентности

Определение 1.34. *Отношением эквивалентности* называется бинарное отношение, которое обладает рефлексивностью, симметричностью и транзитивностью.

Теорема 1.4. *Если на множестве A задано отношение эквивалентности, то A разбивается на классы эквивалентности — множества A_α такие, что*

- ▷ $\forall x, y \in A_\alpha \Rightarrow x \sim y$,

▷ $\forall x \in A_\alpha, y \in A_\beta, \alpha \neq \beta \Rightarrow x \not\sim y$.

Доказательство. Пусть $K_x = \{y \mid y \sim x\}$.

1. $x \in K_x$ (из рефлексивности)
2. $K_x \cap K_y \neq \varnothing \Rightarrow K_x = K_y$. Пусть $z \in K_x \cap K_y$. Тогда $z \sim x \Rightarrow x \sim z$ и $z \sim y \Rightarrow x \sim y$. Пусть $t \in K_x$, тогда $t \sim x \Rightarrow t \sim y \Rightarrow t \in K_y$. Отсюда $K_x \subset K_y$. Аналогично $K_y \subset K_x \Rightarrow K_x = K_y$.
3. $y \in K_x, z \in K_x \Rightarrow y \sim z$.
4. $z \in K_x, t \in K_y, K_x \neq K_y \Rightarrow z \not\sim t$. Если же $z \sim t$, то по симметричности и транзитивности $x \sim y$.

□

1.21 Фактормножество

Определение 1.35. *Фактормножеством* $A/_\sim$ называется множество классов эквивалентности по отношению $\sim$. То есть

$$f\colon A \to A/_\sim, \quad f(x) = K_x,$$
$$x \sim y \Leftrightarrow f(x) = f(y).$$

1.22 Отношения (частичного) порядка

Определение 1.36. *Отношением (частичного) порядка* называется бинарное отношение, которое обладает (анти)рефлексивностью, антисимметричностью и транзитивностью.

Определение 1.37. Отношением (частичного) *линейного* порядка называется отношение (частичного) порядка, к которому добавили свойство полноты.

Определение 1.38. *Упорядоченным множеством* называется пара из множества и отношения порядка на нём.

Пример. $(A, \leqslant_A)$

1.23 Изоморфизм

Определение 1.39. $(A, \leqslant_A)$ изоморфно $(B, \leqslant_B)$, если существует биекция $f\colon A \to B$ такая, что $x \leqslant_A y \Leftrightarrow f(x) \leqslant_B f(y)$. Обозначается как $A \simeq B$.

1.24 Операции над упорядоченными множествами

▷ Сумма:

$(A, \leqslant_A) + (B, \leqslant_B) = (C, \leqslant_C)$. $C = A \sqcup B$, $x \leqslant_C y \Leftrightarrow \begin{bmatrix} x, y \in A, x \leqslant_A y, \\ x, y \in B, x \leqslant_B y, \\ x \in A, y \in B. \end{bmatrix}$

▷ Произведение (используется обратный лексикографический порядок):

$(A, \leqslant_A) \cdot (B, \leqslant_B) = (C, \leqslant_C)$, где $C = A \times B$ и $(a_1, b_1) \leqslant_C (a_2, b_2)$, если $\begin{bmatrix} b_1 <_B b_2, \\ b_1 = b_2, a_1 \leqslant_A a_2. \end{bmatrix}$

1.25 Плотный порядок

Определение 1.40. Порядок *плотен*, если $\forall x, y \mid x < y \Rightarrow \exists z \mid x < z < y$.

Пример. $\mathbb{Q}, \mathbb{R}$ обладают плотным порядком, а $\mathbb{N}, \mathbb{Z}$ не обладают.

Теорема 1.5. *Любые 2 счётных плотно линейно упорядоченных множества без наименьшего и наибольшего элементов изоморфны.*

Доказательство. По индукции построим инъекцию $f\colon A \to B$ и докажем, что она также сюръективна.

Оба множества счётны. Формально это означает существование биекций $g\colon A \to \mathbb{N}$ и $h\colon B \to \mathbb{N}$, но фактически для нас важно, что мы можем занумеровать элементы. Будем последовательно определять $f(a_0), f(a_1), \ldots$, тем самым построив f:

1. За базу положим $f(a_0) = b_0$.
2. Теперь мы на шаге определения $f(a_n)$, $n > 0$ и все предыдущие значения уже определены. Определим положение a_n среди $a_0, \ldots, a_{n-1}$ и рассмотрим 3 случая:
   (a) $a_n > \max\{a_0, \ldots, a_{n-1}\}$. В этом случае нам нужно такое свободное b_j, что
   $$b_j > \max\{f(a_0), \ldots, f(a_{n-1})\}$$
   Оно точно есть, так как B не имеет наибольшего элемента.
   (b) $a_n < \min\{a_0, \ldots, a_{n-1}\}$. Поступаем аналогично предыдущему случаю:
   $$b_j < \min\{f(a_0), \ldots, f(a_{n-1})\}$$
   (c) $\min\{a_0, \ldots, a_{n-1}\} < a_n < \max\{a_0, \ldots, a_{n-1}\}$. В таком случае найдём a_l и a_r, заданные следующим образом:
   $$a_l = \max\{a_q \mid q \in [0; n-1],\ a_q < a_n\}$$
   $$a_r = \min\{a_q \mid q \in [0; n-1],\ a_q > a_n\}$$
   Осталось выбрать b_j из свободных такое, что оно удовлетворяет условию:
   $$f(a_l) < b_j < f(a_r)$$
   Оно точно есть, так как множество B плотное.

Инъективность и гомоморфность f очевидна в силу построения. Если потребовать, что во всех случаях j - это минимальный подходящий номер, то мы получаем возможность доказать сюръективность от противного. Пусть есть b_t без прообраза, при этом t - минимальный такой номер, то есть для $b_0, \ldots, b_{t-1}$ прообразы нашлись. Тогда, выберем такой номер s, что если $f(a_n) \in \{b_0, \ldots, b_{t-1}\}$, то $n < s$. Это можно сделать, например, так: взять максимальный номер из прообразов $\{b_0, \ldots b_{t-1}\}$ и прибавить к нему единицу. Снова разберём 3 случая:

(a) $b_t > \max\{f(a_0), \dots, f(a_s)\}$. В таком случае, так как в A нету наибольшего элемента, найдётся $a_p > \max\{a_0, \dots, a_s\}$. Из всех таких a_p выберем элемент с минимальным номером. По построению, должно было оказаться

$$f(a_p) = b_t$$

(b) $b_t < \min\{f(a_0), \dots, f(a_s)\}$. Аналогично предыдущему случаю, выберем a_p с минимальным номером и $a_p < \min\{f(a_0), \dots, f(a_s)\}$. Опять получаем, что

$$f(a_p) = b_t$$

(c) $\min\{f(a_0), \dots, f(a_s)\} < b_t < \max\{f(a_0), \dots, f(a_s)\}$. Здесь b_t лежит между какими-то элементами $a_i, a_j \in \{a_0, \dots, a_s\}$. Так как A - плотное множество, то есть свободные элементы между ними, и среди таких мы снова должны взять с минимальным номером и положить

$$f(a_p) = b_t$$

по построению

Во всех трёх случаях было достигнуто противоречие. Стало быть, f - изоморфизм.

□

Пример. $\mathbb{Q}$, $\mathbb{Q} \cap (0; 1)$, $\mathbb{Q}_2 = \{\frac{k}{2^n} \mid k \in \mathbb{Z}, n \in \mathbb{N}\}$, $\mathbb{A}$ - алгебраические числа.

1.26 Предпорядки

Определение 1.41. Отношение предпорядка $\precsim$ — это рефлексивное и транзитивное отношение.

Определение 1.42. Отношение *полного* предпорядка — это такой предпорядок, что

$$\forall a, b \Rightarrow (a \precsim b) \vee (b \precsim a).$$

Из полноты следует рефлексиность. В экономике отношение полного предпорядка называется *рациональным предпочтением.*

Теорема 1.6. *(Структурная теорема) Назовём отношением безразличия следующее отношение:* $a \sim b := (a \precsim b) \wedge (b \precsim a)$*, тогда:*

Для любого отношения предпорядка отношение безразличия $\sim$ *— это отношение эквивалентности. При этом* $\precsim$ *задаёт отношение порядка на фактормножестве.*

Доказательство. Проверим $\sim$ на отношение эквивалентности:

1. $a \sim a$, так как $a \precsim a$ (рефлексивность).
2. $a \sim b = b \sim a$, так как конъюнкция симметрична.
3. $(a \sim b) \wedge (b \sim c) \Rightarrow \begin{Bmatrix} a \precsim b, & b \precsim c \\ b \precsim a, & c \precsim b \end{Bmatrix} \Rightarrow \begin{matrix} a \precsim c, \\ c \precsim a, \end{matrix} \Rightarrow a \sim c.$

□

Агрегирование

Определение 1.43. Пусть $\precsim_1, \ldots, \precsim_n$ - предпорядки на одном и том же множестве.

Агрегирование по большинству: $x \precsim y$, если $\#\{i \mid x \precsim_i y\} \geqslant \#\{i \mid x \succsim_i y\}$, где $\#$ означает количество.

Замечание. Может получиться нетранзитивное отношение. Таким примером служит цикл Кондорсе:

$$a \prec_1 b \prec_1 c,$$
$$b \prec_2 c \prec_2 a,$$
$$c \prec_3 a \prec_3 b.$$

Отсюда получим $a \prec b \prec c \prec a$.

Теорема 1.7 (об агрегировании по большинству)**.** *Агрегированием по большинству* ***на конечном множестве*** *можно получить любое рефлексивное полное отношение.*

Доказательство. Пусть мы хотим $x \prec y$. Добавим 2 порядка: $x <_1 y <_1 a_1 <_1 \cdots <_1 a_{n-2}$, а другое $a_{n-2} <_2 a_{n-3} <_2 \cdots <_2 a_1 <_2 x <_2 y$. □

Определение 1.44. Пусть $\preceq_1, \ldots, \preceq_n$ - предпорядки на одном и том же множестве.

Тогда их *агрегированием по большинству* назовём отношение, в котором

$$x \preceq y \Leftrightarrow (\forall i \in [1; n]\ x \preceq_i y)$$

Теорема 1.8 (об агрегировании консенсусом)**.** *Агрегирование порядков консенсусом — порядок. Агрегирование предпорядков консенсусом — тоже порядок.*

Теорема 1.9. *Любой предпорядок может быть получен агрегированием консенсусом полных предпорядков.*

1.27 Решётки (как упорядоченное множество)

Определение 1.45. Пусть задан некоторое частично упорядоченное множество $(A, \leqslant)$. Тогда, *верхняя грань* элементов x и y — любой z такой, что $z \geqslant x$ и $z \geqslant y$.

Определение 1.46. *Точная верхняя грань (супремум)* — такая верхняя грань, что она $\leqslant$ любой другой верхней грани.

Определение 1.47. *Точная нижняя грань (инфинум)* — такая нижняя грань, что она $\geqslant$ любой другой нижней грани.

Определение 1.48. *Решётка* — это частично упорядоченное множество, в котором у любых x и y, лежащих в нём, есть sup и inf.

Замечание. Необходимо и достаточно существования такой грани, что она сравнима со всеми остальными из того же типа (то есть верхними или нижними).

2 Основы комбинаторики и теории чисел

2.1 Правило сложения

Утверждение 2.1. *Пусть у нас есть множество A, содержащее n объектов, и B, содержащее m объектов. Тогда число способов выбрать 1 объект из A **или** один объект из B равно $n + m$.*

2.2 Правило умножения

Утверждение 2.2. *Пусть у нас есть множество A, содержащее n объектов, и B, содержащее m объектов. Тогда число способов выбрать 1 объект из A **и** один объект из B равно $n \cdot m$.*

2.3 Способы выбора объектов из множества

Размещения с повторениями

Определение 2.1. Числом $\bar{A}_n^k$ называется количество способов выбрать k элементов из множества n элементов так, что при этом нам **важен** порядок выбора и мы **допускаем** повторения элементов.

Замечание. Читается как «A из n по k с чертой».

Замечание. Размещение из k элементов с повторениями также называют *k-размещением с повторениями*.

Теорема 2.1.

$$\bar{A}_n^k = n^k.$$

Доказательство. Сколько способов выбрать i-й элемент ($1 \leqslant i \leqslant k$)? Ровно n. Мы последовательно выбираем 1-й, **и** 2-й, **и** 3-й, **и** ..., **и** k-й, то есть

$$\bar{A}_n^k = \underbrace{n \cdot \ldots \cdot n}_{\text{k раз}} = n^k.$$

□

Размещения без повторений

Определение 2.2. *Факториалом* числа $n > 0$ называют число

$$n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1.$$

При этом считают, что

$$0! = 1! = 1.$$

Определение 2.3. Числом A_n^k называется количество способов выбрать k элементов из множества n элементов так, что при этом нам **важен** порядок выбора и мы **не допускаем** повторения элементов.

Замечание. Читается как «A из n по k».

Замечание. Размещение из k элементов без повторений также называют *k-размещением без повторений*. При этом n-размещение без повторений называется *перестановкой*.

Теорема 2.2.

$$A_n^k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}.$$

Доказательство. Сколько способов выбрать i-й элемент ($1 \leqslant i \leqslant k$)? Мы можем взять лишь те элементы, которые ещё не брали. Таких $n-i+1$. Мы выбираем 1-й, **и** 2-й, **и** 3-й, **и** ..., **и** k-й, то есть

$$A_n^k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}.$$

□

Сочетания без повторений

Определение 2.4. Множество элементов, из которых составлен объект (то же множество, перестановка или размещение), называется *набором* или же *сочетанием*.

Определение 2.5. Числом C_n^k называется количество способов выбрать k элементов из множества n элементов так, что при этом нам **не важен** порядок выбора и мы **не допускаем** повторения элементов. (То есть количество различных наборов размера k, которые можно получить из n элементного множества).

Замечание. Читается как «C из n по k».

Замечание. Сочетание из k элементов без повторений также называют *k-сочетанием без повторений*.

Теорема 2.3.

$$C_n^k = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!}.$$

Доказательство. Для некоторого множества из n элементов мы знаем число k-размещений без повторений. При этом все размещения можно распределить по группам, где все имеют одинаковый набор. Сколько существует k-размещений из множества с k элементами?

$$A_k^k = \frac{k!}{0!} = k!.$$

Это значит, что всего различных наборов из множества n элементов будет

$$C_n^k = \frac{A_n^k}{A_k^k} = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!}.$$

□

Сочетания с повторениями

Определение 2.6. Числом $\bar{C}_n^k$ называется количество способов выбрать k элементов из множества n элементов так, что при этом нам **не важен** порядок выбора и мы **допускаем** повторения элементов. (Количество различных k-сочетаний с повторениями).

Теорема 2.4.

$$\bar{C}_n^k = C_{n+k-1}^k.$$

Доказательство. Поймём, что любой набор с повторениями определяется числами вхождений каждого элемента в данный набор. Для определённости будем считать, что мы работаем с множеством A:

$$A = \{a_1, \ldots, a_n\}.$$

Обозначим как u_i — число вхождений a_i в данный набор. Тогда сразу следует равенство

$$u_1 + \ldots + u_n = k.$$

Теперь построим последовательность нулей и единиц, которая однозначно задаст нам набор:

$$\underbrace{1\ldots1}_{u_1 \text{ раз}}0\underbrace{1\ldots1}_{u_2 \text{ раз}}0\ldots0\underbrace{1\ldots1}_{u_n \text{ раз}}.$$

То есть мы записываем между нулями-разделителями столько единиц, сколько у нас имеется a_i в наборе.

- ▷ Сколько всего нулей? Ответ: $n-1$.
- ▷ Сколько всего единиц? Ответ: k.
- ▷ Какова длина всей последовательности? Ответ: $n+k-1$.

При этом длина последовательности всегда одинакова. Давайте просто выберем k позиций среди $n+k-1$ в ней, куда мы поставим единицы, а в остальных местах будут нули. Тогда мы получим какую-то последовательность, которая точно описывает какой-то из наборов. Отсюда

$$\bar{C}_n^k = C_{n+k-1}^k.$$

□

2.4 Принцип Дирихле

Определение 2.7. Пусть у нас есть $n+1$ кролик и n клеток для них. Тогда абсолютно очевидно, что если мы заполним все клетки, то в одной из них будет 2 кролика. Это и называется *принципом Дирихле*. Более формально ещё можно сказать так:

Если у нас есть $nk+1$ объект и n ящиков, то в каком-нибудь ящике окажется не менее $k+1$ объектов.

Пример. У нас есть квадрат со стороной 2. Если мы выберем 5 произвольных точек на его границах или внутри него, то хотя бы 2 из них будут на расстоянии не более $\sqrt{2}$.

Доказательство. Разделим квадрат на 4 меньших со стороной 1. Тогда, по принципу Дирихле хотя бы в одном из таких квадратов будет 2 точки, а наибольшее расстояние между точками в квадрате — это его диагональ, то есть $\sqrt{1^2+1^2} = \sqrt{2}$ □

2.5 Бином Ньютона

Определение 2.8. *Биномом Ньютона* называется выражение

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}.$$

Доказательство. n-ю степень суммы можно записать в виде

$$(a+b)^n = \underbrace{(a+b)\cdot(a+b)\cdot\ldots\cdot(a+b)}_{n \text{ раз}}.$$

Чтобы получить слагаемое в сумме, мы должны последовательно выбрать из каждой скобки a или b. Любое слагаемое точно будет иметь вид

$$a^k \cdot b^{n-k}.$$

Более того, чтобы определить слагаемое, нам необходимо и достаточно знать, сколько a мы выбрали. При этом выбирать его можно в любых скобках, а это можно сделать C_n^k способами. Отсюда и формула

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}.$$

□

2.6 Свойства биномиальных коэффициентов

Теорема 2.5.

1. $C_n^k = C_n^{n-k}$;
2. $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$;
3. $C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^n = 2^n$;
4. $(C_n^0)^2 + \ldots + (C_n^n)^2 = C_{2n}^n$;
5. $C_{n+m-1}^{n-1} + \ldots + C_{n-1}^{n-1} = C_{n+m}^n = C_{n+m}^m$, $m \geqslant 0$.

Доказательство.

1. Выбрать k объектов из n - это то же самое, что оставить $n-k$ объектов из n.
2. Количество способов выбрать k-набор из n элементного множества уже известно: C_n^k. Заметим, что каждый набор либо содержит n-й элемент, либо нет. То есть все наборы можно разбить на 2 группы:
   (a) Все наборы, которые содержат n-й элемент. Помимо него в них ещё надо выбрать $k-1$ элемент, а стало быть, их всего C_{n-1}^{k-1} штук.
   (b) Все наборы, которые не содержат n-й элемент. То есть набор выбирается только из первых $n-1$ элементов. Отсюда их C_{n-1}^k штук.

Так как эти две группы в сумме составляют все возможные наборы, то и очевиден ответ

$$C_n^k = C_{n-1}^k + C_{n-1}^{k-1}.$$

3. Сколько существует подмножеств у множества n элементов? — 2^n. С другой стороны, каждое из этих подмножеств характеризуется своей мощностью, а число подмножеств, чья мощность i, равно C_n^i. Отсюда

$$\sum_{i=0}^{n} C_n^i = 2^n.$$

4. Рассмотрим всевозможные n-наборы из $2n$ элементного множества. Их C_{2n}^n штук. С другой стороны, пусть $i \in [0, \ldots, n]$ — количество элементов для набора, которые мы возьмём из первой части исходного множества. Тогда из второй части мы выберем $n - i$ элементов. В итоге, получим сумму

$$\sum_{i=0}^{n} C_n^i \cdot C_n^{n-i} = \sum_{i=0}^{n} \left(C_n^i\right)^2 = C_{2n}^n.$$

5. Давайте рассмотрим всевозможные m-сочетания с повторениями в множестве $A = \{a_1, \ldots, a_{n+1}\}$. Их $\bar{C}_{n+1}^m = C_{n+1+m-1}^m = C_{n+m}^m = C_{n+m}^n$ штук. С другой стороны, каждое сочетание принадлежит группе наборов, которые содержат $i \in [0, \ldots, m]$ элементов a_1. Отсюда

$$C_{n+m}^n = \sum_{i=0}^{m} \bar{C}_n^{m-i} = \sum_{i=0}^{m} C_{n+m-i-1}^{m-i} = \sum_{i=0}^{m} C_{n+m-i-1}^{(n+m-i-1)-(m-i)} = \sum_{i=0}^{m} C_{n+m-1-i}^{n-1}.$$

□

Замечание. Если расписать 5-е свойство для $n = 1, 2, 3, \ldots$, то можно получить сумму $1, 2, 3, \ldots$ степеней первых $m + 1$ натуральных чисел соответственно.

2.7 Полиномиальный коэффициент

У нас есть n_i объектов a_i для всех $i \in [1, \ldots, t]$. Сколько различных последовательностей можно составить, используя абсолютно все объекты?

Заметим, что у нас всегда одинаковая длина слова, равная n:

$$n = \sum_{i=1}^{t} n_i.$$

Чтобы собрать слово, будем последовательно расставлять все t групп объектов.

▷ Сколько мест есть для первой группы? Ответ: n.

▷ Сколько мест есть для второй группы? Ответ: $n - n_1$ (первую поставили первой).

▷ ⋮

▷ Сколько мест есть для последней группы? Ответ: $n - n_1 - \ldots - n_{t-1} = n_t$.

Очевидно, что для i-й группы происходит выбор n_i мест из тех, что остались не занятыми. В итоге имеем

$$P(n_1, n_2, \ldots, n_t) = C_n^{n_1} \cdot C_{n-n_1}^{n_2} \cdot C_{n-n_1-n_2}^{n_3} \cdot \ldots \cdot C_{n-n_1-\ldots-n_{t-1}}^{n_t} =$$
$$= \frac{n!}{n_1!(n-n_1)!} \cdot \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \cdot \frac{(n-n_1-n_2)!}{n_3!(n-n_1-n_2-n_3)!} \cdot \ldots \cdot \frac{(n-n_1-\ldots-n_{t-1})!}{n_t!(n-n_1-\ldots-n_t)!} =$$
$$= \frac{n!}{n_1! \cdot n_2! \cdot n_3! \cdot \ldots \cdot n_t! \cdot 0!} = \frac{n!}{n_1! \cdot n_2! \cdot n_3! \cdot \ldots \cdot n_t!}.$$

Определение 2.9. Число $P(n_1, \ldots, n_t)$ называют *полиномиальным коэффициентом.*

2.8 Полиномиальная формула

Определение 2.10. Бином Ньютона позволяет выяснить разложение любой степени для суммы двух элементов. Его обобщением на случай t переменных служит *полиномиальная формула.*

Теорема 2.6. *Полиномиальной формулой называется выражение*

$$(x_1 + \ldots + x_t)^n = \sum_{n_1+\ldots+n_t=n} P(n_1, \ldots, n_t) \cdot x_1^{n_1} x_2^{n_2} \cdot x_t^{n_t}.$$

Доказательство. Аналогично биному Ньютона распишем скобки:

$$(x_1 + \ldots + x_t)^n = \underbrace{(x_1 + \ldots + x_t) \cdot \ldots \cdot (x_1 + \ldots + x_t)}_{n \text{ раз}}.$$

Чтобы получить полное слагаемое, нам нужно выбрать из каждой скобки по одному объекту. Если его привести, то мы получим выражение вида

$$x_1^{n_1} \cdot \ldots \cdot x_t^{n_t}.$$

При этом верно равенство:

$$n_1 + \ldots + n_t = n,$$

где n_i значит то же, что и до этого: количество раз, сколько мы выбрали (имеем) x_i.

Несложно понять, что такое слагаемое мы могли получить разными способами - в зависимости от того, из каких скобок какие объекты мы брали. Количество различных способов набрать $n_1, n_2, \ldots, n_t$ из скобок определяется полиномиальным коэффициентом. Отсюда

$$(x_1 + \ldots + x_t)^n = \sum_{n_1+\ldots+n_t=n} P(n_1, \ldots, n_t) \cdot x_1^{n_1} \cdot \ldots \cdot x_t^{n_t}.$$

□

Сумма полиномиальных коэффициентов

Утверждение 2.3.

$$\sum_{n_1+\ldots+n_t=n} P(n_1, \ldots, n_t) = k^n.$$

Доказательство. Просто положим в полиномиальной формуле все $x_i = 1$. □

2.9 Формула включений и исключений

Пусть есть N элементов. Обозначим $N(\alpha_i)$ — количество элементов, обладающих свойством α_i. $N(\alpha_i')$ — количество элементов, не обладающих свойством α_i. Ну и понятно, что $N(\alpha_i, \alpha_j')$ — количество элементов, обладающих свойством α_i **и** не обладающих свойством α_j.

Теорема 2.7. *Если мы рассмотрим n свойств, которые мы можем приписать N объектам, то имеет место формула включений и исключений:*

$$N(\alpha_1', \ldots, \alpha_n') = N - N(\alpha_1) - \ldots - N(\alpha_n) + \\ + N(\alpha_1, \alpha_2) + \ldots + N(\alpha_{n-1}, \alpha_n) - \ldots + (-1)^n N(\alpha_1, \ldots, \alpha_n).$$

Доказательство. Воспользуемся математической индукцией

- ▷ База $n = 1$:
$$N(\alpha_1') = N - N(\alpha_1)$$
верность очевидна.

- ▷ Предположение индукции: формула включений и исключений верна **для любых** N **объектов и для любых** n **свойств**. Докажем, что она также верна и в случае $(n+1)$-го свойства для данного N.

  Применим предположение индукции для N объектов и свойствам $\alpha_1, \ldots, \alpha_n$:

  $$N(\alpha_1', \ldots, \alpha_n') = N - N(\alpha_1) - \ldots - N(\alpha_n) + \\ + N(\alpha_1, \alpha_2) + \ldots + N(\alpha_{n-1}, \alpha_n) - \ldots + (-1)^n N(\alpha_1, \ldots, \alpha_n).$$

  Теперь сделаем то же самое для $M \leqslant N$ объектов, которые точно обладают свойством α_{n+1}, и свойств $\alpha_1, \ldots, \alpha_n$.

  $$M(\alpha_1', \ldots, \alpha_n') = M - M(\alpha_1) - \ldots - M(\alpha_n) + \\ M(\alpha_1, \alpha_2) + \ldots + M(\alpha_{n-1}, \alpha_n) - \ldots + (-1)^n M(\alpha_1, \ldots, \alpha_n)$$

  В силу определения M также верно, что $M := N(\alpha_{n+1})$. То есть можно переписать последнее выражение в виде

  $$N(\alpha_1', \ldots, \alpha_n', \alpha_{n+1}) = N(\alpha_{n+1}) - N(\alpha_1, \alpha_{n+1}) - \ldots - N(\alpha_n, \alpha_{n+1}) + \\ N(\alpha_1, \alpha_2, \alpha_{n+1}) + \ldots + N(\alpha_{n-1}, \alpha_n, \alpha_{n+1}) - \ldots + (-1)^n N(\alpha_1, \ldots, \alpha_n, \alpha_{n+1}).$$

  Теперь вычтем полученное выражение из того, что было для всех N объектов:

  $$N(\alpha_1', \ldots, \alpha_n', \alpha_{n+1}') = N(\alpha_1', \ldots, \alpha_n') - N(\alpha_1', \ldots, \alpha_n', \alpha_{n+1}') = \\ = N - N(\alpha_1) - \ldots - N(\alpha_n) - N(\alpha_{n+1}) + \\ + N(\alpha_1, \alpha_2) + \ldots + N(\alpha_n, \alpha_{n+1}) - \ldots + (-1)^n N(\alpha_1, \ldots, \alpha_n, \alpha_{n+1}).$$

□

Замечание. По понятным причинам слагаемых, содержащих ровно k свойств, будет C_n^k.

Следствие. Пусть у нас есть множество $A = \{a_1, \ldots, a_n\}$. Рассмотрим все возможные m-размещения с повторениями из этого множества, при этом $m < n$. их $N := n^m$ штук. Положим их объектами для формулы включений и исключений и скажем, что $N(\alpha_i)$ — это все размещения, в которые **не** входит элемент a_i. Тогда, верны следующие утверждения:

$$N(\alpha_i) = (n-1)^m,$$
$$N(\alpha_i, \alpha_j) = (n-2)^m,$$
$$N(\alpha_1, \ldots, \alpha_n) = (n-n)^m = 0,$$
$$N(\alpha'_1, \ldots, \alpha'_n) = 0, \text{ так как } m < n.$$

По формуле включений и исключений имеем:

$$\sum_{k=0}^{n} (-1)^k \cdot C_n^k \cdot (n-k)^m = 0.$$

2.10 Основная теорема арифметики

Теорема 2.8. *Любое натуральное число единственным образом (с точностью до перестановки) представляется как*

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s},$$

где p_i — простое число (1 не является таковым), а также $\forall i$ $\alpha_i \geqslant 1$. Такой вид числа называется каноническим.

Замечание. Считается, что 1 не обладает каноническим видом.

Доказательство.

▷ Существование.

Доказывается по индукции n:

1. База $n = p$ - простое число. Верность очевидна.
2. Переход n - составное число. Это значит, что

$$\exists a, b \in (1; n) \mid n = a \cdot b$$

Так как $a, b \in (1; n)$, то для них верно предположение индукции. Разложив эти числа, получим разложение и для n.

▷ Единственность.

Предположим обратное, и рассмотрим минимальное из чисел, у которого есть как минимум 2 разложения на простые множители. Тогда, все множители в разложениях различны (иначе сократим и получим меньшее число с двумя разложениями, что противоречит предположению). Пусть они имеют вид:

$$n = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$$

где p_1 и q_1 - минимальные из всех сомножителей в своих разложениях. Не умаляя общности, положим $p_1 < q_1$. Тогда, рассмотрим число m:

$$m = (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_l$$

Докажем, что оно тоже имеет 2 разложения, вопреки предположению индукции. С одной стороны, m делится на p_1, так как выражение выше можно переписать в следующем виде:

$$m = q_1 \cdot \ldots \cdot q_l - p_1 \cdot q_2 \cdot \ldots \cdot q_l = p_1(p_2 \cdot \ldots \cdot p_k - q_2 \cdot \ldots \cdot q_l)$$

Отсюда следует, что у m есть разложение, содержащее p_1. С другой стороны, в изначальной записи m ни $q_1 - p_1$ не делится на p_1, ни любое $q_i \neq p_1$. Значит, разложив $q_1 - p_1$ на простые множители, мы придём к новому разложению, не содержащему p_1. Противоречие.

□

2.11 Функция Мёбиуса

Определение 2.11. *Функцией Мёбиуса* $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ называется функция

$$\mu(n) = \begin{cases} 1, \ n = 1, \\ 0, \ \exists \alpha_i \geqslant 2, \ 1 \leqslant i \leqslant s, \\ (-1)^s, \ n = p_1^1 \cdot \ldots \cdot p_s^1, \end{cases}$$

где n в каноническом виде выглядит как

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}.$$

Лемма 2.1. *Сумма значений функции Мёбиуса от натурального числа равна 1 для единицы и 0 для всех остальных чисел.*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, \ n = 1, \\ 0, n > 1. \end{cases}$$

Доказательство. Пусть n имеет канонический вид

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}.$$

Тогда d — делитель n, если

$$d = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s},$$

где $0 \leqslant \beta_i \leqslant \alpha_i$.

Это значит, что нашу сумму по делителям можно переписать как сумму по всем возможным наборам $\beta_1, \ldots, \beta_s \mid 0 \leqslant \beta_i \leqslant \alpha_i$:

$$\sum_{d|n} \mu(d) = \sum_{\substack{\beta_1, \ldots, \beta_s \\ 0 \leqslant \beta_i \leqslant \alpha_i}} \mu(d) = \sum_{\substack{\beta_1, \ldots, \beta_s \\ 0 \leqslant \beta_i \leqslant 1}} \mu(d).$$

Заметим, что теперь у нас только 2^s делителей, которые влияют на сумму в зависимости от того, сколько простых чисел они содержат. Следовательно,

$$\sum_{\substack{\beta_1,\ldots,\beta_s \\ 0\leqslant\beta_i\leqslant 1}} \mu(d) = 1 - C_s^1 + C_s^2 - \ldots + (-1)^s C_s^s = C_s^0 - C_s^1 + C_s^2 - \ldots + (-1)^s C_s^s = (1-1)^s = 0.$$

□

Теорема 2.9. *(Обращение Мёбиуса) Пусть задана* $f\colon \mathbb{N} \to \mathbb{R}$. *Определим* g*:*

$$g(n) := \sum_{d|n} f(d).$$

Тогда

$$f(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right).$$

Доказательство. Распишем сумму:

$$\sum_{d|n} \mu(d) \cdot g(n/d) = \sum_{d|n} \mu(d) \cdot \sum_{d'|\frac{n}{d}} f(d').$$

Выбрать d такое, что $d \mid n$ и потом выбрать $d' \mid \frac{n}{d}$ — это то же самое, что выбрать пару $(d, d') : d \cdot d' \mid n$. Отсюда

$$\sum_{d|n} \mu(d) \cdot \sum_{d'|\frac{n}{d}} f(d') = \sum_{dd'|n} \mu(d) \cdot f(d') = \sum_{d'd|n} \mu(d') \cdot f(d) = \sum_{d|n} f(d) \cdot \sum_{d'|\frac{n}{d}} \mu(d') =$$

$$= f(n) + \sum_{\substack{d:d|n \\ d<n}} f(d) \cdot \underbrace{\sum_{d'|\frac{n}{d}} \mu(d')}_{0} = f(n).$$

Последний переход следует из доказанной выше леммы. □

2.12 Циклические слова

Определение 2.12. Пусть задан алфавит $X = \{b_1, \ldots, b_r\}$ и число $n \in \mathbb{N}$. Тогда *линейным словом длины* n называется последовательность букв из алфавита

$$a_1, \ldots, a_n.$$

Пусть V — это множество всех линейных последовательностей длины $n \in \mathbb{N}$ над алфавитом X, $|X| = r$. Очевидно, что

$$|V| = r^n.$$

Определение 2.13. *Сдвиг* — это операция, которая переводит линейное слово $a_1, \ldots, a_n$ в слово $a_2, \ldots, a_n, a_1$.

Определение 2.14. Объединим слова, получающиеся из данного при помощи сдвига, в один класс эквивалентности. Тогда этот класс называется *циклическим словом.*

Определение 2.15. *Период линейной последовательности* — это минимальное число сдвигов d, которое переводит линейное слово само в себя.

Лемма 2.2. *Если d — период линейного слова длины n, то $d \mid n$.*

Доказательство. Предположим обратное. Тогда n можно представить в виде

$$n = kd + b,\ 0 < b < d.$$

Тогда, раз d — период, то после kd сдвигов слово перейдёт в себя. То же самое верно и для $n = kd + b$ сдвигов. Но это значит, что слово переходит в себя и за $(kd + b) - kd = b < d$ сдвигов, противоречие. □

Лемма 2.3. *Любая последовательность длины n и периода d имеет вид*

$$a_1, \ldots, a_d, a_1, \ldots, a_d, \ldots, a_1, \ldots, a_d$$

Доказательство. Пусть мы сделали $kd < n$ сдвигов некоторого слова. Тогда, на его первых d позициях стоит слово

$$a_{kd+1}, \ldots, a_{kd+d}.$$

Раз полученное и текущее слова равны, то

$$a_i = a_{kd+i},\ 1 \leqslant i \leqslant d.$$

□

Теорема 2.10. *Если $T_r(n)$ — это количество циклических слов длины n над алфавитом X, $|X| = r$. Тогда*

$$T_r(n) = \sum_{d|n} \frac{1}{d} \left(\sum_{d'|d} \mu(d') r^{d/d'} \right).$$

Доказательство. Пусть $\{d_1, \ldots, d_s\}$ — это все делители числа $n \in \mathbb{N}$. Тогда множество V можно представить как объединение множеств слов V_i длины n с одинаковым периодом d_i:

$$V = V_1 \sqcup \ldots \sqcup V_s,$$
$$|V| = |V_1| + \ldots + |V_s|.$$

Обозначим за W_i — множество слов длины d_i с периодом d_i. Понятно, что

$$|W_i| = |V_i| \Rightarrow |V| = |W_1| + \ldots + |W_s|$$

Ещё введём понятие U_i — это множество циклических слов длины d_i и периодом d_i. Тогда

$$|W_i| = d_i \cdot |U_i|.$$

И обозначим $|U_i| =: M(d_i)$. Теперь $|V|$ можно записать как

$$|V| = r^n = \sum_{i=1}^{s} d_i |U_i| = \sum_{d|n} d \cdot M(d).$$

Заметим, что если ввести функции

$$f(n) = r^n,$$
$$g(n) = n \cdot M(n),$$

то $M(n)$ можно посчитать через обращение Мёбиуса:

$$g(n) = \sum_{d|n} \mu(d) \cdot f(n/d),$$
$$M(n) = \frac{1}{n} \sum_{d|n} \mu(d) \cdot r^{n/d}.$$

Отсюда получаем

$$T_r(n) = \sum_{d|n} M(d) = \sum_{d|n} \frac{1}{d} \left(\sum_{d'|d} \mu(d') r^{d/d'} \right)$$

□

2.13 Обобщённая Мёбиуса

Определение 2.16. *Функцией Мёбиуса на частично упорядоченном множестве* (ЧУМе) $\langle \mathcal{P}, \preceq \rangle$ называется функция μ, определяемая как

$$\mu(x, y) = \begin{cases} 1, \ x = y, \\ -\sum\limits_{x \preceq z \prec y} \mu(x, z), \ x \prec y. \end{cases}$$

При этом считается, что $\forall y \in \mathcal{P}$ существует лишь конечное число $x \in \mathcal{P}$ таких, что $x \preceq y$.

Теорема 2.11. *(Связь между обобщённой и стандартной функцией Мёбиуса) Переобозначим стандартную функцию Мёбиуса за $\hat{\mu}$. Тогда, если $\langle \mathcal{P}, \preceq \rangle = \langle \mathbb{N}, | \rangle$, то*

$$\mu(y, x) = \hat{\mu}\left(\frac{x}{y}\right).$$

Доказательство. Докажем теорему при помощи индукции по $\frac{x}{y}$:

▷ База: $\frac{x}{y} = 1 \Rightarrow x = y$. Тогда

$$\mu(x, x) = 1 = \hat{\mu}(1) \text{ — верно.}$$

▷ Переход: $y \prec x \Leftrightarrow y | x$ и $y \neq x$. Значит

$$x = y \cdot p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}, \ \alpha_i \geqslant 1.$$

Тогда

$$\mu(y, x) = -\sum_{y \preceq z \prec x} \mu(y, z).$$

Из определения z следует, что $\frac{z}{y} < \frac{x}{y}$. То есть мы можем применить предположение индукции:

$$\mu(y,x) = -\sum_{y \preceq z \prec x} \hat{\mu}\left(\frac{z}{y}\right).$$

Так как $y \preceq z$, то z содержит в себе правую часть из выражения x и можно записать следующее:

$$\mu(y,x) = -\sum_{\substack{0 \leqslant \beta_i \leqslant \alpha_i \\ \exists j : \beta_j < \alpha_j}} \hat{\mu}(p_1^{\beta_1} \dots p_s^{\beta_s}).$$

Рассмотрим частный случай, когда $(a_1, \dots, a_s) = (1, \dots, 1)$. Тогда значения кортежа $(\beta_1, \dots, \beta_s)$ являются битовым представлением числа от 0 до $2^s - 2$. Отсюда имеем:

$$\mu(y,x) = -\sum_{\substack{0 \leqslant \beta_i \leqslant 1 \\ \exists \beta_j = 0}} \hat{\mu}(p_1^{\beta_1} \dots p_s^{\beta_s}) = -\sum_{k=0}^{s-1} (-1)^k \cdot C_s^k = -\left(0 - (-1)^s \cdot C_s^s\right) = (-1)^s = \hat{\mu}\left(\frac{x}{y}\right).$$

Теперь докажем другой случай, когда $\exists \alpha_j \geqslant 2$: если рассматривать z такое, что в нём содержится $\beta_j \geqslant 2$, то всё слагаемое сразу будет ноль. Значит снова $0 \leqslant \beta_i \leqslant 1$, при этом кортеж уже может быть представлением числа $2^s - 1$:

$$\mu(y,x) = -\sum_{0 \leqslant \beta_i \leqslant 1} \hat{\mu}(p_1^{\beta_1} \dots p_s^{\beta_s}) = -\sum_{k=0}^{s} (-1)^k C_s^k = 0 = \hat{\mu}\left(\frac{x}{y}\right).$$

□

Теорема 2.12. *(Обобщённое обращение Мёбиуса) Пусть $\langle \mathcal{P}, \preceq \rangle$ — некоторый ЧУМ. Пусть $f \colon \mathcal{P} \to \mathbb{C}$, $g(x) := \sum\limits_{y \preceq x} f(y)$. Тогда*

$$f(x) = \sum_{y \preceq x} \mu(y,x) g(y).$$

Лемма 2.4.

$$\sum_{x \preceq y \preceq z} \mu(y,z) = \mathbb{I}_{x=z} = \begin{cases} 1, & x = z, \\ 0, & x \neq z. \end{cases}$$

Доказательство.

1. Если $x = z$, то
$$\sum_{x \preceq y \preceq z} \mu(y,z) = \mu(x,z) = 1.$$

2. Иначе $x \prec z$. Проведём доказательство индукция по длине максимальной цепи вида
$$x \prec \dots \prec \dots \prec z.$$

   (a) База: такая цепочка имеет длину 2, то есть вида $x \prec z$,
   $$\sum_{x \preceq y \preceq z} \mu(y,z) = \mu(x,z) + \mu(z,z) = \left(-\sum_{x \preceq w \prec z} \mu(x,w)\right) + 1 = 0.$$

(b) Переход: цепочка имеет длину $\geqslant 3$, а для меньших уже доказано:

$$\sum_{x\preceq y\preceq z}\mu(y,z)=\sum_{x\preceq y\prec z}\mu(y,z)+\mu(z,z)=1-\sum_{x\preceq y\prec z}\sum_{y\preceq u\prec z}\mu(y,u)=1-\sum_{x\preceq y\preceq u\prec z}\mu(y,u)=$$
$$=1-\sum_{x\preceq u\prec z}\sum_{x\preceq y\preceq u}\mu(y,u)=1-\sum_{x\preceq y\preceq x}\mu(y,x)-\sum_{x\prec u\prec z}\sum_{x\preceq y\preceq u}\mu(y,u).$$

Так как в последнем слагаемом $x\prec u\prec z$, то максимальная цепочка, соединяющая x и u, короче, чем x и z. Значит, можно воспользоваться предположением индукции:

$$\sum_{x\preceq y\preceq u}\mu(y,u)=\mathbb{I}_{x=u}=0,$$

то есть

$$\sum_{x\preceq y\preceq z}\mu(y,z)=1-1-0=0.$$

□

Доказательство. (Теоремы 2.12) Поступаем аналогично стандартной функции Мёбиуса:

$$\sum_{y\preceq x}\mu(y,x)g(y)=\sum_{y\preceq x}\mu(y,x)\sum_{z\preceq y}f(z)=\sum_{z\preceq y\preceq x}\mu(y,x)f(z)=\sum_{z\preceq x}f(z)\cdot\sum_{z\preceq y\preceq x}\mu(y,x)=$$
$$=f(x)+\sum_{z\prec x}f(z)\cdot\underbrace{\sum_{z\preceq y\preceq x}\mu(y,x)}_{0}=f(x).$$

□

Теорема 2.13. *Рассмотрим ЧУМ* $\langle 2^{\{1,\dots,n\}},\subseteq\rangle$. *Утверждается, что*

$$\mu(X,Y)=(-1)^{|Y|-|X|},\ X\subseteq Y.$$

Доказательство. Воспользуемся индукцией по $|Y|-|X|$:

1. База: $|X|=|Y|\Leftrightarrow X=Y$, а значит:

$$\mu(X,Y)=\mu(X,X)=1=(-1)^{|Y|-|X|}.$$

2. Шаг: $|Y|>|X|\Leftrightarrow Y\supset X$

$$\mu(X,Y)=-\sum_{X\subseteq Z\subset Y}\mu(X,Z)=-\sum_{X\subseteq Z\subset Y}(-1)^{|Z|-|X|}=-\sum_{k=|X|}^{|Y|-1}(-1)^{k-|X|}\cdot C_{|Y|-|X|}^{k-|X|}=$$
$$=-\sum_{m=0}^{|Y|-|X|-1}C_{|Y|-|X|}^{m}\cdot(-1)^m=-(0-(-1)^{|Y|-|X|})=(-1)^{|Y|-|X|}.$$

□

2.14 Доказательство формулы включений и исключений через обращение Мёбиуса

Рассмотрим произвольные множества $A_1, \ldots, A_n$, при этом $A = \bigcup_{i=1}^{n} A_i$ и дополнительно рассмотрим ЧУМ $\langle 2^{\{1,\ldots,n\}}, \subseteq \rangle$.

Введём функцию $f(\{i_1, \ldots, i_k\})$, $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ — количество элементов множества A, которые **могут** принадлежать множествам $A_{i_1}, \ldots, A_{i_k}$ **и точно принадлежат всем остальным**. Тогда

$$f(\{1, \ldots, n\}) = |A|,$$
$$f(\{i_1, \ldots, i_k\}) = \left| \bigcap_{i \notin \{i_1, \ldots, i_k\}} A_i \right|, \quad \{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}.$$

Ещё нам нужна функция $g(\{i_1, \ldots, i_k\})$ — количество элементов множества A, которые **не принадлежат** $A_{i_1}, \ldots, A_{i_k}$, **но принадлежат всем остальным**. Тогда, если обозначить за $I = \{i_1, \ldots, i_k\}$, получим

$$f(I) = \sum_{I' \subseteq I} g(I').$$

Коль скоро у нас определена функция Мёбиуса на ЧУМе $\langle 2^{\{1,\ldots,n\}}, \subseteq \rangle$, мы можем воспользоваться общим обращением Мёбиуса и получить выражение для $g(I)$:

$$g(I) = \sum_{I' \subseteq I} \mu(I', I) f(I') = \sum_{I' \subseteq I} (-1)^{|I| - |I'|} f(I')$$

Рассмотрим случай, когда $I = \{1, \ldots, n\}$:

$$g(\{1, \ldots, n\}) = 0 = \sum_{I' \subseteq I} (-1)^{n - |I'|} f(I') = |A| + \sum_{I' \subset I} (-1)^{|I| - |I'|} f(I').$$

Отсюда

$$|A| = -\sum_{I' \subset I} (-1)^{|I| - |I'|} f(I') = \sum_{I' \subset I} (-1)^{|I| - |I'| + 1} f(I').$$

Сделаем замену $J = I \backslash I'$:

$$|A| = |A_1 \cup \ldots \cup A_n| = \sum_{J \neq \varnothing} (-1)^{|J| + 1} f(J).$$

Последнее выражение есть ничто иное, как формула включений и исключений.

2.15 Разбиение чисел на слагаемые

Общая постановка задачи формулируется так: дано число $n \in \mathbb{N}$ (без нуля). Необходимо найти разбиения числа n на слагаемые так, что $n = x_1 + \ldots + x_t$, при условии, что ограничения на x_i и на число t известны.

Самый первый вопрос в такой задаче — считаем ли мы разбиения равными при одинаковом наборе слагаемых, или же их порядок важен.

Разбиение чисел на слагаемые с учётом порядка

Решим поставленную задачу в предположении, когда у нас нет ограничений на t, но зато $\forall i \in [1;t]\ x_i \in \{n_1, \ldots, n_k\}$.

Введём функцию $f(n; n_1, \ldots, n_k)$ — количество разбиений числа n, удовлетворяющих условиям задачи.

Теорема 2.14. *Количество разбиений числа n можно вычислить рекурсивно:*

$$f(n; n_1, \ldots, n_k) = f(n - n_1; n_1, \ldots, n_k) + \ldots + f(n - n_k; n_1, \ldots, n_k)$$

Базой при этом являются утверждения:

$$f(0; n_1, \ldots, n_k) = 1,$$
$$f(a < 0; n_1, \ldots, n_k) = 0.$$

Доказательство. База очевидна. Основное равенство в теореме следует из того, что нам важен порядок и мы просто суммируем все случаи, где на первое место разложения было поставлено n_i. □

Следствие. $k(n)$ — это число разбиений числа n на слагаемые, каждое из которых лежит в диапазоне $[1;n]$. Тогда

$$k(n) = f(n; 1, \ldots, n) = 2^{n-1}.$$

Доказательство. Можно просто доказать по индукции полученную формулу, используя теорему 2.14. Но как вывести данную формулу?

Число n — это сумма n единиц. Любое разбиение можно записать в виде

$$n = (1 + \ldots + 1)_{x_1} + \ldots + (1 + \ldots + 1)_{x_t}.$$

Давайте упростим нашу запись: уберём все плюсы и оставим просто n единиц. Тогда, у нас есть $n - 1$ позиция между единицами, куда мы можем поставить перегородку и тем самым разбить единицы на группы — слагаемые. Любая из $n-1$ перегородок может быть как поставлена, так и нет. Значит, всего 2^{n-1} разбиений. □

Разбиение чисел на слагаемые без учёта порядка

Решим поставленную задачу в том же предположении, когда у нас нет ограничений на t, но зато $\forall i \in [1;t]\ x_i \in \{n_1, \ldots, n_k\}$.

Теперь введём функцию $F(n; n_1, \ldots, n_k)$ — количество разбиений числа n, удовлетворяющих условиям задачи.

Теорема 2.15. *Количество разбиений числа n можно вычислить рекурсивно:*

$$F(n; n_1, \ldots, n_k) = F(n - n_1; n_1, \ldots, n_k) + F(n; n_2, \ldots, n_k).$$

Базой при этом являются утверждения:

$$F(0; n_1, \ldots, n_k) = 1,$$
$$F(a; \varnothing) = 0,$$
$$F(a < 0; n_1, \ldots, n_k) = 0.$$

Доказательство. База очевидна. Формула же следует из рассуждений для набора: данное разбиение содержит n_1 в своём наборе или нет? Если да, то спускаемся по первому слагаемому. Иначе идём по второму. □

Замечание. Понятно, что

$$p(n) = F(n; 1, \ldots, n) < 2^{n-1}.$$

Точной формулы у данной функции нет, а вот её асимптотику изучали Сриниваса Рамануджан, Годфри Харди и Джон Литлвуд. Было получено утверждение

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2}{3}}\sqrt{n-\frac{1}{24}}}, \quad n \to .\infty.$$

Диаграммы Юнга

Продолжим говорить про задачу с неупорядоченными разбиениями. Пусть у нас есть некоторое разбиение числа n:

$$n = x_1 + \ldots + x_t.$$

Раз порядок не важен, то для удобства его можно потребовать

$$x_1 \leqslant x_2 \leqslant \ldots \leqslant x_t.$$

Теперь просто будем говорить, что разбиение, которое удовлетворяет данному условию, будет представителем класса эквивалентных разбиений (то есть таких, у которых набор слагаемых одинаков).

Несложно понять, как визуализировать данное представление — это просто пирамидка из кубиков, где число кубиков на каждом слое соответствует своему слагаемому:

Здесь должна быть картинка, которая когда-нибудь возможно появится. Можно в гугле найти.

Замечание. В теоремах ниже полагается, что разбиение рассматривается без учёта порядка.

Теорема 2.16. *Количество разбиений числа n на не более k слагаемых равно количеству разбиений числа $n + k$ на ровно k слагаемых.*

Доказательство. Нарисуем диаграммы Юнга для какого-то произвольного случая.

Несложно заметить, что если мы добавим слева столбец высоты k к любой диаграмме Юнга, соответствующей разбиению числа n, то получим диаграмму Юнга для разбиения $n + k$. □

Теорема 2.17. *Количество разбиений числа n на не более k слагаемых равно количеству разбиений числа $n + \frac{k(k+1)}{2}$ на ровно k различных слагаемых.*

Доказательство. Нарисуем диаграммы Юнга: идея в том, чтобы сложить диаграмму справа с треугольником высоты k и длиной первого слоя $k + 1$. □

Теорема 2.18. *Количество разбиений числа n на не более k слагаемых равно количеству разбиений числа n на слагаемые, величина каждого из которых не более k.*

Доказательство. Надо просто транспонировать диаграмму Юнга для числа n: □

Формальный ряд

Рассмотрим как чисто алгебраическое выражение следующее бесконечное произведение:

$$\prod_{n=1}^{\infty}(1-x^n) = (1-x)(1-x^2)(1-x^3)(1-x^4)\dots$$

Мы **не будем подставлять никаких** x. Мы просто хотим раскрыть данное выражение и посмотреть, что получится.

Утверждение 2.4. *Если раскрыть все скобки, то получится выражение*

$$\prod_{n=1}^{\infty}(1-x^n) = 1 - x - x^2 + x^5 + x^7 - \dots$$

Как получается любое слагаемое, отличное от 1? Если оно имеет степень n, то оно задаётся выражением

$$(-x^{n_1})(-x^{n_2})\dots(-x^{n_t}) = (-1)^t x^n$$

То есть оно получается путём набора степени n из t скобок, где возьмём x^{n_i} (в остальных выбираем 1). В силу рассматриваемого бесконечного произведения, верно 2 утверждения:

$$n = n_1 + \dots + n_t,$$
$$\forall i, j \in [1;t] \quad n_i \neq n_j.$$

При этом нам не важен порядок, в котором мы выбираем множители из скобок.

Выражение, которое записано справа в утверждении 2.4, является приведённым многочленом. Можно ли как-то сказать, какие x^n останутся и с каким коэффициентом (до этого мы говорили об элементарном слагаемом, которое получается при раскрытии без приведения)?

Теорема 2.19. *Если* $n \neq \frac{3k^2 \pm k}{2}$ *ни при каком* k, *то коэффициент при* x^n *равен нулю. Иначе равен* $(-1)^k$.

Из этой теоремы можно получить ещё одну для разбиений числа n. Обозначим за $n_{\text{чёт}}$ — количество разбиений числа n на чётное число различных слагаемых, и еще введём $n_{\text{нечёт}}$.

Теорема 2.20. *Если* $n \neq \frac{3k^2 \pm k}{2}$ *для любых* k, *то* $n_{чёт} = n_{нечёт}$. *Иначе* $n_{чёт} - n_{нечёт} = (-1)^k$.

2.16 Линейные рекуррентные соотношения с постоянными коэффициентами

Замечание. Далее: $\mathbb{N} = \{0, 1, 2\dots\}$.

Определение 2.17. Последовательность $\{y_n\}_{n=0}^{\infty}$ удовлетворяет *линейному рекуррентному соотношению (ЛРС) k-го порядка с постоянными коэффициентами*, если для любого $n \in \mathbb{N}$ верно:

$$a_k \cdot y_{n+k} + a_{k-1} \cdot y_{n+k-1} + \dots + a_1 \cdot y_{n+1} + a_0 \cdot y_n = 0,$$

где $a_0, \dots, a_k \in \mathbb{C}$, $a_k \neq 0$, $a_0 \neq 0$.

Замечание. Последовательность задана однозначно, если заданы конкретные числа $y_0, \ldots, y_{k-1}$.

Ключевой вопрос: можно ли написать явную формулу для y_n?

Утверждение 2.5. *Для линейных рекуррентных соотношений любого порядка существует общая формула.*

1. $k = 1$, $a_0, a_1 \in \mathbb{C}$:
$$a_1 y_{n+1} + a_0 y_n = 0.$$
Или же
$$y_{n+1} = \left(-\frac{a_0}{a_1}\right) y_n.$$
Несложно понять и доказать общую формулу:
$$y_n = y_0 \cdot \left(-\frac{a_0}{a_1}\right)^n.$$

2. $k = 2$, $a_0, a_1, a_2 \in \mathbb{C}$:
$$a_2 y_{n+2} + a_1 y_{n+1} + a_0 y_n = 0.$$
Составим *характеристическое уравнение*:
$$a_2 x^2 + a_1 x + a_0 = 0.$$
Просто заменили все y_i на x^i. Решений у полученного уравнения всегда 2 в поле $\mathbb{C}$. Введём обозначения для этих корней λ_1 и λ_2.

Теорема 2.21. *Пусть $\lambda_1 \neq \lambda_2$. Тогда*

(a) $\forall c_1, c_2 \in \mathbb{C}$ последовательность $y_n = c_1\lambda_1^n + c_2\lambda_2^n$ является решением данного ЛРС.

(b) Если $\{y_n\}_{n=0}^{\infty}$ удовлетворяет данному ЛРС, то $\exists c_1, c_2 \mid y_n = c_1\lambda_1^n + c_2\lambda_2^n$.

Доказательство.

(a) Подставим выражение для y_n в левую часть ЛРС:
$$a_2(c_1\lambda_1^{n+2} + c_2\lambda_2^{n+2}) + a_1(c_1\lambda_1^{n+1} + c_2\lambda_2^{n+1}) + a_0(c_1\lambda_1^n + c_2\lambda_2^n) =$$
$$= c_1\lambda_1^n \underbrace{(a_2\lambda_1^2 + a_1\lambda_1 + a_0)}_{0} + c_2\lambda_2^n \underbrace{(a_2\lambda_2^2 + a_1\lambda_2 + a_0)}_{0} = 0$$

(b) Мы знаем, что $\{y_n\}_{n=0}^{\infty}$ удовлетворет ЛРС. Составим систему
$$\begin{cases} c_1 + c_2 = y_0, \\ c_1\lambda_1 + c_2\lambda_2 = y_1. \end{cases}$$
Определитель её матрицы равен $\Delta = \lambda_2 - \lambda_1 \neq 0$. Значит, решение c_1^*, c_2^* существует и единственно. Рассмотрим последовательность $y_n^* = c_1^*\lambda_1^n + c_2^*\lambda_2^n$. При этом уже по первому пункту y_n^* тоже является решением ЛРС. Более того, $y_0 = y_0^*$ и $y_1 = y_1^*$. Таким образом, последовательности y_n и y_n^* совпадают.

□

Пример. Последовательность Фибоначчи задаётся ЛРС второго порядка:

$$F_{n+2} - F_{n+1} - F_n = 0, \;\; F_0 = 0, \, F_1 = 1.$$

Характеристическим уравнением будет

$$x^2 - x - 1 = 0.$$

Корни $\lambda_{1,2} = \frac{1 \pm \sqrt{5}}{2}$. Отсюда общая формула

$$F_n = c_1 \left(\frac{1 + \sqrt{5}}{2} \right)^n + c_2 \left(\frac{1 - \sqrt{5}}{2} \right)^n,$$

где $c_{1,2}$ находятся из выбранных начальных значений.

Теорема 2.22. *Пусть $\lambda := \lambda_1 = \lambda_2$. Тогда*

(a) $\forall c_1, c_2 \in \mathbb{C}$ *последовательность* $y_n = (c_1 n + c_2)\lambda^n$ *является решением данного ЛРС.*

(b) Если $\{y_n\}$ *является решением, то* $\exists c_1, c_2 \in \mathbb{C} \;\big|\; y_n = (c_1 n + c_2)\lambda^n$.

Доказательство.

(a) Подставим выражение y_n в левую часть ЛРС:

$$a_2(c_1(n+2) + c_2)\lambda^{n+2} + a_1(c_1(n+1) + c_2)\lambda^{n+1} + a_0(c_1 n + c_2)\lambda^n = \\ \lambda^n \left(c_1 n(a_2\lambda^2 + a_1\lambda + a_0) + c_2(a_2\lambda^2 + a_1\lambda + a_0) + a_2 \cdot 2c_1 \cdot \lambda^2 + a_1 \cdot c_1 \cdot \lambda \right) = \\ \lambda^n \left(c_1\lambda(2a_2\lambda + a_1) \right)$$

При этом мы воспользовались тем, что

$$a_2\lambda^2 + a_1\lambda + a_0 = 0$$

Значит, по теореме Виета:

$$2\lambda = -\frac{a_1}{a_0} \Rightarrow 2a_2\lambda + a_1 = 0$$

Отсюда следует, что и оставшееся выражение тоже обнуляется. Следовательно, наша последовательность является решением данного ЛРС.

(b) Абсолютно аналогично случаю $\lambda_1 \neq \lambda_2$.

□

3. Общий случай $a_0, \ldots, a_k \in \mathbb{C}$, $a_k \neq 0$, $a_0 \neq 0$:

$$a_k y_{n+k} + a_{k-1} y_{n+k-1} + \ldots + a_1 y_{n+1} + a_0 y_n = 0$$

Так же, как и для $k = 2$, составим характеристическое уравнение:

$$a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0 = 0$$

Слева записано не что иное, как многочлен степени k. Если обозначить за $P_m(x)$ - произвольный многочлен степени *не выше* m от x, то выражение перепишется как

$$P_k(x) = 0$$

Согласно основной теореме алгебры, у любого многочлена с комплексными коэффициентами степени k существует ровно k комплексных корней (не обязательно разных), то есть

$$\exists \lambda_1, \ldots, \lambda_k \in \mathbb{C} \mid P_k(x) = a_k(x - \lambda_1) \cdot \ldots \cdot (x - \lambda_k)$$

Разобьём эти k корней на r групп совпадающих. Представителей групп переобозначим как $\mu_1, \ldots, \mu_r$, а размеры групп обозначим за $m_1, \ldots, m_r$.

Теорема 2.23.

(a) Для любых многочленов $P_{m_1-1}(n), \ldots, P_{m_r-1}(n)$ последовательность $\{y_n\}_{n=0}^{\infty}$ вида:

$$y_n = P_{m_1-1}(n) \cdot \mu_1^n + \ldots + P_{m_r-1}(n) \cdot \mu_r^n$$

удовлетворяет решению данного ЛРС.

(b) Если $\{y_n\}_{n=0}^{\infty}$ удовлетворяет решению данного ЛРС, то существуют многочлены $P_{m_1-1}(n), \ldots, P_{m_r-1}(n)$ такие, что можно выписать y_n в общем виде, описанном выше.

Доказательство. Оставляется читателю в качестве домашнего задания (не входит в читаемый курс). □

2.17 Степенные ряды и производящие функции

Формальный степенной ряд

Определение 2.18. Мы уже рассматривали бесконечный многочлен вида:

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots$$

И нам не очень понравилось то, что здесь есть x, вместо которого возможно что-то подставить. Вместо этого, мы можем рассмотреть просто бесконечную последовательность чисел:

$$(a_0, a_1, \ldots, a_n, \ldots), \quad \forall n \in \mathbb{N}\ a_n \in \mathbb{C}$$

Такую последовательность мы и будем называть *формальным степенным рядом* (ФРС).

Дополнительно введём обозначение A_i для формального степенного ряда A, обозначающее i-ое число в последовательности.

Арифметические операции над формальным степенным рядом

Теперь можно определить операции над формальными степенными рядами:

- ▷ Пусть есть 2 формальных степенных ряда $A = (a_0, \ldots, a_n, \ldots)$ и $B = (b_0, \ldots, b_n, \ldots)$. Тогда назовём их *суммой* формальный степенной ряд $A + B$:

$$A + B = (a_0 + b_0, \ldots, a_n + b_n, \ldots)$$

- ▷ Пусть есть 2 формальных степенных ряда A и B. Тогда назовём их *произведением* формальный степенной ряд $A \cdot B$ такой, что

$$(A \cdot B)_n = A_n B_0 + A_{n-1} B_1 + \ldots + A_0 B_n = \sum_{i=0}^{n} A_{n-i} B_i = \sum_{i=0}^{n} A_i B_{n-i}$$

- ▷ Пусть есть 2 формальных степенных ряда A и B. Тогда возможно осуществить *деление* $A/B = C$, если существует формальный степенной ряд C такой, что $C \cdot B = A$. Для нахождения чисел C необходимо последовательно решать уравнения из системы:

$$\begin{cases} c_0 b_0 = a_0 \\ c_0 b_1 + c_1 b_0 = a_1 \\ \vdots \\ c_0 b_n + \ldots + c_n b_0 = a_n \\ \vdots \end{cases}$$

  Из записанных уравнений понятно, что необходимым и достаточным условием для деления является $b_0 \neq 0$.

Замечание. Определив умножение, мы сразу получили возведение в натуральную степень, а также взятие натурального корня:

- ▷
$$A^n = \underbrace{A \cdot \ldots \cdot A}_{n}$$

- ▷
$$B = \sqrt[n]{A} \Leftrightarrow B^n = A$$

Замечание. Из определения операций видно, что если положить за единицу ряд

$$1 = (1, 0, \ldots, 0, \ldots)$$

А за некоторое t ряд

$$t = (0, 1, \ldots, 0, \ldots)$$

То тогда t^n будет иметь вид

$$t^n = (\underbrace{0, \ldots, 0}_{n}, 1, 0, \ldots)$$

Из этого следует, что любой ряд $A = (a_1, \ldots, a_n, \ldots)$ можно записать в следующем виде:

$$A = (a_1, \ldots, a_n, \ldots) = a_1 \cdot 1 + a_2 \cdot t + \ldots + a_n \cdot t^n + \ldots$$

То есть формальный степенной ряд - это бесконечный многочлен. Довольно легко проверить, что для формальных степенных рядов, как и для многочленов, верна ассоциативность и дистрибутивность, чем мы и воспользуемся далее.

Пример. Посчитаем ряд, который можно записать как $\frac{1}{(1-x^2)^2}$:

$$\frac{1}{(1-x^2)^2} = \left(\frac{1}{1-x}\right)^2 \left(\frac{1}{1+x}\right)^2$$

где ряды под скобками запишутся как

$$\frac{1}{1-x} = 1 + x + x^2 + \ldots + x^n + \ldots$$
$$\frac{1}{1+x} = 1 - x + x^2 - \ldots + (-1)^n x^n + \ldots$$

Возведение в квадрат - это умножение ряда самого на себя. Отсюда имеем

$$\left(\frac{1}{1-x}\right)^2 = 1 + 2x + 3x^2 + \ldots + (n+1)x^n + \ldots$$
$$\left(\frac{1}{1+x}\right)^2 = 1 - 2x + 3x^2 - \ldots + (-1)^n(n+1)x^n + \ldots$$

Записать произведение квадратов в общем виде - можно, но не нужно. Посмотрим на коэффициент при n-м слагаемом:

$$\left(\left(\frac{1}{1-x}\right)^2 \left(\frac{1}{1+x}\right)^2\right)_n = \sum_{k=0}^{n} (k+1) \cdot (-1)^{n-k}(n+1-k)$$

С другой стороны мы можем заметить, исходный ряд можно получить, если сделать подставить x^2 вместо x для $\left(\frac{1}{1-x}\right)^2$:

$$\frac{1}{(1-x^2)^2} = 1 + 2x^2 + 3x^4 + \ldots + (n+1)x^{2n} + \ldots$$

На нечётных местах коэффициенты обнулились, на чётных остались прежними. Коль скоро ряды равны, то коэффициенты в одинаковых местах также совпадают. Получили тождество:

$$\sum_{k=0}^{n} (k+1) \cdot (-1)^{n-k}(n+1-k) = \begin{cases} 0, \text{ если } n = 2l+1 \\ l+1, \text{ если } n = 2l \end{cases}$$

Если рассматривать формальный степенные ряды как многочлены, то появляются ещё 2 операции, которые мы можем совершать над рядами:

▷ Взятие производной от ряда. Если ряд A имеет вид:

$$f(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n + \ldots$$

то его *производной* назовётся ряд

$$f'(t) = a_1 + 2a_2t + \ldots + na_nt^{n-1} + (n+1)a_{n+1}t^n + \ldots$$

▷ Если есть 2 формальных степенных ряда $f(t) = a_0 + a_1t + \ldots + a_nt^n + \ldots$ и $g(t) = b_0 + b_1t + \ldots + b_nt^n + \ldots$, то можно определить *композицию* рядов $f(g(t))$:

$$f(g(t)) = a_0 + a_1g(t) + a_2g^2(t) + \ldots + a_ng^n(t) + \ldots$$

При этом, если $b_0 \neq 0$, то ряд не имеет смысла, так как свободный член будет бесконечен:

$$f(g(t)) = a_0 + a_1b_0 + a_2b_0^2 + a_3b_0^3 + \ldots + a_nb_0^n + \ldots$$

Поэтому необходимым и достаточным условием композиции является равенство:

$$b_0 = 0$$

Сходимость ряда

Определение 2.19. И всё-таки, мы можем рассмотреть формальный степенной ряд как функцию $f(x)$:

$$f(x) = \sum_{k=0}^{\infty} a_kx^k$$

Будем говорить, что $f(x)$ *сходится в точке* x_0, если последовательность частичных сумм этого ряда в этой точке имеет конечный предел. То есть

$$S_n(x_0) = \sum_{k=0}^{n} a_kx_0^k$$
$$\exists \lim_{n\to\infty} S_n = S = f(x_0) \in \mathbb{C}$$

Теорема 2.24. *(Признак Коши-Адамара) Пусть задан формальный степенной ряд* $A = (a_0, \ldots, a_n, \ldots)$, *причём* $\forall n \in \mathbb{N}\ a_n \in \mathbb{R}$. *Обозначим за* $\rho = \frac{1}{\overline{\lim\limits_{k\to\infty}} \sqrt[k]{|a_k|}}$. *Тогда:*

▷ *Если* $|x_0| < \rho$, *то ряд сходится в* x_0.

▷ *Если* $|x_0| > \rho$, *то ряд расходится в* x_0.

▷ *Если же* $|x_0| = \rho$, *то может быть всё, что угодно.*

При этом ρ *называется радиусом сходимости.*

Замечание. Взятие производной сохраняет радиус сходимости.

Пример. Со школьных лет известно, что

$$1 + x + \ldots + x^n + \ldots = \frac{1}{1-x},\ |x| < 1$$

При этом про левую часть мы знаем, что это - формальный ряд, где $a_n = 1$. Значит, $\rho = \frac{1}{1} = 1$ - сходится с утверждением, которое заявляет нам признак Коши-Адамара.

Определение 2.20. Если нам задана последовательность (ряд) $\{a_k\}_{k=0}^{\infty}$, то её *производящей функцией* называется

$$f(x) = \sum_{k=0}^{\infty} a_k x^k$$

Пример. (Производящая функция чисел Фибоначчи) Как уже выяснено, числа Фибоначчи можно выписать в явном виде. Если положить $F_0 = 0$, $F_1 = 1$, то формула примет вид:

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

Посчитаем производящую функцию для данной последовательности:

$$f(x) = \sum_{k=0}^{\infty} F_k x^k$$

Мы хотим «свернуть» бесконечную сумму в какое-то деление конечных чисел, как для рядов, показанных выше. Посмотрим на следующие ряды:

$$\begin{aligned} xf(x) &= F_0 x + F_1 x^2 + \ldots + F_n x^{n+1} + \ldots \\ x^2 f(x) &= F_0 x^2 + F_1 x^3 + \ldots + F_n x^{n+2} + \ldots \\ xf(x) + x^2 f(x) &= \underbrace{F_0 x}_{0} + \underbrace{(F_0 + F_1)}_{F_2} x^2 + \underbrace{(F_1 + F_2)}_{F_3} x^3 + \ldots = f(x) - x \end{aligned}$$

Получили линейное уравнение относительно $f(x)$. Решив его, получим ответ:

$$f(x) = \frac{x}{1 - x - x^2}$$

2.18 Числа Каталана

Обозначим за T_n - количество правильных скобочных выражений из $2n$ скобок вида (). Тогда T_n - это n-ое *число Каталана.*

Утверждение 2.6. *Для чисел Каталана имеет место следующее рекуррентное соотношение:*

$$T_n = T_{n-1}T_0 + T_{n-2}T_1 + \ldots + T_0 T_{n-1}$$

При этом $T_0 = T_1 = 1$

Само рекуррентное соотношение уже даёт подсказку для производящей функции $f(x)$ чисел Каталана. Составим её:

$$f(x) = T_0 + T_1 x + T_2 x^2 + \ldots + T_n x^n + \ldots$$

А теперь посмотрим на $f^2(x)$:

$$f^2(x) = \underbrace{T_0^2}_{T_1} + \underbrace{(T_0T_1 + T_1T_0)}_{T_2} x + \underbrace{(T_0T_2 + T_1T_1 + T_2T_0)}_{T_3} x^2 + \ldots + \underbrace{(T_0T_n + \ldots + T_nT_0)}_{T_{n+1}} x^n + \ldots$$

То есть верно равенство:

$$f(x) = T_0 + xf^2(x) = 1 + xf^2(x) \Leftrightarrow xf^2 - f + 1 = 0$$

Получаем квадратное уравнение относительно $f(x)$. Решая его, получим корни:

$$f = \frac{1 \pm \sqrt{1-4x}}{2x}$$

Как отобрать нужный корень? Для этого домножим на x и так как выражение должно оставаться корректным при всех $|x| < \rho$, то оно должно быть верным для $x = 0$. Отсюда получаем, что нам нужен корень с минусом (или из других соображений о том, что деление на x должно быть корректным. Значит, единица должна сократиться с той, что появится в ряду корня):

$$f(x) = \frac{1 - \sqrt{1-4x}}{2x}$$

Осталось, собственно, вычислить корень. Это можно сделать последовательным вычислением $\frac{1}{\sqrt{1-x}}$ и подстановкой $4x$ вместо x:

$$\sqrt{1-x} = 1 - C^1_{1/2}x + C^2_{1/2}x^2 - \ldots + (-1)^n C^n_{1/2}x^n + \ldots$$

где $C^n_{1/2}$ можно переписать так:

$$C^n_{1/2} = \frac{\frac{1}{2}\cdot\left(\frac{1}{2}-1\right)\cdot\ldots\cdot\left(\frac{1}{2}-n+1\right)}{n!} = \frac{\frac{1}{2}\cdot\left(-\frac{3}{2}\right)\cdot\ldots\cdot\left(-\frac{2n-3}{2}\right)}{n!} =$$
$$(-1)^{n-1}\frac{1\cdot 3\cdot\ldots\cdot(2n-3)}{n!\cdot 2^n} = \frac{(-1)^{n-1}}{2^n}\cdot\frac{(2n-2)!}{n!\cdot 2\cdot 4\cdot\ldots\cdot(2n-2)} =$$
$$\frac{(-1)^{n-1}}{2^n}\cdot\frac{(2n-2)!}{n!\cdot 2^{n-1}\cdot(n-1)!} = \frac{(-1)^{n-1}}{2^{2n-1}}\cdot\frac{C^{n-1}_{2n-2}}{n}$$

Тогда коэффициент при x^n в ряду $\sqrt{1-4x}$ имеет вид:

$$C^n_{1/2}\cdot(-4)^n = \frac{-2C^{n-1}_{2n-2}}{n}$$

Отсюда уже получаем общий вид для $\sqrt{1-4x}$:

$$\sqrt{1-4x} = 1 - \frac{2C^0_0}{1}x - \frac{2C^1_2}{2}x^2 - \ldots - \frac{2C^{n-1}_{2n-2}}{n}x^n - \ldots$$

Стало быть

$$f(x) = \frac{1-\sqrt{1-4x}}{2x} = \frac{C^0_0}{1} + \frac{C^1_2}{2}x^2 + \ldots + \frac{C^{n-1}_{2n-2}}{n}x^{n-1} + \frac{C^n_{2n}}{n+1}x^n + \ldots$$

Теорема 2.25. *n-е число Каталана можно записать в явном виде:*

$$T_n = \frac{C^n_{2n}}{n+1}$$

2.19 Предварительные сведения о теории чисел

Сравнения по модулю

Определение 2.21. Пусть есть произвольные $a, b, m \in \mathbb{Z}$. Тогда говорят, что a *сравнимо с* b *по модулю* m, если m является делителем разности $a - b$.

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b)$$

Определение 2.22. Полученное сравнение является отношением эквивалентности на $\mathbb{Z}$ и соответственно разбивает его на классы эквивалентности. Число, взятое за представителя класса эквивалентности сравнения по модулю, называется *вычетом по модулю* m.

Типично берут набор либо $1, 2, \ldots, m$, либо $0, 1, \ldots, m-1$. Если набор, как выше, содержит представителей всех классов эквивалентностей, то его также называют *полной системой вычетов*. Если из полной системы мы выбираем только такие элементы, которые взаимно просты с m, то новая система называется *приведённой системой вычетов*.

Определение 2.23. Пусть есть $a, b \in \mathbb{Z}$. Тогда *Наибольший Общий Делитель* этих чисел мы будем обозначать как (a, b), а *Наименьшее Общее Кратное* как $[a, b]$.

Числа a и b называются *взаимно простыми*, если $(a, b) = 1$.

Определение 2.24. *Функцией Эйлера* называется $\varphi(m)$, которая возвращает количество взаимно простых с m чисел из множества $\{1, \ldots, m\}$:

$$\varphi(m) = \left|\{a \in \{1, \ldots, m\} \mid (a, m) = 1\}\right|$$

Теорема 2.26. *(Малая теорема Ферма) Пусть* p *- простое число. Пусть* $a \in \mathbb{N}$ *такое, что* $(a, p) = 1$. *Тогда*

$$a^{p-1} \equiv 1 \pmod{p}$$

Следствие. Для любого $a \in \mathbb{N}$, удовлетворяющего условию теоремы, будет верно также и следующее утверждение:

$$a^p \equiv a \pmod{p}$$

Доказательство. Докажем теорему двумя способами:

1. Чтобы не облегчить себе жизнь, будем доказывать её следствие, которое равносильно исходной теореме (в силу $(a, p) = 1$). Представим a^p в следующем виде:

$$a^p = (\underbrace{1 + \ldots + 1}_{a})^p = \underbrace{1 + \ldots + 1}_{a} + \sum_{\substack{n_1 + \ldots + n_a = p \\ \forall i \in [1;a] \;\; n_i < p}} P(n_1, \ldots, n_a) 1^{n_1} \cdot \ldots \cdot 1^{n_a}$$

   Кроме единиц останутся только слагаемые, содержащие полиномиальные коэффициенты и произведение единиц (которое, естественно, можно просто убрать). Распишем его:

$$P(n_1, \ldots, n_a) = \frac{p!}{n_1! \cdot \ldots \cdot n_a!}$$

   При этом $\forall i \in [1; a]$ $n_i < p$. Отсюда следует, что $n_i!$ не будет делиться на p для любого i. При этом числитель на p делится. Следовательно, все слагаемые с полиномиальным коэффициентом обнуляются в кольце вычетов по p и мы получаем необходимое тождество:

$$a^p \equiv a \pmod{p}$$

2. Возьмём $\{1, 2, \ldots, p-1\}$ за приведенную систему вычетов по модулю p. Тогда утверждается, что множество $\{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$ - тоже приведённая система вычетов по модулю p. Почему это так? Предположим противное:

$$\exists i, j \in \{1, \ldots, p-1\} \mid i \neq j, \;\; a \cdot i \equiv a \cdot j \pmod{p}$$

В таком случае верно следующее:

$$a \cdot (i - j) \equiv 0 \pmod{p}$$

Но разность $i-j$ заведомо меньше p и даже не может равняться $-p$ или 0. Значит, что a делится на p. Противоречие. Существование такой приведённой системы вычетов даёт нам следующий факт:

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv (a \cdot 1) \cdot (a \cdot 2) \cdot \ldots \cdot (a \cdot (p-1)) \pmod{p}$$

Так как одинаковые сомножители с обеих сторон взаимно просты с p, то сократив их получим утверждение теоремы:

$$1 \equiv a^{p-1} \pmod{p}$$

□

Теорема 2.27. *(Теорема Эйлера) Пусть $m \in \mathbb{N}$, а также есть $a \in \mathbb{N}$ такое, что $(a, m) = 1$. Тогда*

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Замечание. Теорема Эйлера является полным обобщением Малой теоремы Ферма из-за того факта, что

$$\varphi(p) = p - 1$$

Доказательство. По аналогии со вторым доказательством Малой теоремы Ферма, выберем приведённую систему вычетов по модулю m: $\{b_1, \ldots, b_{\varphi(m)}\}$. Тогда и $\{ab_1, \ldots, ab_{\varphi(m)}\}$ будет приведённой системой вычетов по модулю m. Следовательно

$$a^{\varphi(m)} \cdot b_1 \cdot \ldots \cdot b_{\varphi(m)} \equiv b_1 \cdot \ldots \cdot b_{\varphi(m)} \pmod{m}$$

Сокращая сомножители с обеих сторон снова получим нужное тождество:

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

□

2.20 Проблема Эрдеша-Гинзбурга-Зива

Теорема 2.28. *(Теорема Эрдеша-Гинзбурга-Зива для одномерного случая) Для любых целых чисел $a_1, \ldots, a_{2n-1}$ существует подмножество $I \subset \{1, 2, \ldots, 2n-1\}$ такое, что $|I| = n$, а также*

$$\sum_{i \in I} a_i \equiv 0 \pmod{n}$$

Замечание. Числа в теореме могут быть любыми, то есть и совпадать тоже. Более того, нам не важно само число, а только его вычет в кольце n, поэтому можно говорить, что мы имеем дело не с числами, а с вычетами и тем самым позволяем себе брать любого представителя класса вычета.

Теорема важна тем, что даёт точную нижнюю грань для количества a_i: если взять $2n-2$ числа, то она верна не всегда. Контрпримером будет

$$\underbrace{0,\ldots,0}_{n-1},\underbrace{1,\ldots,1}_{n-1}$$

Всего чисел здесь $2n-2$, но какие ни возьми, делиться на n без остатка они не будут.

Доказательство. Доказательство состоит из двух частей:

1. $n=p$ - простое.

   Обозначим за $S=\sum\limits_{\substack{I\subset\{1,\ldots,2p-1\}\\|I|=p}}\left(\sum\limits_{i\in I}a_i\right)^{p-1}$. Предположим, что теорема не выполнена:

   $$\forall I\subset\{1,\ldots,2p-1\},\ |I|=p\Rightarrow\sum_{i\in I}a_i\not\equiv 0 \pmod p$$

   Но при этом, согласно малой теореме Ферма мы знаем, что

   $$\left(\sum_{i\in I}a_i\right)^{p-1}\equiv 1 \pmod p$$

   Отсюда имеем следующее:

   $$S\equiv C_{2p-1}^{p} \pmod p$$

   Если вычислять значения числа сочетаний в кольце, то можно заметить факт:

   $$C_{2p-1}^{p}\equiv 1 \pmod p$$

   Остаётся его только доказать. Для этого обратим внимание на соотношение:

   $$C_{2p}^{p}=2C_{2p-1}^{p}$$

   То есть достаточно доказать, что $C_{2p}^{p}\equiv 2 \pmod p$. Рассмотрим комбинаторное тождество:

   $$C_{2p}^{0}+\ldots+C_{2p}^{p}+\ldots+C_{2p}^{2p}=4^p$$

   Будем рассматривать $p>5$, а для меньших просто проверим руками. Тогда $4^p=4^{p-1}\cdot 4\equiv 4 \pmod p$. При этом $C_{2p}^{0}=C_{2p}^{2p}=1\equiv 1 \pmod p$. Что можно сказать про C_{2p}^{k}, $k\in[1;p-1]$ (для $k>p$ всё зеркально)?

   $$C_{2p}^{k}=\frac{(2p)!}{k!(2p-k)!}=\frac{2p\cdot(2p-1)\cdot\ldots\cdot(2p-k+1)}{k!}$$

   Коль скоро $k!$ не делится на p, то делимость на p зависит только от числителя, кото-

рый, очевидно, на p делится. Отсюда

$$C_{2p}^{k} \equiv 0 \pmod{p}$$

В итоге мы получили, что

$$S \equiv 1 \pmod{p}$$

Осталось в рамках предположения опровергнуть его при помощи доказательства делимости S на n. Для этого придётся совершить ужасное дело: раскрыть $(p-1)$-ю степень внутренней суммы и перегруппировать слагаемые. Выберем произвольное $I \subset \{1, \ldots, 2p-1\}$. Из него выберем подмножество индексов $\{i_1, \ldots, i_q\} \subset I$ - это элементы, чьи степени в слагаемом положительны. То есть

$$\left(\sum_{i \in I} a_i\right)^{p-1} = \sum_{\substack{\{i_1,\ldots,i_q\} \subset I \\ 1 \leqslant q \leqslant p-1}} P(\alpha_{i_1}, \ldots, \alpha_{i_q}) \cdot a_{i_1}^{\alpha_{i_1}} \cdot \ldots \cdot a_{i_q}^{\alpha_{i_q}}$$

При этом выполнены условия:

$$\forall l \in [1; q] \ \alpha_{i_l} \geqslant 1$$
$$\alpha_{i_1} + \ldots + \alpha_{i_q} = p - 1$$

Теперь зададимся вопросом: а сколько же таких слагаемых, которые записаны под суммой, получится, если расписать внешнюю сумму? Ровно столько, сколько есть множеств $I \supset \{i_1, \ldots, i_q\}$ для некоторого конкретного набора $\{i_1, \ldots, i_q\}$. Это число в точности равно C_{2p-1-q}^{p-q}. Осталось заметить, что оно всегда делится на p для $q \in [1; n-1]$:

$$C_{2p-1-q}^{p-q} = \frac{(2p-1-q)!}{(p-q)! \cdot (p-1)!}$$

Ни одно из нижних слагаемых не делится на p, а числитель точно содержит в себе $p!$. Значит, мы можем перегруппировать слагаемые в S так, что каждое делится на p. Следовательно

$$S \equiv 0 \pmod{p}$$

Противоречие.

2. Доказать, что если n, m удовлетворяют теореме ЭГЗ, то и $n \cdot m$ удовлетворяет ей.

По основной теореме арифметики любое натуральное число больше единицы представляется единственным образом как произведение простых в некоторых степенях, для которых мы знаем, что теорема верна. $\Rightarrow$ доказали для всех натуральных чисел (единица тривиальна). $\square$

Изначальная проблема была сформулирована для целых чисел. Но что мешает обобщить её, скажем, на $\mathbb{Z}^d$, $d \geqslant 1$? Так и поступили учёные. История случая $d = 2$ такова:

1. В 70е годы Кемниц высказал гипотезу, что в $\mathbb{Z}^2$ теорема Эрдеша-Гинзбурга-Зива будет верна для $4n-3$ пар чисел. Для $4n-4$ существует простой контрпример: нужно взять $n-1$ пару $(0,0)$, $n-1$ пару $(0,1)$, $n-1$ пару $(1,0)$ и $n-1$ пару $(1,1)$. Несложно увидеть, что сумма n пар никогда не будет делиться на n.

2. В 90е математиками Алоном и Дубинером было доказано, что начиная с некоторого n_0 минимальное количество пар чисел точно $\leqslant 6n-5$.

3. В 2004м году математик Ро́ньяи доказал, что минимальное количество пар не может быть больше $4n-2$.

4. В 2006м году математик Райер (нем. *Reiher*) подтвердил гипотезу Кемница и доказал теорему Эрдеша-Гинзбурга-Зива в случае $d=2$.

Теорема 2.29. *(Теорема Роньяи) Для любого множества пар* $(a_1,b_1),\ldots,(a_{4n-2},b_{4n-2})$ *найдётся подмножество* $I\in\{1,\ldots,4n-2\}$, $|I|=n$ *такое, что*

$$\sum_{i\in I} a_i \equiv \sum_{i\in I} b_i \equiv 0 \pmod{n}$$

Перед тем, как доказывать теорему, нам необходимо ввести обозначение для многочлена многих переменных - $F(x_1,\ldots,x_n)$.

Пример. $F(x_1,x_2)=x_1^3+x_1^2x_2+3x_2^{15}$

При этом обычно рассматривают многочлены над некоторым полем (то, откуда берутся коэффициенты). В нашем случае мы будет работать с многочленами многих переменных над полем $\mathbb{Z}_p$:

$$F\in\mathbb{Z}_p[x_1,\ldots,x_n]$$

Теорема 2.30. *(Теорема Шевалле) Пусть* $F\in\mathbb{Z}_p[x_1,\ldots,x_n]$, $\deg F<n$ *и при этом* N_p *- число решений сравнения* $F(x_1,\ldots,x_n)\equiv 0 \pmod{p}$ *(естественно решения* $(x_1,\ldots,x_n)\in\mathbb{Z}_p^n$*. То есть* $N_p\leqslant p^n$*). Тогда утверждается, что*

$$N_p\equiv 0 \pmod{p}$$

Доказательство. Для начала заметим способ, которым можно сосчитать вычет N_p:

$$N_p\equiv\sum_{x_1=1}^{p}\sum_{x_2=1}^{p}\ldots\sum_{x_n=1}^{p}\left(1-F^{p-1}(x_1,\ldots,x_n)\right) \pmod{p}$$

Суммы в конечном итоге фиксируют набор $(x_1,\ldots,x_n)$.

Если он является решением, то $F(x_1,\ldots,x_n)\equiv 0 \pmod{n}$ и следовательно $p-1$ степень тоже имеет вычет 0, то есть в сумму добавится единица.

Если же верно $F(x_1,\ldots,x_n)\not\equiv 0 \pmod{n}$, то по малой теореме Ферма $p-1$ степень значения многочлена будет сравнима с единицей по модулю p. Стало быть, такой многочлен обратит слагаемое в 0 и не будет никак учтён.

При этом заметим, что если раскрыть всё суммирование в слагаемые, то все единицы в сумме дадут $p^n\Rightarrow$ не имеют вклада в вычет по модулю p. Это означает, что нам надо проверить лишь следующее утверждение:

$$\sum_{x_1=1}^{p}\ldots\sum_{x_n=1}^{p}F^{p-1}(x_1,\ldots,x_n)\equiv 0 \pmod{p}$$

Отметим, что оценка на степень многочлена в сумме - это $\deg F^{p-1}\leqslant(n-1)\cdot(p-1)$. Рассмотрим произвольный моном в этом многочлене. Он имеет вид $C\cdot x_1^{\alpha_1}\cdot\ldots x_n^{\alpha_n}$, где

$0 \leqslant \alpha_i \leqslant \deg F^{p-1}$ и $\sum\limits_{i=1}^{n} \alpha_i = \deg F^{p-1}$. Если мы докажем утверждение ниже, то докажем и предыдущее тоже:

$$\sum_{x_1=1}^{p} \dots \sum_{x_n=1}^{p} x_1^{\alpha_1} \cdot \dots x_n^{\alpha_n} \equiv 0 \pmod{p}$$

1. $p = 2$. Тогда $\alpha_1 + \dots + \alpha_n \leqslant (n-1)(p-1) = n-1$. По принципу Дирихле это значит, что найдётся хотя бы один $\alpha_i = 0$, а так как мы можем произвольно менять знаки суммирования, то «подвинув» суммирование x_i вправо, можно вынести все остальные сомножители монома за знак суммирования по x_i и получить внутри следующее:

$$\sum_{x_i=1}^{p} x_i^{\alpha_i} = p \equiv 0 \pmod{p}$$

2. $p \geqslant 3$. Эта ситуация тоже разбивается на 2:

   (a) Нашлось $\alpha_i = 0$. Тогда действуем как в первом случае

   (b) $\forall i \in [1; n]$ $\alpha_i \geqslant 1$, но при этом всё ещё верно $\alpha_1 + \dots + \alpha_n \leqslant (n-1)(p-1)$. Тогда, согласно принципу Дирихле:

$$\exists i \in [1; n] \;\Big|\; 1 \leqslant \alpha_i \leqslant p-2$$

Утверждение 2.7. *Если $1 \leqslant \alpha_i \leqslant p-2$, то существует $a > 1$ такое, что*

$$a^{\alpha_i} \not\equiv 1 \pmod{p}$$

Доказательство. Если перенести единицу влево, то получим

$$a^{\alpha_i} - 1 \not\equiv 0 \pmod{p}$$

Теперь слева записан многочлен степени α_i над кольцом $\mathbb{Z}_p$. В курсе алгебры доказывается, что у этого многочлена α_i корней, а так как $a = 1$ является корнем, то отличных от 1 и 0 у него $\alpha_i - 1 < p-2$ корней, что меньше числа вычетов, удовлетворяющих тем же условиям $\Rightarrow$ найдётся нужное $a > 1$. □

Зная этот факт, обозначим за $S = \sum\limits_{x_i=1}^{p} x_i^{\alpha_i}$ и рассмотрим выражение $a^{\alpha_i} \cdot S$:

$$a^{\alpha_i} \cdot S = \sum_{x_i=1}^{p} (a x_i)^{\alpha_i} \equiv \sum_{x_i=1}^{p} x_i^{\alpha_i} = S \pmod{p}$$

То есть

$$a^{\alpha_i} \cdot S \equiv S \pmod{p} \Rightarrow S(a^{\alpha_i} - 1) \pmod{p}$$

Так как $a^{\alpha_i} \not\equiv 1 \pmod{p}$, то $(a^{\alpha_i} - 1) \not\equiv 0 \pmod{p}$. Значит

$$S \equiv 0 \pmod{p}$$

Что и требовалось доказать.

□

Теорема 2.31. *(Теорема Варнинга) Пусть* $F \in \mathbb{Z}_p[x_1, \ldots, x_n]$, $\deg F < n$ *и при этом* N_p *- число решений сравнения* $F(x_1, \ldots, x_n) \equiv 0 \pmod p$ *и* $(0, \ldots, 0)$ *входит в* N_p*. Тогда существует такое решение* $(x_1, \ldots, x_n)$ *сравнения, что*

$$\exists i \in [1; n] \mid x_i \neq 0$$

То есть существует нетривиальное решение.

Доказательство. Прямое следствие теоремы Шевалле. □

Теорема 2.32. *(Обобщённая теорема Варнинга) Пусть* $F_1, \ldots, F_k \in \mathbb{Z}_p[x_1, \ldots, x_n]$, $\deg F_1 + \ldots + \deg F_k < n$ *и* $(0, \ldots, 0)$ *- решение системы сравнений:*

$$\begin{cases} F_1(x_1, \ldots, x_n) \equiv 0 \pmod p \\ \vdots \\ F_1(x_1, \ldots, x_n) \equiv 0 \pmod p \end{cases}$$

Тогда утверждается, что существует и нетривиальное решение данной системы.

Доказательство. Оставляется в качестве домашнего задания читателю (не входит в курс). P.S. Возможно придумаю и допишу, не знаю. □

Лемма 2.5. *Пусть есть* $(a_1, b_1), \ldots, (a_{3p}, b_{3p}) \in \mathbb{Z}^2$ *пар чисел и при этом*

$$\sum_{i=1}^{3p} a_i \equiv \sum_{i=1}^{3p} b_i \equiv 0 \pmod p$$

Тогда $\exists I \subset \{1, \ldots, 3p\}$, $|I| = p$, *что выполнено утверждение:*

$$\sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \pmod p$$

Доказательство. Для доказательства будем пользоваться уже сформулированными теоремами Варнинга и Шевалле. Положим за многочлен F_1 следующее:

$$F_1(x_1, \ldots, x_n) = \sum_{i=1}^{3p-1} a_i \cdot x_i^{p-1}$$

Аналогично определим F_2 и F_3:

$$F_2(x_1, \ldots, x_{3p-1}) := \sum_{i=1}^{3p-1} b_i x_i^{p-1}$$

$$F_3(x_1, \ldots, x_{3p-1}) := \sum_{i=1}^{3p-1} x_i^{p-1}$$

В силу определения очевидно, что $\forall i \in \{1, 2, 3\}$ $F_i(0, \ldots, 0) = 0$. При этом $\deg F_1 + \deg F_2 + \deg F_3 = 3(p-1) = 3p - 3 < 3p - 1$. Значит, можно применить обобщённую теорему

Варнинга и заявить следующее:

$$\exists(x_1,\ldots,x_{3p-1}) \mid \forall i \in \{1,2,3\}\ F_i(x_1,\ldots,x_{3p-1}) \equiv 0 \pmod p$$

Обозначим за J множество номеров ненулевых координат. Оно непустое - в этом и суть теоремы Варнинга. Тогда заметим, что все нулевые координаты никак не влияют на значение многочлена. А отсюда, если прибавить к этому малую теорему Ферма, получается утверждение:

$$\sum_{i=1}^{3p-1} a_i x_i^{p-1} = \sum_{i\in J} a_i x_i^{p-1} \equiv \sum_{i\in J} a_i \pmod p$$

Аналогично для оставшихся многочленов:

$$\sum_{i\in J} b_i \equiv 0 \pmod p$$
$$\sum_{i\in J} x_i^{p-1} \equiv \sum_{i\in J} 1 \equiv |J| \equiv 0 \pmod p$$

Мы почти доказали лемму. Осталось заметить, что $|J| \in \{p, 2p\}$, а от $3p$ и больше мы избавились из-за рассмотрения многочленов с $(3p-1)$-й переменной.

- ▷ Если $|J| = p$, то теорема доказана.
- ▷ Если $|J| = 2p$, то возьмём за $I := \{1,\ldots,3p\}\backslash J$. Тогда $|I| = p$ и при этом

$$\sum_{i\in I} a_i = \sum_{i=1}^{3p} a_i - \sum_{i\in J} a_i \equiv 0 \pmod p$$

Аналогично с $\sum\limits_{i\in I} b_i \equiv 0 \pmod p$.

□

Определение 2.25. *Симметрическим многочленом* степени k от n переменных называется следующий многочлен:

$$\sigma_k(x_1,\ldots,x_n) = \sum_{\substack{I\subset\{1,\ldots,n\}\\|I|=k}} \sum_{i\in I} x_i$$

Пример.

$$\sigma_1(x_1,\ldots,x_n) = x_1 + x_2 + \ldots + x_n$$
$$\sigma_2(x_1,\ldots,x_n) = x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n$$
$$\sigma_n(x_1,\ldots,x_n) = x_1 \cdot \ldots \cdot x_n$$

Доказательство. (теоремы Роньяи) Докажем случай, когда $n = p$ - простое число. Дополнительно обозначим за $m = 4p-2$. Как и в теореме ЭГЗ, предположим противное:

$$\forall I \subset \{1,\ldots,m\},\ |I| = p \quad \left(\sum_{i\in I} a_i \not\equiv 0 \pmod p\right) \vee \left(\sum_{i\in I} b_i \not\equiv 0 \pmod p\right)$$

В силу доказанной леммы, мы можем усилить отрицание и сказать, что $|I| = 3p$, ведь если бы такое I подходило, то из него можно было бы извлечь подходящее подмножество $|I'| = p$.

Теперь рассмотрим многочлен $F(x_1, \ldots, x_m)$ вида:

$$F(x_1, \ldots, x_m) = \left(\left(\sum_{i=1}^{m} a_i x_i\right)^{p-1} - 1\right) \cdot \left(\left(\sum_{i=1}^{m} b_i x_i\right)^{p-1} - 1\right) \cdot \left(\left(\sum_{i=1}^{m} x_i\right)^{p-1} - 1\right) \cdot (\sigma_p(x_1, \ldots, x_m) - 2)$$

Посмотрим, какие значения по модулю p принимает F на $(x_1, \ldots, x_m) \in \{0, 1\}^m$:

1. Пусть $(x_1, \ldots, x_m)$ таков, что в нём p единиц и, соответственно, $m-p$ нулей. Обозначим за I - множество индексов, где стоят единицы. Тогда понятно $|I| = p$. Более того, теперь суммы внутри первых двух скобок стали иметь вид:

$$\left(\sum_{i=1}^{m} a_i x_i\right)^{p-1} = \left(\sum_{i \in I} a_i\right)^{p-1}$$
$$\left(\sum_{i=1}^{m} b_i x_i\right)^{p-1} = \left(\sum_{i \in I} b_i\right)^{p-1}$$

   По предположению хотя бы одна из них не обнуляется. Значит, возведение в степень $p-1$ даст единицу по модулю p и в итоге получим, что

$$F(x_1, \ldots, x_m) \equiv 0 \pmod{p}$$

2. Аналогично предыдущему случаю, но теперь $|I| = 3p$. Так как предположение усиляется, то и в данном случае

$$F(x_1, \ldots, x_m) \equiv 0 \pmod{p}$$

3. $|I| \not\equiv 0 \pmod{p}$. В таком случае, посмотрим на третью скобку многочлена:

$$\left(\sum_{i=1}^{m} x_i\right)^{p-1} = \left(\sum_{i \in I} 1\right)^{p-1} = |I|^{p-1} \equiv 0 \pmod{p}$$

   Снова получили, что

$$F(x_1, \ldots, x_m) \equiv 0 \pmod{p}$$

4. $|I| = 2p$. Это последний случай, и он уже связан с симметрическим многочленом. Заметим, что если слагаемое содержит x_j, где $j \notin I$, то оно сразу обнуляется и не вносит вклада в значение $\sigma_p(x_1, \ldots, x_m)$. Отсюда следует 2 вещи: во-первых, каждое слагаемое - это просто единица, а во-вторых, этих слагаемых всего C_{2p}^{p}. Следовательно

$$\sigma(x_1, \ldots, x_m) = C_{2p}^{p} \equiv 2 \pmod{p}$$

Величина C_{2p}^{p} по модулю p уже доказывалась выше. В последний раз получили, что

$$F(x_1, \ldots, x_m) \equiv 0 \pmod{p}$$

5. $|I| = 0$. В таком случае

$$F(x_1, \ldots, x_m) = F(0, \ldots, 0) = 2$$

И это единственный набор $(x_1, \ldots, x_m)$, на котором F отличен от нуля.

Нам снова нужно совершить ужасное деяние: раскрыть скобки у данного многочлена. В общем случае слагаемое будет иметь вид:

$$C \cdot x_{i_1}^{\alpha_{i_1}} \cdot \ldots \cdot x_{i_q}^{\alpha_{i_q}}$$

Где $\forall l \in [1; q]\ \alpha_{i_l} \geqslant 1$. Сделаем все эти степени равными единицами, а полученный многочлен обозначим за $F'(x_1, \ldots, x_m)$. Коль скоро мы разобрали все случаи, когда $(x_1, \ldots, x_m) \in \{0, 1\}^m$, то для этих же наборов будет верно следующее:

$$\forall (x_1, \ldots, x_m) \in \{0, 1\}^m \quad F(x_1, \ldots, x_m) = F'(x_1, \ldots, x_m)$$

Из всего вышесказанного несложно заметить, что тогда F' можно указать явно(как минимум на наборах из $\{0, 1\}^m$, но как будет доказано ниже, это вообще единственный вид данного многочлена):

$$F'(x_1, \ldots, x_m) = 2(1 - x_1) \cdot (1 - x_2) \cdot \ldots \cdot (1 - x_m)$$

Чтобы доказать, что вид $F'(x_1, \ldots, x_m)$ единственнен, мы должны доказать, что все возможные мономы вида:

$$x_{i_1} \cdot \ldots \cdot x_{i_q}$$

образуют базис всех функций $f\colon \{0, 1\}^m \to \mathbb{Z}_p$. Размер множества из всех рассматриваемых мономов – 2^m и при этом очевидно, что это множество образует линейно независимую систему (зафиксируем любой моном и рассмотрим набор $(x_1, \ldots, x_m)$, где ненулевыми будут только те x_j, что входят в рассматриваемый моном. Тогда все остальные обнулятся). Зафиксируем произвольную $f\colon \{0, 1\}^m \to \mathbb{Z}_p$. Тогда, f точно можно выразить в базисе характеристических функций:

$$\mu_u(v) = \begin{cases} 1, & \text{если } u = v \\ 0, & \text{иначе} \end{cases}$$

где $u, v \in \{0, 1\}^m$. А любую такую характеристическую функцию можно явно записать через мономы:

$$\mu_{(u_1, \ldots, u_m)}(v_1, \ldots, v_m) = \prod_{i\colon u_i = 1} v_i \cdot \prod_{j\colon u_j = 0} (1 - v_j)$$

Тем самым мы доказали, что множество мономов образует базис в пространстве функций $f\colon \{0, 1\}^m \to \mathbb{Z}_p$. Значит, представление F' единственно и мы его нашли.

Если вид F' действительно такой, то $\deg F' = m = 4p - 2$. При этом $\deg F' \leqslant \deg F = 3(p - 1) + p = 4p - 3$ - получили противоречие. $\square$

Проблема Эрдеша-Гинзбурга-Зива в многомерном случае

Обозначим нижнюю оценку для d-мерного случая за функцию от двух переменных $f(n, d)$. Тогда, известно следующее:

- $f(n, 1) = 2n - 1$
- $f(n, 2) = 4n - 3$
- $f(n, 3) \geqslant 8n - 7$, но уже доказано, что $f(n, 3) \geqslant 9n - 9$
- $f(n, d) \geqslant 2^d \cdot (n - 1) + 1$ - обобщение рассказанных контрпримеров.

Полностью решены случаи лишь для $d = 1, 2$. Для всех остальных точные ответы остаются неизвестными.