Арифметические свойства биномиальных коэффициентов

На конференции Вам будет предложено несколько исследовательских проектов. Цель — как можно дальше продвинуться в каком-то из проектов. Задачи можно решать коллективно, объединившись в любые команды (члены команды могут быть из разных городов). Вы можете решать задачи сразу из нескольких проектов, причем по разным проектам Вы можете участвовать в разных командах. Единственное, чего не следует делать, — это присваивать себе чужие результаты, такое случается, если команда слишком велика и не все из нее активно решают задачи данного проекта.

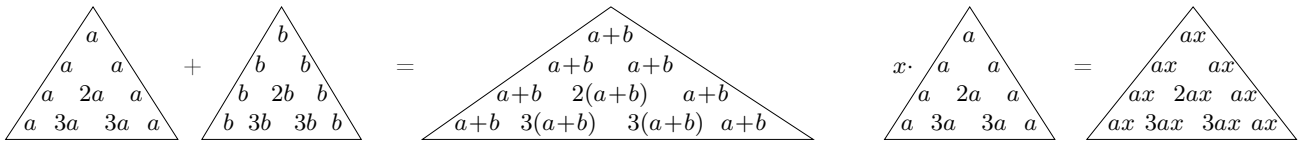
Это ознакомительная подборка задач по теме о биномиальных коэффициентах. Задачи следует решать письменно и сдавать Кохасю К.П. (вагон 15, место 17). В Теберде набор задач будет существенно расширен и все задачи, кроме задачи 1.2, можно будет сдавать и позже. По задаче 1.2 решения принимаются только в поезде, после этого задача снимается с конкурса.

1 Задачи в поезд

1.1. Докажите, что а) $C_{p-1}^k \equiv (-1)^k \pmod p$; б) $C_{2n}^n \equiv (-4)^n C_{\frac{p-1}{2}}^n \pmod p$ при $n \leqslant \frac{p-1}{2}$.

1.2. Докажите, что количество нечетных биномиальных коэффициентов в n-й строке треугольника Паскаля равно 2^r, где r — количество единиц в двоичной записи числа n.

1.3. Зафиксируем натуральное число m. Назовем m-арифметическим треугольником Паскаля треугольник, в котором вместо чисел C_n^k расставлены их остатки по модулю m. Кроме того, мы будем рассматривать похожие треугольники из остатков, у которых вдоль боковых сторон вместо единиц стоят одинаковые остатки a по модулю m. Такие треугольники можно умножать на число, а также складывать (если размеры совпадают), причем будем считать, что операции тоже выполняются по модулю m.



Пусть в s-й строке m-арифметического треугольника Паскаля все элементы, кроме крайних, — нули. Докажите, что тогда этот треугольник имеет вид, показанный на рис. 1. Заштрихованные треугольники состоят из нулей, а треугольники Δ_n^k состоят из s строк и подчинены следующим соотношениям:

1) $\Delta_n^{k-1} + \Delta_n^k = \Delta_{n+1}^k$; 2) $\Delta_n^k = C_n^k \cdot \Delta_0^0 \pmod m$.

Головоломка Ханойская башня представляет собой три стержня, на которые надеваются диски разной величины. Вначале все диски упорядочены по размеру (более крупные — ниже) и находятся на первом стержне. Разрешается снять со стержня один верхний диск и переместить его на другой стержень. При этом запрещается более крупный диск класть на диск меньшего размера. В головоломке требуется переложить все диски с первого стержня на второй.

Пусть количество дисков равно n. Рассмотрим граф TH_n, вершины которого — это всевозможные расположения дисков Ханойской башни, а ребра соединяют те состояния головоломки, которые получаются друг из друга за один ход. Рассмотрим также граф P_n, вершины которого — это единицы, расположенные в первых 2^n строках 2-арифметического треугольника Паскаля, а ребра соединяют соседние единицы (т.е. соседние в строке или в двух смежных строках по диагонали).

1.4. Докажите, что графы TH_n и P_n изоморфны.

1.5. Докажите, что в первых 10^6 строках 2-арифметического треугольника Паскаля единицы составляют меньше 1 %.

1.6. Докажите, что если n делится на $p-1$, то $C_n^{p-1} + C_n^{2(p-1)} + C_n^{3(p-1)} + \ldots + C_n^n \equiv 1 \pmod p$. Или лучше докажите в общем виде: если $1 \leqslant j, k \leqslant p-1$ и $n \equiv k \pmod{p-1}$, то

$$C_n^j + C_n^{(p-1)+j} + C_n^{2(p-1)+j} + C_n^{3(p-1)+j} + \ldots \equiv C_k^j \pmod p.$$

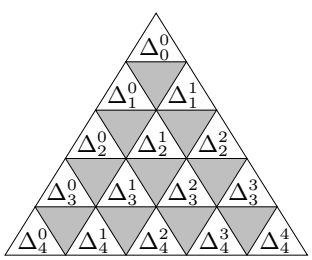


Рис. 1.

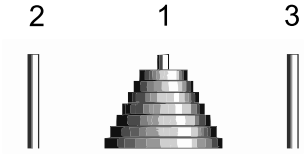


Рис. 2.

Арифметические свойства биномиальных коэффициентов — 2

Официальным "теоретическим материалом" для этого цикла задач служит статья Э. Б. Винберга [1]. В частности, считаются известными следующие теоремы.

1. Теорема Вильсона. Для всех простых p (и только для простых) выполнено сравнение $(p-1)! \equiv -1 \pmod{p}$.
2. Теорема Люка. Запишем числа n и k в системе счисления по основанию p:
$$n = n_d p^d + n_{d-1} p^{d-1} + \ldots + n_1 p + n_0, \qquad k = k_d p^d + k_{d-1} p^{d-1} + \ldots + k_1 p + k_0. \tag{1}$$
Тогда $C_n^k \equiv C_{n_d}^{k_d} C_{n_{d-1}}^{k_{d-1}} \cdot \ldots \cdot C_{n_1}^{k_1} C_{n_0}^{k_0} \pmod{p}$.
3. Теорема Куммера. Показатель $\operatorname{ord}_p C_n^k$ равен числу переносов при сложении столбиком чисел k и $\ell = n - k$ в p-ичной записи.
4. Теорема Волстенхолма. При $p \geqslant 5 \quad C_{2p}^p \equiv 2 \pmod{p^3}$ или, что то же самое, $C_{2p-1}^{p-1} \equiv 1 \pmod{p^3}$.

Напомним, что по определению $C_0^0 = 1$, $C_n^k = 0$ при $k > n$ и при $k < 0$.

Всюду буквой p мы обозначаем простое число. Для произвольного натурального числа n обозначим через $(n!)_p$ произведение всех натуральных чисел от 1 до n, не делящихся на p. Если задано число p, то символами n_i, m_i и т. д. обозначаются цифры p-ичной записи чисел n, m и т. д.

* * *

2 Арифметический треугольник и делимость

2.1. a) Докажите, что в первых 3^k строках 3-арифметического треугольника Паскаля содержится $\frac{1}{2}(6^k + 4^k)$ единиц и $\frac{1}{2}(6^k - 4^k)$ двоек.

b) Найдите число нулевых элементов в первых 5^k строках 5-арифметического треугольника Паскаля.

c) Найдите число ненулевых элементов в первых p^k строках p-арифметического треугольника Паскаля.

2.2. Докажите, что количество единиц в первых m строках 2-арифметического треугольника Паскаля равно
$$\sum_{i=0}^{n-1} m_i \cdot 2^{\sum_{k=i+1}^{n-1} m_k} \cdot 3^i.$$
Полагая $m = 2^{\alpha_1} + 2^{\alpha_2} + \ldots + 2^{\alpha_r}$, где $\alpha_1 > \alpha_2 > \ldots > \alpha_r$, можно то же выражение записать в виде
$$3^{\alpha_1} + 2 \cdot 3^{\alpha_2} + 2^2 \cdot 3^{\alpha_3} + \ldots + 2^{r-1} \cdot 3^{\alpha_r}.$$

2.3. Рассмотрим n-ю строку 2-арифметического треугольника Паскаля как двоичную запись некоторого натурального числа P_n. Докажите, что
$$P_n = F_{i_1} \cdot \ldots \cdot F_{i_s},$$
где $i_1, \ldots, i_s$ — номера разрядов, в которых в двоичной записи числа n стоят единицы, и $F_i = 2^{2^i} + 1$ — i-е число Ферма.

2.4. Докажите, что количество ненулевых элементов в n-й строке p-арифметического треугольника Паскаля равно $\prod_{i=0}^{d} (n_i + 1)$.

2.5. a) Для того чтобы все биномиальные коэффициенты C_n^k, где $0 < k < n$, делились на p, необходимо и достаточно, чтобы n было степенью числа p.

b) Для того чтобы все биномиальные коэффициенты C_n^k, где $0 \leqslant k \leqslant n$, не делились на p, необходимо и достаточно, чтобы $n+1$ делилось на p^d, иными словами, чтобы все цифры p-ичной записи числа n, кроме старшей, были равны $p-1$.

2.6. Пусть $0 < k < n+1$. Докажите, что если $C_n^{k-1} \not\vdots\, p$ и $C_n^k \not\vdots\, p$, то $C_{n+1}^k \not\vdots\, p$, *кроме* случая, когда $n+1$ делится на p.

3 Обобщение теорем Вильсона и Люка

3.1. Докажите, что $\operatorname{ord}_p(n!) = \dfrac{n - (n_d + \ldots + n_1 + n_0)}{p-1}$.

3.2. Докажите следующие обобщения теоремы Вильсона. a) $(-1)^{[n/p]}(n!)_p \equiv n_0! \pmod p$;
b) При $p \geqslant 3$ выполнено сравнение

$$(p^q!)_p \equiv -1 \pmod{p^q},$$

а при $p = 2$, $q \geqslant 3$ выполнено сравнение $(p^q!)_p \equiv 1 \pmod{p^q}$.
c) $\dfrac{n!}{p^\mu} \equiv (-1)^\mu n_0! n_1! \ldots n_d! \pmod p$, где $\mu = \operatorname{ord}_p(n!)$

3.3. Обобщенная теорема Люка. Пусть $r = n - k$, $\ell = \operatorname{ord}_p(C_n^k)$. Тогда

$$\frac{1}{p^\ell} C_n^k \equiv (-1)^\ell \Big(\frac{n_0!}{k_0! r_0!}\Big)\Big(\frac{n_1!}{k_1! r_1!}\Big) \ldots \Big(\frac{n_d!}{k_d! r_d!}\Big) \pmod p$$

3.4. a) Докажите, что $(1+x)^{p^d} \equiv 1 + x^{p^d} \pmod p$ при всех $x = 0, 1, \ldots, p-1$.
b) Докажите теорему Люка алгебраически.

3.5. a) Пусть m, n, k — натуральные числа, причем $(n, k) = 1$. Докажите, что $C_{mn}^k \equiv 0 \pmod n$.
b) Если $n \vdots p^k$, $m \not\vdots p$, то $C_n^m \vdots p^k$.

3.6. Пусть $f_{n,a} = \sum\limits_{k=0}^{n} (C_n^k)^a$. Докажите, что $f_{n,a} \equiv \prod\limits_{i=0}^{d} f_{n_i,a} \pmod p$.

4 Вариации на тему теоремы Волстенхолма

4.1. Докажите, что $\dfrac{1}{1} + \dfrac{1}{2} + \ldots + \dfrac{1}{p-1} \equiv 0 \pmod{p^2}$ при $p \geqslant 5$.

4.2. Пусть $p = 4k + 3$ — простое число. Найдите $\dfrac{1}{0^2+1} + \dfrac{1}{1^2+1} + \ldots + \dfrac{1}{(p-1)^2+1} \pmod p$.

4.3. a) Пусть натуральное число k таково, что для каждого простого делителя p числа m $k \not\vdots (p-1)$. Докажите, что

$$\frac{1}{1^k} + \frac{1}{2^k} + \ldots + \frac{1}{(m-1)^k} \equiv 0 \pmod m.$$

Здесь суммирование распространяется на все слагаемые, знаменатели которых взаимно просты с m.
b) Пусть k нечетно и $(k+1) \not\vdots (p-1)$. Докажите, что $\dfrac{1}{1^k} + \dfrac{1}{2^k} + \ldots + \dfrac{1}{(p-1)^k} \equiv 0 \pmod{p^2}$.

4.4. Докажите, что сравнение (12) из статьи Винберга выполнено по модулю p^4.

4.5. Докажите эквивалентность следующих сравнений. 1) $C_{2p-1}^{p-1} \equiv 1 \pmod{p^4}$;
2) $\dfrac{1}{1} + \dfrac{1}{2} + \ldots + \dfrac{1}{p-1} \equiv 0 \pmod{p^3}$; 3) $\dfrac{1}{1^2} + \dfrac{1}{2^2} + \ldots + \dfrac{1}{(p-1)^2} \equiv 0 \pmod{p^2}$.

4.6. a) Докажите алгебраически, что для всякого простого p и произвольных k и n $(C_{pk}^{pm} - C_k^m) \vdots p^2$. В статье Винберга этот факт доказан комбинаторно.
b) Докажите утверждение (9) из статьи Винберга: для всякого простого $p \geqslant 5$ и произвольных k и n $(C_{pk}^{pm} - C_k^m) \vdots p^3$.

4.7. Пусть $p \geqslant 5$. Докажите, что a) $C_{p^2}^p \equiv C_p^1 \pmod{p^5}$; b) $C_{p^{s+1}}^p \equiv p^s \pmod{p^{2s+3}}$.

4.8. Докажите, что $C_{p^3}^{p^2} \equiv C_{p^2}^p \pmod{p^8}$.

Арифметические свойства биномиальных коэффициентов — 3

Дополнения к предыдущим темам

2.7. Докажите, что $C^k_{p^n-1} \equiv (-1)^{S_k} \pmod p$, где S_k — сумма цифр p-ичной записи числа k.

2.8. Докажите, что если биномиальный коэффициент C^k_n нечетен, (т. е. в обозначениях из (1) $k_i \leqslant n_i$ при всех $i = 0, \ldots, d$), то

$$C^k_n \equiv \prod_{i=1}^{d} (-1)^{k_{i-1}n_i + k_i n_{i-1}} \pmod 4 .$$

2.9. Докажите, что если в двоичной записи числа n нет двух единиц подряд, то все нечетные числа в n-й строке треугольника Паскаля сравнимы с 1 по модулю 4, а в противном случае ровно половина из них сравнима с 1 по модулю 4.

2.10. Докажите, что количество пятерок в каждой строке 8-арифметического треугольника Паскаля равно степени двойки. То же касается единиц, троек и семерок.

2.11. Докажите, что если все элементы двух множеств

$$\{C^1_{2^n-1}, C^3_{2^n-1}, C^5_{2^n-1}, \ldots, C^{2^n-1}_{2^n-1}\} \quad \text{и} \quad \{1, 3, 5, \ldots, 2^n - 1\}$$

рассматривать как остатки по модулю 2^n, то эти множества совпадают.

2.12. Докажите, что элементы одной строки треугольника Паскаля не взаимно просты в следующем довольно сильном смысле. Для каждого числа $\varepsilon > 0$ существует N, такое, что при всех натуральных $n > N$ и $k_1, k_2, \ldots, k_{100} < \varepsilon\sqrt{n}$ верно, что числа

$$C^{n+k_1}_{2n},\ C^{n+k_2}_{2n},\ \ldots,\ C^{n+k_{100}}_{2n}$$

имеют общий делитель.

2.13. а) Даны натуральные числа $m > 1$, n, k. Докажите, что хотя бы одно из чисел C^k_n, C^k_{n+1}, …, C^k_{n+k} не делится на m.

b) Докажите, что для любого k найдется бесконечно много таких n, что все числа C^k_n, C^k_{n+1}, …, C^k_{n+k-1} делятся на m.

4.9. Докажите, что при $n > 1$ $C^{2^n}_{2^{n+1}} - C^{2^{n-1}}_{2^n}$ делится на 2^{2n+2}.

4.10. Докажите, что при $p \geqslant 5$ $(-1)^{\frac{p-1}{2}} C^{\frac{p-1}{2}}_{p-1} \equiv 4^{p-1} \pmod{p^3}$.

Арифметические свойства биномиальных коэффициентов — 4

Дополнения к предыдущим темам

4.11. Пусть m — произвольное натуральное число, $p \geqslant 5$ — простое. Докажите, что

$$\frac{1}{mp+1} + \frac{1}{mp+2} + \cdots + \frac{1}{mp+(p-1)} \equiv 0 \pmod{p^2}.$$

4.12. Пусть p и q — различные простые числа. Докажите, что сравнение $C_{2pq-1}^{pq-1} \equiv 1 \pmod{pq}$ выполнено в том и только в том случае, когда $C_{2p-1}^{p-1} \equiv 1 \pmod{q}$ и $C_{2q-1}^{q-1} \equiv 1 \pmod{p}$.

5 Суммы биномиальных коэффициентов

5.1. a) Докажите, что $\sum\limits_{k=0}^{3^a-1} C_{2k}^k$ делится на 3; b) делится на 3^a.

5.2. Пусть $C_k = \frac{1}{k+1}C_{2k}^k$ — последовательность чисел Каталана. Докажите, что $\sum\limits_{k=1}^{n} C_k \equiv 1 \pmod 3$ тогда и только тогда, когда троичное разложение числа $n+1$ содержит хотя бы одну цифру 2.

5.3. Пусть $p \geqslant 5$, $k = [2p/3]$. Докажите, что сумма $C_p^1 + C_p^2 + \ldots + C_p^k$ делится на p^2.

5.4. Если $n \vdots (p-1)$, где p — нечетное простое, то

$$C_n^{p-1} + C_n^{2(p-1)} + C_n^{3(p-1)} + \ldots \equiv 1 + p(n+1) \pmod{p^2}.$$

5.5. Докажите, что при $0 \leqslant j \leqslant p-1 < n$ и $q = [\frac{n-1}{p-1}]$

$$\sum_{m:m\equiv j \pmod p} (-1)^m C_n^m \equiv 0 \pmod{p^q}.$$

5.6. Докажите, что если p — нечетное простое, то $n \vdots (p+1)$ тогда и только тогда, когда

$$C_n^j - C_n^{j+(p-1)} + C_n^{j+2(p-1)} - C_n^{j+3(p-1)} + \ldots \equiv 0 \pmod p$$

при всех $j = 1, 3, \ldots, p-2$.

Решения

1 Задачи в поезд

1.1. а) Решение 1. $C_{p-1}^k = \dfrac{(p-1)(p-2)\dots(p-k)}{1\cdot 2\cdots k} \equiv \dfrac{(-1)(-2)\dots(-k)}{1\cdot 2\cdots k} \equiv (-1)^k \pmod p$.

Решение 2. По формуле для биномиальных коэффициентов очевидно, что C_p^i при $1 \leqslant i \leqslant p-1$ делится на p. Кроме того, имеет место основное рекуррентное соотношение $C_{p-1}^{k-1} + C_{p-1}^k = C_p^k$. Так как $C_{p-1}^0 = 1 \equiv 1 \pmod p$ и $(C_{p-1}^0 + C_{p-1}^1) \vdots p$, заключаем отсюда, что $C_{p-1}^1 \equiv -1 \pmod p$. Но $C_{p-1}^1 + C_{p-1}^2$ тоже делится на p, значит, $C_{p-1}^2 \equiv 1 \pmod p$ и т.д.

б) Это задача [3, задача 162]. Поскольку дроби C_{2n+2}^{n+1}/C_{2n}^n и $C_{\frac{p-1}{2}}^{n+1}/C_{\frac{p-1}{2}}^n$ сильно сократимы, утверждение легко проверяется по индукции. Но мы предложим прямое вычисление из [3].

Как нетрудно видеть,

$$C_{2n}^n = 2^n \cdot \frac{1\cdot 3\cdots(2n-1)}{n!}$$

При этом

$$1\cdot 3\cdots(2n-1) = (-1)^n(-1)(-3)\cdots(-2n+1) \equiv (-1)^n(p-1)(p-3)\cdots(p-2n+1) =$$

$$= (-1)^n 2^n \Big(\frac{p-1}{2}\Big)\Big(\frac{p-3}{2}\Big)\cdots\Big(\frac{p-2n+1}{2}\Big) = (-1)^n 2^n \Big(\frac{p-1}{2}\Big)\Big(\frac{p-1}{2}-1\Big)\cdots\Big(\frac{p-1}{2}-n+1\Big) =$$

$$= (-1)^n 2^n \frac{(\frac{p-1}{2})!}{(\frac{p-1}{2}-n)!} \pmod p.$$

Таким образом, $C_{2n}^n \equiv (-1)^n 4^n \dfrac{(\frac{p-1}{2})!}{n!(\frac{p-1}{2}-n)!} = (-4)^n C_{\frac{p-1}{2}}^n \pmod p$.

1.2. Это непосредственно следует из самоподобной структуры арифметического треугольника Паскаля, описанной в следующих задачах. Это также сразу следует из теоремы Люка. Доказательство можно прочесть в статье Винберга [1].

1.3. Мы ограничимся небольшим созерцанием, полное решение см. в [3, задача 133].

Поскольку в s-й строке расположен длинный ряд из нулей, в $(s+1)$-й строке под этими нулями также расположен ряд из нулей (на единицу короче), в $(s+2)$-й строке — опять ряд из нулей (снова на 1 короче) и т. д. Этим объясняется наличие серого треугольника снизу от Δ_0^0 (рис. 1).

Далее, ненулевые элементы s-й строки равны 1, тогда ряды чисел, идущих вдоль наклонных границ серого треугольника, состоящего из нулей, — это тоже всё сплошь единицы (по рекуррентному правилу построения треугольника Паскаля). Таким образом, вдоль боковых сторон треугольников Δ_1^0 и Δ_1^1 расположены единицы, и значит, оба этих треугольника идентичны Δ_0^0.

Теперь понятно, как выглядит $2s$-я строка треугольника. Крайние элементы в ней — единицы, остальные элементы — нули, кроме центрального элемента, который равен 2, как сумма двух вышестоящих единиц. Отсюда получаем, что снизу от $2s$-й строки находятся два серых нулевых треугольника, по краям от них — треугольники Δ_2^0 и Δ_2^2, идентичные Δ_0^0, а между ними — треугольник Δ_2^1, у которого вдоль боковых сторон расположены двойки. Как нетрудно понять, это значит, что $\Delta_2^1 = 2\cdot\Delta_0^0$.

Ну и так далее.

1.4. Этот сюжет мы взяли в статье [21], где некоторые факты о биномиальных коэффициентов доказываются с помощью рассмотрения Ханойской башни и графа TH_n.

Пусть на первом стержне самый верхний диск имеет диаметр a, на втором — диаметр b, на третьем — c, $a < b < c$, тогда в этом положении есть три возможных хода: с a на b или на c, либо с b на c; аналогично имеется три хода, если диски занимают лишь два стержня. Если же все диски находятся на одном стержне, возможных ходов только два, обозначим такие конфигурации A_1, A_2, A_3 по номеру стержня, на который нанизаны диски.

Заметим, что 2^s-я строка треугольника Паскаля состоит из одних единиц — это следует из задачи 1.2 или проверяется непосредственно с помощью формулы Лежандра (4). Отсюда следует, что граф P_n имеет поворотную симметрию третьего порядка, поскольку основное соотношение

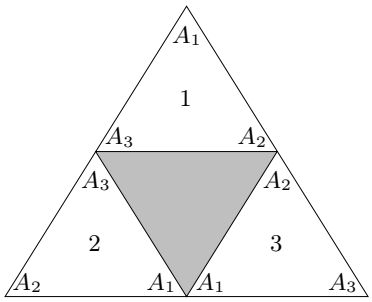


Рис. 3.

$C_n^{k-1} + C_n^k = C_{n+1}^k$, при помощи которого мы строим треугольник Паскаля "сверху вниз", в арифметике по модулю 2 равносильно соотношениям $C_n^{k-1} = C_n^k + C_{n+1}^k$ и $C_n^k = C_n^{k-1} + C_{n+1}^k$, с помощью которых можно аналогично построить треугольник Паскаля "слева снизу — вправо вверх" и "справа снизу — влево вверх". Кроме того, отсюда следует (из предыдущей задачи), что треугольник Паскаля в 2 раза большего размера содержит три копии исходного треугольника.

Докажем по индукции, что существует биекция между TH_n и P_n, при которой вершинам треугольника P_n соответствуют конфигурации A_1, A_2, A_3. База $n = 1$ очевидна.

Докажем переход. Пусть мы уже умеем строить биекцию между TH_n и P_n. Рассмотрим 2-арифметический треугольник треугольник Паскаля со стороной 2^{n+1}, он содержит три копии треугольника со стороной 2^n. Пронумеруем копии и разметим их вершины, как показано на рис. 3. Рассмотрим все положения Ханойской башни, в которых самый крупный диск находится на стержне i. Если мы не двигаем этот диск, то все эти положения и перекладывания остальных дисков задают граф, изоморфный TP_n. С помощью уже имеющейся биекции отождествим этот граф с графом P_n, расположенным в i-й копии треугольника, причем потребуем, чтобы конфигурации A_j были отождествлены в соответствии с разметкой вершин. Перемещение самого крупного диска, скажем, с первого стержня на второй возможно, только если все остальные диски находятся на третьем стержне. Это в точности соответствует ребру, соединяющему соседние вершины A_3 на левой боковой стороне треугольника, аналогично обстоят дела с другими перемещениями самого большого диска. Таким образом, построенное соответствие действительно дает изоморфизм графов TP_{n+1} и P_n.

1.5. Биекция с Ханойской башней дает простую явную формулу (когда число строк – степень двойки): в первых 2^k строках треугольника Паскаля содержится 3^k единиц. Та же формула легко доказывается по индукции из рекуррентности задачи 1.3. Пользуясь этим фактом легко получаем оценку. Так как $10^6 < 2^{20}$, количество элементов в этих строках равно $\frac{1}{2} \cdot 10^6(10^6 + 1)$, а количество единиц не превосходит 3^{20}. Доля единиц не превосходит $\frac{2 \cdot 3^{20}}{10^6(10^6+1)} \ll 0.01$.

1.6. Мы взяли это утверждение в обзоре [18].

Р е ш е н и е 1 ([CSTTVZ]). При $p = 2$ утверждение задачи легко проверяется. Будем далее считать, что p — нечетное простое. Пусть $n = x(p-1) + k$. Будем доказывать утверждение индукцией по x.

База $x = 0$ тривиальна: $C_k^j \equiv C_k^j \pmod p$.

Для доказательства перехода воспользуемся свойством биномиальных коэффициентов

$$C_{a+b}^s = \sum_i C_a^{s-i} C_b^i \qquad \text{(суммирование в естественных границах)},$$

которое выражает два способа подсчета числа вариантов взять s шаров из коробки, в которой лежит a черных и b белых шаров. Пусть $n = m + (p-1)$. Заметим, что

$$C_n^{\ell(p-1)+j} = C_{m+(p-1)}^{\ell(p-1)+j} = \sum_{i=0}^{p-1} C_m^{\ell(p-1)+j-i} C_{p-1}^i \equiv \sum_{i=0}^{p-1} (-1)^i C_m^{\ell(p-1)+j-i} \pmod p$$

(последнее сравнение — по утверждению задачи 1.1 а). Отметим, что в последней сумме первое и

последнее слагаемое присутствуют со знаком плюс. Преобразуем теперь интересующую нас сумму.

$$\sum_\ell C_n^{\ell(p-1)+j} \equiv$$
$$\equiv \left(C_m^j - C_m^{j-1} + \ldots\right) + \left(C_m^{p-1+j} - C_m^{p-1+j-1} + \ldots + C_m^j\right) + \left(C_m^{2(p-1)+j} - C_m^{2(p-1)+j-1} + \ldots + C_m^{(p-1)+j}\right) + \ldots$$
$$= \sum_{i=0}^{m} (-1)^i C_m^i + \sum_\ell C_m^{\ell(p-1)+j} \pmod p.$$

Здесь первая сумма равна нулю, а вторая по предположению индукции сравнима с $C_k^j \pmod p$. ЧТД

Решение 2 (основное рекуррентное тождество, [J], [T]). Утверждение доказывается индукцией по n. База $n \leqslant p-1$ тривиальна: левая часть содержит всего одно слагаемое — то же самое, что и в правой части. Переход:

$$C_n^j + C_n^{(p-1)+j} + \ldots = \left(C_{n-1}^j + C_{n-1}^{j-1}\right) + \left(C_{n-1}^{(p-1)+j} + C_{n-1}^{(p-1)+j-1}\right) + \ldots =$$
$$= \left(C_{n-1}^j + C_{n-1}^{(p-1)+j} + \ldots\right) + \left(C_{n-1}^{j-1} + C_{n-1}^{(p-1)+j-1} + \ldots\right) \equiv C_{k-1}^j + C_{k-1}^{j-1} = C_k^j \pmod p.$$

Но тут следует иметь в виду, что в формулировке утверждения в случае, когда параметры j и k делятся на $p-1$, они приравниваются к $p-1$, а не к 0. Таким образом, выписанное соотношение требует отдельного рассмотрения при $j = 1$ или $k = 1$. Мы ограничимся рассмотрением частного случая, которое проясняет ситуацию. Пусть $p = 5$, $j = 1$ и мы доказываем переход к $n = 13$. Имеем

$$C_1^1 \stackrel{?}{\equiv} C_{13}^1 + C_{13}^6 + C_{13}^{11} = \left(C_{12}^1 + C_{12}^6 + C_{12}^{11}\right) + \left(C_{12}^0 + C_{12}^5 + C_{12}^{10}\right)$$

Здесь первая скобка дает по индукционному предположению остаток C_4^1 (а вовсе не C_0^1, как могло показаться по предыдущему вычислению). Во второй скобке первое слагаемое не участвует в индукционном предположении, а сумма остальных сравнима с C_4^0. Записывая для ясности $p-1$ вместо 4, получаем, что вся сумма сравнима с $C_{n-1}^0 + C_{p-1}^1 + C_{p-1}^0 \equiv C_1^1 \pmod p$, что и требуется.

Решение 3 (алгебраическое рассуждение с теоремой Люка, [18]). Индукция по n. База $n \leqslant p-1$ тривиальна. Пусть теперь $n \geqslant p$, запишем все встречающиеся параметры в системе счисления по основанию p, сумму цифр числа m будем обозначать $\sigma_p(m)$. Очевидно, если $m \equiv j \pmod p$, то $\sigma_p(m) \equiv j \pmod p$. Тогда по теореме Люка интересующая нас сумма равна

$$\sum C_{n_0}^{m_0} C_{n_1}^{m_1} \ldots C_{n_d}^{m_d} \pmod p,$$

где суммирование распространяется на все $m = \overline{m_d \ldots m_1 m_0} \leqslant n$, для которых $\sigma_p(m) \equiv j \pmod p$. Эта сумма в точности равна сумме коэффициентов при x^j, x^{j+p-1}, $x^{j+2(p-1)}$, ... в выражении

$$(1+x)^{n_0}(1+x)^{n_1} \ldots (1+x)^{n_d} = (1+x)^{\sigma_p(n)}.$$

Но очевидно, что указанная сумма коэффициентов равна

$$\sum_{\substack{1 \leqslant r \leqslant \sigma_p(n) \\ r \equiv j \pmod{p-1}}} C_{\sigma_p(n)}^r,$$

которая удовлетворяет индукционному предположению, так как $1 \leqslant \sigma_p(n) \leqslant n-1$, и дает нужное нам сравнение, поскольку $\sigma_p(n) \equiv n \equiv j \pmod p$.

Решение 4 (немного здравого смысла и линейной алгебры, [Д]). Многочлены x, x^2, ..., x^{p-1} линейно независимы над $\mathbb{Z}_p$ и образуют базис в пространстве функций $f\colon \mathbb{Z}_p \to \mathbb{Z}_p, f(0) = 0$. По малой теореме Ферма $(1+x)^n \equiv (1+x)^k \pmod p$. Редуцируя левую часть с помощью соотношений $x^{i+a(p-1)} \equiv x^i$, получаем, что интересующая нас сумма как элемент $\mathbb{Z}_p$ равна коэффициенту при x^j в правой части, т. е. C_k^j.

2 *Арифметический треугольник и делимость*

2.1. a) Это результат Робертса [27]. Обозначим количество единиц в первых 3^k строках через a_k, а количество двоек b_k — через b_k. Пользуясь рекуррентностью из задачи 1.3, получаем соотношения:

$$a_{k+1} = 5a_k + b_k, \qquad b_{k+1} = 5b_k + a_k.$$

Отсюда утверждение задачи легко следует по индукции.

b) Ответ: $\frac{1}{2} \cdot 5^k(5^k + 1) - 15^k$. Обозначая искомую величину a_k, аналогично предыдущей задаче получаем соотношение

$$a_{k+1} = 15a_k + 10 \cdot \frac{5^k(5^k - 1)}{2}.$$

Поскольку в целом треугольник содержит $\frac{5^k(5^k+1)}{2}$ элементов, естественно ввести замену переменных $a_k = \frac{5^k(5^k+1)}{2} - b_k$. Тогда для переменной b_k предыдущее соотношение записывается в виде $b_{k+1} = 15b_k$.

c) Ответ: $\left(\frac{p(p+1)}{2}\right)^k$. Это результат Файна [13]. Он аналогично предыдущим пунктам получается по индукции из рекуррентности задачи 1.3.

2.2. Решение 1. Индукция по α_1. База для $\alpha_1 = 0, 1$ легко проверяется. Пусть для всех $\alpha_1 < a$ утверждение уже доказано. Докажем его для $\alpha_1 = a$. Очевидно, $\tilde{m} - 2^{\alpha_1} < 2^{\alpha_1}$. Пусть в обозначениях задачи 1.3 $s = 2^{\alpha_1}$. Числу $\tilde{m} = 2^{\alpha_2} + 2^{\alpha_3} + \ldots + 2^{\alpha_r}$ соответствует строчка в треугольнике Δ_0^0. В этой строке и в строках над ней по индукционному предположению содержится

$$3^{\alpha_2} + 2 \cdot 3^{\alpha_3} + \ldots + 2^{r-2} \cdot 3^{\alpha_r} \tag{2}$$

единиц. Тогда числу $m = \tilde{m} + 2^{\alpha_1}$ соответствует строчка, пересекающая треугольники Δ_0^1 и Δ_1^1 (идентичные треугольнику Δ_0^0, поскольку у нас 2-арифметика). В этой строке и выше находится целиком треугольник Δ_0^0 (в нем по предположению индукции 3^{α_1} единиц) и два неполных треугольника Δ_0^1 и Δ_1^1, в каждом из которых число единиц задается формулой (2). В сумме получаем

$$3^{\alpha_1} + 2(3^{\alpha_2} + 2 \cdot 3^{\alpha_3} + \ldots + 2^{r-2} \cdot 3^{\alpha_r})$$

единиц, что и требуется.

Решение 2 (комбинаторный смысл коэффициентов — разбиваем на слои, [T]).

Лемма 1. Пусть число единиц в k-й строке равно 2^r (или, что то же самое, бинарная запись числа k содержит r единиц) и пусть $\alpha_1 > \alpha_2 > \cdots > \alpha_m$, $2^{\alpha_m} > k$. Тогда число единиц в строке с номером $2^{\alpha_1} + 2^{\alpha_2} + \ldots + 2^{\alpha_m} + k$ равно 2^{m+r}.

Доказательство. Очевидно, бинарная запись числа $2^{\alpha_1} + 2^{\alpha_2} + \ldots + 2^{\alpha_m} + k$ содержит $m + r$ единиц и тогда в строке треугольника Паскаля с этим номером 2^{m+r} единиц. □

Лемма 2. Суммарное количество единиц в строках с номерами

$$2^{\alpha_1} + 2^{\alpha_2} + \ldots + 2^{\alpha_{m-1}}, \quad 2^{\alpha_1} + 2^{\alpha_2} + \ldots + 2^{\alpha_{m-1}} + 1, \quad \ldots, \quad 2^{\alpha_1} + 2^{\alpha_2} + \ldots + 2^{\alpha_{m-1}} + 2^{\alpha_m} - 1,$$

равно $2^k 3^{\alpha_m}$.

Доказательство. По лемме 1 количество единиц в строке с номером $2^{\alpha_1} + 2^{\alpha_2} + \ldots + 2^{\alpha_{m-1}} + i$ равно $2^k x_i$, где x_i — количество единиц в i-й строке. Тогда суммарное число единиц в упомянутых строках равно $2^k \sum x_i$. Но $\sum x_i$ — это число единиц в первых $2^{\alpha_m} - 1$ строках треугольника Паскаля, оно равно 3^{α_m} (это нам известно, например, из задачи 1.4). □

Осталось просуммировать по m количества единиц из леммы 2.

2.3. Мы взяли утверждение задачи из статьи Винберга [1], а решение из статьи Гранвилля [18]. Утверждение выводится из теоремы Люка с помощью следующего наблюдения (тоже упомянутого в [1]): биномиальный коэффициент C_n^k нечетен в том и только том случае, когда единицы в двоичном разложении числа k могут стоять лишь в тех разрядах, где стоят единицы в записи числа n. Отсюда

сразу следует, что $P_n = \sum 2^k$, где суммирование распространяется на все числа k, описанные в предыдущем предложении. В обозначениях формулы (1) при $p = 2$ положим $S_n = \{i : n_i = 1\}$. Тогда

$$P_n = \sum_{I \subseteq S_n} \prod_{i \in I} 2^{2^i} = \prod_{i \in S_n} F_i.$$

2.4. Этот результат Файна [13], 1947 г, — простое следствие теоремы Куммера. Чтобы биномиальный коэффициент C_n^k не делился на p, не должно быть переносов при сложении чисел k и $n-k$, записанных в системе счисления по основанию p. При фиксированном n это означает, что выбор i-й цифры p-ичной записи числа k можно сделать $n_i + 1$ способом.

2.5. a) Это сразу следует из формулы, доказанной в предыдущей задаче, поскольку речь идет о строке, в которой ровно два элемента не делятся на p.

b) [13]. Если $(n+1) \vdots p^d$, то $n = \overline{a(p-1)(p-1)\dots(p-1)}$ в системе счисления по основанию p. Тогда для каждого k, $0 \leqslant k \leqslant n$, каждая цифра числа k не превосходит соответствующей цифры числа n. Тогда все биномиальные коэффициенты $C_{n_i}^{k_i}$ не равны нулю (в том числе, по модулю p) и по теореме Люка C_n^k не делится на p.

В обратную сторону. Пусть все биномиальные коэффициенты C_n^k не делятся на p, но число n является числом вида $\overline{a(p-1)(p-1)\dots(p-1)}$. Это значит, что одна из цифр, скажем n_i, меньше $p-1$. Возьмем $k = (p-1)\cdot p^i$. Тогда $k_i = p-1$, следовательно, $C_{n_i}^{k_i} = 0$ и по теореме Люка C_n^k делится на p. Противоречие.

2.6. Это известное утверждение мы почерпнули в [12].

Решение 1. Допустим, что $C_n^{k-1} \not\vdots p$ и $C_n^k \not\vdots p$, но при этом $C_{n+1}^k = (C_n^{k-1} + C_n^k) \vdots p$. Тогда $C_n^k \equiv -C_n^{k-1} \pmod p$. Так как оба биномиальных коэффициента не делятся на p, мы можем сократить правую и левую части. Получим $\frac{n-k+1}{k} \equiv -1 \pmod p$, откуда $n+1 \equiv 0 \pmod p$.

Решение 2 ([K]). Хотя утверждение выглядит очень естественным, напоминая нам основное тождество для биномиальных коэффициентов, часть "$C_n^{k-1} \not\vdots p$" в нем лишняя. Действительно, если $(n+1) \not\vdots p$, то $0 \leqslant n_0 \leqslant p-2$. Поскольку $C_n^k \not\vdots p$, то по теореме Куммера при всех i верно неравенство $k_i \leqslant n_i$. Но тогда аналогичные неравенства верны и для пары чисел k и $n+1$, поскольку у числа $n+1$ те же цифры, что и у n, кроме цифры в самом младшем разряде, которая у числа $n+1$ на 1 больше. Следовательно, $C_{n+1}^k \not\vdots p$.

2.7. [2]. Сразу следует из теоремы Люка и задачи 1.1.a)

2.8. Задача из статьи Винберга [1]. Индукция по числу цифр. База тривиальна. Для перехода добавляем очередную цифру в конец числа. В силу нечетности биномиального коэффициента $n_i \geqslant k_i$. Пользуясь рекуррентностью $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$, перебирая разные варианты четности n и k с помощью теоремы Куммера и задачи 4.6a) сводим все к индукционному предположению.

Например, при нечетном $n = 2\ell + 1$ и четном $k = 2m$, если $k_1 = 1$, то $k = \dots 10$, $n = \dots 11$ (двоичные записи), Тогда $(n-k) = \dots 01$ (потому что по теореме Куммера не должно было быть переносов), $(k-1)_2 = \dots 01$, значит, по теореме Куммера при сложении $(k-1)_2 + (n-k)_2$ есть ровно 1 перенос, т. е. $C_{n-1}^{k-1} \equiv 2 \pmod 4$, откуда

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k \equiv -C_{n-1}^k = -C_{2\ell}^{2m} \equiv -C_\ell^m \pmod 4,$$

последнее — по задаче 4.6a). Этот минус в точности соответствует множителю $(-1)^{k_0 n_1 + k_1 n_0}$.

2.9. Задача из статьи Винберга [1]. Утверждение следует из результата предыдущей задачи. Если в записи n нет двух единиц подряд, то все показатели $k_{i-1}n_i + k_i n_{i-1}$ равны нулю и все биномиальные коэффициенты дают остаток 1 при делении на 4. Если же запись числа n содержит участок из единиц, начинающийся с $n_j = 1$, то у половины нечетных биномиальных коэффициентов $k_j = 0$, а у другой половины $k_j = 1$ и, как нетрудно видеть по формуле из предыдущей задачи, по модулю 4 эти половины отличаются знаком.

2.10. Этому запутанному сюжету посвящены две статьи в Monthly [19, 20].

2.11. Эта задача Д.Джукича была в 2002 г. на олимпиаде 239 школы г. Санкт-Петербурга, а потом засветилась в шорт-листе IMO-2008.

Поскольку все биномиальные коэффициенты из условия задачи нечетны (по теореме Люка), для доказательства утверждения достаточно проверить, что все числа $C_{2^n-1}^1$, $C_{2^n-1}^3$, $\ldots$, $C_{2^n-1}^{2^n-1}$ дают разные остатки при делении на 2^n. Дальше можно действовать по-разному.

Р е ш е н и е 1 ([Д]). Предположим противное, пусть $C_{2^n-1}^k \equiv C_{2^n-1}^m \pmod{2^n}$ при нечетных k и m, $k > m$. Заметим, что

$$C_{2^n-1}^k = C_{2^n}^k - C_{2^n-1}^{k-1} = C_{2^n}^k - C_{2^n}^{k-1} + C_{2^n-1}^{k-2} = \cdots = C_{2^n}^k - C_{2^n}^{k-1} + C_{2^n}^{k-2} - \ldots - C_{2^n}^{m+1} + C_{2^n-1}^m\,.$$

В частности,

$$C_{2^n}^k - C_{2^n}^{k-1} + C_{2^n}^{k-2} - \ldots - C_{2^n}^{m+1} \equiv 0 \pmod{2^n}\,.$$

Теорема Куммера позволяет для каждого r легко вычислить показатель $\operatorname{ord}_2 C_{2^n}^r$, а именно, если $\operatorname{ord}_2 r = a$, то при сложении r и $2^n - r$ произойдет $n - a$ переносов (это очевидно из алгоритма сложения столбиком), и значит, $\operatorname{ord}_2 C_{2^n}^r = n - a$. В частности, $C_{2^n}^r$ делится на 2^n при нечетном r, что позволяет отбросить в последнем сравнении половину слагаемых:

$$C_{2^n}^{k-1} + C_{2^n}^{k-3} + \ldots + C_{2^n}^{m+1} \equiv 0 \pmod{2^n}\,.$$

Другое следствие из приведенных рассуждений состоит в том, что у всех слагаемых $C_{2^n}^i$ в левой части параметр i четный и поэтому $\operatorname{ord}_2 C_{2^n}^x < n$. Докажем теперь, что выполнение этого сравнения невозможно. Выберем x, для которого $\operatorname{ord}_2 C_{2^n}^x$ имеет минимальное значение. Так как $\operatorname{ord}_2 C_{2^n}^x < n$, но при этом вся сумма делится на 2^n, найдется y, для которого $\operatorname{ord}_2 C_{2^n}^x = \operatorname{ord}_2 C_{2^n}^y$. Но тогда бинарные записи чисел x и y оканчиваются на одинаковое число нулей, поэтому между x и y найдется число z, оканчивающееся на большее число нулей. Тогда $\operatorname{ord}_2 C_{2^n}^z < \operatorname{ord}_2 C_{2^n}^x$, что противоречит минимальности.

Р е ш е н и е 2 ([CSTTVZ]). Предположим противное, пусть нашлись числа k и ℓ, $k \neq \ell$, такие что $C_{2^n-1}^{2k+1} \equiv C_{2^n-1}^{2\ell+1} \mod 2^n$, $0 \leqslant k, \ell \leqslant 2^n - 1$. Кроме того, мы будем вести рассуждения по индукции, считая, что для меньших значений n утверждение задачи уже доказано. Заметим, что

$$\begin{aligned} C_{2^n-1}^{2k+1} &= \left(\frac{2^n}{1} - 1\right)\left(\frac{2^n}{2} - 1\right)\ldots\left(\frac{2^n}{2k+1} - 1\right) = \\ &= \left(\frac{2^n}{1} - 1\right)\left(\frac{2^n}{3} - 1\right)\ldots\left(\frac{2^n}{2k+1} - 1\right)\cdot\left(\frac{2^{n-1}}{1} - 1\right)\left(\frac{2^{n-1}}{2} - 1\right)\ldots\left(\frac{2^{n-1}}{k} - 1\right) = \qquad (3) \\ &= \left(\frac{2^n}{1} - 1\right)\left(\frac{2^n}{3} - 1\right)\ldots\left(\frac{2^n}{2k+1} - 1\right)\cdot C_{2^{n-1}-1}^k \equiv \\ &\equiv (-1)^{k+1} C_{2^{n-1}-1}^k \pmod{2^n}\,. \end{aligned}$$

И аналогично $C_{2^n-1}^{2\ell+1} \equiv (-1)^{\ell+1} C_{2^{n-1}-1}^{\ell} \pmod{2^n}$. По индукционному предположению, отсюда следует, что k и ℓ не могут быть оба нечетными. Кроме того, в силу симметрии $C_{2^n-1}^r = C_{2^n-1}^{2^n-1-r}$ утверждение задачи означает также, что все биномиальные коэффициенты с четными показателями — $C_{2^n-1}^{2r}$ — тоже попарно различны и по модулю 2^n образуют то же множество, что и биномиальные коэффициенты с нечетными показателями. Поэтому k и ℓ не могут быть оба четными.

Осталось разобрать случай, когда k и ℓ разной четности, пусть $k = 2a + 1$, $\ell = 2b$. Тогда

$$C_{2^{n-1}-1}^{2a+1} + C_{2^{n-1}-1}^{2b} \equiv 0 \pmod{2^n}\,.$$

При $a = b$ это сравнение невозможно, так как $C_{2^{n-1}-1}^{2a}$ нечетно и

$$C_{2^{n-1}-1}^{2a+1} + C_{2^{n-1}-1}^{2a} = C_{2^{n-1}-1}^{2a}\left(1 + \frac{2^{n-1} - 1 - 2a}{2a+1}\right) = C_{2^{n-1}-1}^{2a}\cdot\frac{2^{n-1}}{2a+1} \equiv 2^{n-1} \pmod{2^n}\,.$$

Если же $b \neq a$, то $C_{2^{n-1}-1}^{2a} \neq C_{2^{n-1}-1}^{2b}$ по индукционному предположению и так как $C_{2^{n-1}-1}^{2a} + C_{2^{n-1}-1}^{2a+1}$ делится на 2^{n-1}, сумма $C_{2^{n-1}-1}^{2b} + C_{2^{n-1}-1}^{2a+1}$ не может делиться на 2^{n-1}.

2.12. Эту задачу нам сообщил А. Белов. Заметим, что

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

и таким образом, C_{2n}^{n+k} имеет много общих множителей с C_{2n}^{n}, кроме тех, которые сократились со знаменателем дроби. Заметим, что знаменатель не превосходит $(2n)^k$. Напишем аналогичные равенства для всех биномиальных коэффициентов $C_{2n}^{n+k_1}$, $C_{2n}^{n+k_2}$, …, $C_{2n}^{n+k_{100}}$. Наибольший общий делитель всех знаменателей в правых частях этих равенств не превосходит $(n+1)(n+2)\dots\big(n+[\varepsilon\sqrt{n}\,]\big) < (2n)^{\varepsilon\sqrt{n}}$. Но при больших n биномиальный коэффициент C_{2n}^{n} — существенно более крупное число, поэтому даже если сократить его на наибольший общий делитель всех знаменателей, останется весьма крупное частное, которое и будет общим делителем всех ста биномиальных коэффициентов.

Поясним последнее соображение с помощью оценки. Заметим, что

$$C_{2n}^{n} = \frac{2n}{n}\cdot\frac{2n-1}{n-1}\dots\frac{n+1}{1} > 2^n.$$

При этом $(2n)^{100\varepsilon\sqrt{n}} = 2^{\varepsilon\sqrt{n}\log_2 n+\varepsilon\sqrt{n}}$. Очевидно, для каждого фиксированного ε существует N, такое что при всех $n > N$ будет выполнено неравенство

$$\frac{n}{2} > \varepsilon\sqrt{n}\log_2 n + \varepsilon\sqrt{n}.$$

Если для таких n поделить C_{2n}^{n} на НОД всех знаменателей, частное будет не меньше $2^{n/2}$.

2.13. a) Задача предлагалась в 1977 г. на Ленинградской олимпиаде школьников.

Р е ш е н и е 1 (без теоремы Куммера). Мы приводим решение из замечательной книжки [4].

Допустим, что все эти числа делятся на m. Тогда числа

$$\begin{aligned} C_{n+k-1}^{k-1} &= C_{n+k}^{k} - C_{n+k-1}^{k}\,,\\ C_{n+k-2}^{k-1} &= C_{n+k-1}^{k} - C_{n+k-2}^{k}\,,\\ &\dots\\ C_{n}^{k-1} &= C_{n+1}^{k} - C_{n}^{k} \end{aligned}$$

также делятся на m. Аналогично, на m делятся и все числа C_{n+i}^{j}, где $i \leqslant j$ — произвольные неотрицательные целые числа. Но среди них есть число C_n^0 $(i = j = 0)$, которое равно 1. Противоречие.

Р е ш е н и е 2 (теорема Куммера). Пусть p — простой множитель числа m. Проверим, что одно из чисел C_n^k, C_{n+1}^k, …, C_{n+k}^k не делится на p. Запишем k в системе счисления по основанию p. По теореме Куммера достаточно найти такое число ℓ (где $n-k \leqslant \ell \leqslant n$), чтобы сложение $k+\ell$ в системе счисления по основанию p выполнялось без переносов, тогда биномиальный коэффициент $C_{k+\ell}^{k}$ не будет делиться на p.

Это сделать совсем нетрудно. Мы ограничимся рассуждением на конкретном примере. Пусть $p = 7$, $k = 133$ (здесь и далее числа записаны в семиричной системе счисления). Поскольку диапазон, в котором мы ищем число ℓ, содержит $k+1$ число, нам всегда удастся выбрать ℓ так, чтобы число $k+\ell$ было одним из чисел следующего вида

$$\dots 133,\quad \dots 233,\quad ,\dots,\quad \dots 633.$$

(Напомним, что цифра 6 в нашем примере самая старшая.) Тогда очевидно, что при сложении $k+\ell$ не было ни одного переноса.

b) Утверждение взято из [2]. Такие n нетрудно построить с помощью теоремы Куммера. Пусть $\operatorname{ord}_p m = s$, и запись числа k в системе счисления по основанию p содержит $d+1$ цифр. Пусть $n \vdots p^{d+s+1}$. Тогда числа $n-k$, $n-k+1$, …, $n-1$ содержат в разрядах с $(d+2)$-го по $(d+s+2)$-й цифры $(p-1)$, поэтому при сложении этих чисел с k в указанных разрядах будут возникать переносы. Таким образом, по теореме Куммера получаем, что интересующие нас биномиальные коэффициенты все делятся на p^s.

Поскольку условия, наложенные на n, легко совмещаются для разных p, мы получаем отсюда требуемое.

3 Обобщение теорем Вильсона и Люка

3.1. Как известно, $\operatorname{ord}_p(n!) = \sum_k \left[\frac{n}{p^k}\right]$. Если $n = n_d p^d + n_{d-1}p^{d-1} + \ldots + n_1 p + n_0$ — запись в системе счисления по основанию p, то $\left[\frac{n}{p^k}\right] = n_d p^{d-k} + n_{d-1}p^{d-k-1} + \ldots + n_{k+1}p + n_k$ и формулу для $\operatorname{ord}_p(n!)$ можно записать в виде

$$\operatorname{ord}_p(n!) = \sum_{k=1}^{d}\left(\sum_{i=k}^{d} n_i p^{i-k}\right) = \sum_{i=1}^{d} n_i(p^{i-1}+p^{i-2}+\ldots+p+1) = \sum_{i=1}^{d} n_i\frac{p^i-1}{p-1} = \frac{\sum\limits_{i=0}^{d} n_i p^i - \sum\limits_{i=0}^{d} n_i}{p-1}.$$

Мы получили в точности требуемое выражение.

Утверждение задачи также нетрудно доказать индукцией по n, см. [5].

3.2. а) Разбивая множители, составляющие выражение $n!$, на группы по $(p-1)$ штук, получаем

$$(n!)_p = \prod_{k=0}^{[\frac{n}{p}]-1}\big((kp+1)\cdot(kp+2)\cdots(kp+p-1)\big)\cdot\big([\tfrac{n}{p}]p+1\big)\big([\tfrac{n}{p}]p+2\big)\ldots\big([\tfrac{n}{p}]p+n_0\big) \equiv (-1)^{[\frac{n}{p}]} n_0! \pmod p.$$

б) Это утверждение встречается у Гаусса [15]. В произведение $(p^q!)_p$ вместе с каждым сомножителем входит и его обратный по модулю p^q, и произведение этой пары равно 1 по модулю p^q. Таким образом, нам следует лишь проследить за теми множителями m, которые совпадают со своими обратными, т.е. удовлетворяют сравнению

$$m^2 \equiv 1 \pmod{p^q}.$$

Для нечетного p сравнение имеет 2 решения: ± 1. Для $p=2$, $q \geqslant 3$ сравнение имеет еще пару решений: $2^{q-1} \pm 1$.

с) Так как $n! = (n!)_p \cdot p^{[\frac{n}{p}]}\big([\frac{n}{p}]\big)!$, утверждение легко доказывается по индукции с помощью сравнения из п. а).

3.3. Мы взяли утверждение со странички Гранвилля [17]. Помимо теоремы Куммера, широко известна прямая и не столь симпатичная формула для числа ℓ (формула Лежандра):

$$\ell = \operatorname{ord}_p(C_n^k) = \left(\left[\frac{n}{p}\right] - \left[\frac{k}{p}\right] - \left[\frac{r}{p}\right]\right) + \left(\left[\frac{n}{p^2}\right] - \left[\frac{k}{p^2}\right] - \left[\frac{r}{p^2}\right]\right) + \ldots \tag{4}$$

Обозначим для краткости $\tilde{n} = [n/p]$ и т. п. и напишем формулу для биномиального коэффициента, собрав отдельно все множители, делящиеся на p:

$$C_n^k = \frac{(n!)_p}{(k!)_p (r!)_p}\cdot\frac{p^{[n/p]}}{p^{[k/p]}\cdot p^{[r/p]}}\cdot\frac{\tilde{n}!}{\tilde{k}!\cdot\tilde{r}!}.$$

Здесь первая дробь может быть преобразована по модулю p в соответствии с обобщенной теоремой Вильсона (задача 3.2, б) к выражению $\frac{n_0!}{k_0! r_0!}$, третья дробь позволяет действовать по индукции, а средняя дробь (и знак из обобщенной теоремы Вильсона, который мы не упомянули) по формуле (4) даст все нужные выражения, содержащие ℓ.

3.4. а) Раскрывая скобки в выражении $(1+x)^{p^d}$, мы можем воспользоваться тем, что при $1 \leqslant k \leqslant p^d-1$ биномиальный коэффициент $C_{p^d}^k$ делится на p (аналогично задаче 1.1 или по теореме Куммера).

b) Положим $n = n'p + n_0$, $k = k'p + k_0$. По утверждению п. а) $(1+x)^{pn'} \equiv (1+x^p)^{n'} \pmod p$ Тогда

$$(1+x)^n = (1+x)^{pn'}(1+x)^{n_0} \equiv (1+x^p)^{n'}(1+x)^{n_0} \pmod p.$$

Указанное сравнение надо понимать в том смысле, что мы преобразовываем коэффициенты многочлена с целыми коэффициентами с точки зрения их делимости на p. Коэффициент при x^k в левой части равен C_n^k. При раскрытии скобок в правой части мы видим, что все показатели в первой скобке делятся на p, поэтому единственный способ получить одночлен $x^{pk'+k_0}$ — это перемножить

$x^{pk'}$ из первой скобки и x^{k_0} из второй. Итоговый коэффициент будет равен $C_{n'}^{k'}C_{n_0}^{k_0}$. Таким образом, $C_n^k = C_{n'}^{k'}C_{n_0}^{k_0}$, откуда теорема Люка следует по индукции.

3.5. a, b) Простое следствие теоремы Куммера.

3.6. [9]. В следующем вычислении мы используем то, что $C_{n_i}^{k_i} = 0$ при $k_i > n_i$; это позволяет, применив теорему Люка, отбросить при суммировании большое число слагаемых.

$$f_{n,a} = \sum_{k=0}^{n}(C_n^k)^a \equiv \sum_{k_d=0}^{n_d}\sum_{k_{d-1}=0}^{n_{d-1}} \cdots \sum_{k_0=0}^{n_0}\prod_{i=0}^{d}(C_{n_i}^{k_i})^a \equiv \prod_{i=0}^{d}\sum_{k_i=0}^{n_i}(C_{n_i}^{k_i})^a \equiv \prod_{i=0}^{d} f_{n_i,a} \pmod p.$$

4 *Вариации на тему теоремы Волстенхолма*

4.1. Это упражнение на чтение статьи. Утверждение доказано в статье Винберга, но доказательство не выделено явно. Заметим, что

$$2\sum_{i=1}^{p-1}\frac{1}{i} = \sum_{i=1}^{p-1}\frac{1}{i} + \frac{1}{p-i} = p\sum_{i=1}^{p-1}\frac{1}{i(p-i)}\,.$$

Таким образом, рассматриваемая сумма делится на p. Так как по модулю p выражения $\frac{1}{i}$ и $-\frac{1}{p-i}$ равны, нам остается проверить, что

$$\sum_{i=1}^{p-1}\frac{1}{i^2} \equiv 0 \pmod p.$$

Или, поскольку $\frac{1}{1^2}, \frac{1}{2^2}, \ldots, \frac{1}{(p-1)^2}$ — это тот же набор остатков[1], что и $1^2, 2^2, \ldots, (p-1)^2$, достаточно проверить, что

$$\sum_{i=1}^{p-1} i^2 \equiv 0 \pmod p. \tag{5}$$

Пусть $\sum\limits_{i=1}^{p-1} i^2 \equiv s \pmod p$. При $p > 5$ всегда можно выбрать остаток a, такой что $a^2 \not\equiv 1 \pmod p$. Тогда множества $\{1, 2, \ldots, p-1\}$ и $\{a, 2a, \ldots, (p-1)a\}$ совпадают (доказательство как в сноске) и

$$s \equiv \sum_{i=1}^{p-1} i^2 = \sum_{i=1}^{p-1}(ai)^2 = a^2\sum_{i=1}^{p-1} i^2 \equiv a^2 s \pmod p\,.$$

Поэтому $s \equiv 0 \pmod p$.

Разумеется, этот факт нетрудно доказать непосредственно, пользуясь соображением $\frac{1}{x} \equiv x^{\varphi(m)-1} \pmod m$. Мы используем эту технику в третьем решении следующей задачи.

4.2. Ответ: $2k+2$. Эта задача А. С. Голованова предлагалась на олимпиаде Туймаада в 2012 г. Мы приводим три решения. Отметим, что при $p = 4k+3$ уравнение $x^2 + 1 = 0$ не имеет решений в поле остатков по модулю p, следовательно, знаменатели всех рассматриваемых дробей не равны нулю.

Р е ш е н и е 1. Обозначим $a_i = i^2 + 1$, для $i = 0, \ldots, p-1$. Тогда рассматриваемое выражение равно

$$\frac{\sigma_{p-1}(a_0, a_1, \ldots, a_{p-1})}{\sigma_p(a_0, a_1, \ldots, a_{p-1})},$$

где σ_i — основной симметрический многочлен степени i. Найдем многочлен, корнями которого являются числа a_i, т. е.

$$\prod_{i=0}^{p-1}(x - 1 - i^2).$$

[1] Напомним доказательство: $\frac{1}{1}, \frac{1}{2}, \ldots, \frac{1}{(p-1)}$ и 1, 2, …, $(p-1)$ — это один и тот же набор остатков, потому что и в том, и в другом наборе по $p-1$ элементу, при этом очевидно, что в каждом наборе все остатки различны и не равны нулю, значит, каждый набор содержит все ненулевые остатки по модулю p. Тогда для квадратов утверждение очевидно.

Сделав замену $x-1=t^2$, получим многочлен

$$\prod_{i=0}^{p-1}(t^2-i^2)=\prod_{i=0}^{p-1}(t-i)\prod_{i=0}^{p-1}(t+i)\equiv(t^p-t)(t^p-t)=t^{2p}-2t^{p+1}+t^2.$$

Теперь, сделав обратную замену, получаем для $p=4k+3$

$$\prod_{i=0}^{p-1}(x-1-i^2)\equiv(x-1)^p-2(x-1)^{\frac{p+1}{2}}+(x-1)=x^p+\ldots+(p+2\cdot\tfrac{p+1}{2}+1)x-4.$$

По теореме Виета, $\sigma_p\equiv 4 \pmod p$, $\sigma_{p-1}\equiv 2 \pmod p$, поэтому $\frac{\sigma_{p-1}}{\sigma_p}\equiv\frac{1}{2}\equiv 2k+2 \pmod p$.

Р е ш е н и е 2. Разобьем все ненулевые остатки по модулю p, кроме ±1, на пары взаимно обратных. Тогда получится $2k$ пар и в каждой паре (i,j)

$$ij\equiv 1 \quad\Leftrightarrow\quad i^2j^2\equiv 1 \quad\Leftrightarrow\quad (ij)^2+i^2+j^2+1\equiv i^2+j^2+2 \pmod p.$$

Следовательно,

$$1\equiv\frac{(ij)^2+i^2+j^2+1}{(i^2+1)(j^2+1)}\equiv\frac{i^2+j^2+2}{(i^2+1)(j^2+1)}=\frac{1}{i^2+1}+\frac{1}{j^2+1} \pmod p.$$

Таким образом, наша сумма равна $\frac{1}{0^2+1}+\frac{1}{1^2+1}+\frac{1}{(-1)^2+1}+2k\equiv 2k+2$.

Р е ш е н и е 3. Как мы знаем, благодаря малой теореме Ферма, при вычислении по модулю p операции $x\mapsto x^{-1}$ и $x\mapsto x^{p-2}$ дают одинаковый результат. Таким образом, достаточно вычислить сумму

$$\sum_{x=0}^{p-1}(x^2+1)^{p-2}=\sum_{x=0}^{p-1}\sum_{m=0}^{p-2}C_{p-2}^m x^{2m}=\sum_{m=0}^{p-2}C_{p-2}^m S_{2m}, \tag{6}$$

где $S_{2m}=\sum\limits_{x=0}^{p-1}x^{2m}$. Очевидно, $S_{2m}\equiv -1 \pmod p$ при $m=\frac{p-1}{2}$. Докажем, что $S_{2m}\equiv 0 \pmod p$ при остальных значениях m, не превосходящих $p-1$. Действительно, для каждого такого m можно подобрать ненулевой остаток a, такой что $a^{2m}\not\equiv 1 \pmod p$ и тогда можно провести рассуждение как в (5). Возвращаясь к интересующей нас сумме (6), получаем

$$\sum_{m=0}^{p-2}C_{p-2}^m S_{2m}\equiv -C_{p-2}^{\frac{p-1}{2}}=-C_{4k+1}^{2k+1}=-\frac{(4k+1)\cdot 4k\cdot\ldots\cdot(2k+1)}{1\cdot 2\cdot\ldots\cdot(2k+1)}\equiv-\frac{(-2)\cdot(-3)\ldots(2k+2)}{1\cdot 2\cdot\ldots\cdot(2k+1)}\equiv 2k+2.$$

4.3. Мы нашли оба утверждения в [16].

a) Для каждого простого делителя p числа m подберем число a_p, для которого $(a_p^k-1)\not\vdots\, p$. С помощью китайской теоремы об остатках выберем число a, такое что $a\equiv a_p \pmod p$ при всех p. Теперь результат получается аналогично рассуждениям (5).

b) Заметим, что при нечетных k по формуле бинома $i^k+(p-i^k)\equiv ki^{k-1}p \pmod{p^2}$. Тогда

$$2\sum_{i=1}^{p-1}\frac{1}{i^k}=\sum_{i=1}^{p-1}\left(\frac{1}{i^k}+\frac{1}{(p-i)^k}\right)=\sum_{i=1}^{p-1}\frac{i^k+(p-i)^k}{i^k(p-i)^k}\equiv\sum_{i=1}^{p-1}\frac{ki^{k-1}p}{i^k(-i)^k}\equiv -kp\sum_{i=1}^{p-1}\frac{1}{i^{k+1}} \pmod{p^2}.$$

Сумма в правой части сравнения делится на p в силу утверждения п. a).

4.4. Как доказывается в [24], сравнение выполнено даже по модулю p^7, но мы не будем заходить так далеко. Действуя как в статье Винберга [1], но следя за степенями до p^4, получаем

$$C_{p-1}^{2p-1}=\frac{(2p-1)(2p-2)\cdot\ldots\cdot(p+1)}{p!}=\left(\frac{2p}{1}-1\right)\left(\frac{2p}{2}-1\right)\cdot\ldots\cdot\left(\frac{2p}{p-1}-1\right)\equiv$$
$$\equiv 1-2p\sum_{i=1}^{p-1}\frac{1}{i}+4p^2\sum_{\substack{i,j=1\\ i<j}}^{p-1}\frac{1}{ij}-8p^3\sum_{\substack{i,j,k=1\\ i<j<k}}^{p-1}\frac{1}{ijk} \pmod{p^4}. \tag{7}$$

Выразим последнюю сумму через степенные суммы:

$$\sum_{\substack{i,j,k=1\\ i<j<k}}^{p-1} \frac{1}{ijk} = \frac{S_3}{3} - \frac{S_1S_2}{2} + \frac{S_1^3}{6}\,, \quad \text{где } S_k = \sum_{i=1}^{p-1} \frac{1}{i^k}.$$

Как мы знаем, S_1 и S_3 делятся на p^2 (последнее — из задачи 4.3б). Поэтому последнее слагаемое в формуле (7) можно отбросить.

4.5. Задача из [1], обсуждение вариаций на эту тему можно прочесть в [14].

Поскольку

$$2\sum_{k=1}^{p-1} \frac{1}{k^2} = \sum_{k=1}^{p-1}\Big(\frac{1}{k^2} + \frac{1}{(p-k)^2}\Big) = \sum_{k=1}^{p-1} \frac{k^2+(p-k)^2}{k^2(p-k)^2} \equiv -2\sum_{k=1}^{p-1} \frac{1}{k(p-k)} \pmod{p^2},$$

утверждение 3) эквивалентно соотношению $\displaystyle\sum_{k=1}^{p-1} \frac{1}{k(p-k)} \equiv 0 \pmod{p^2}$. Утверждение 2) тоже эквивалентно этому соотношению, так как $\displaystyle 2\sum_{k=1}^{p-1} \frac{1}{k} = 2\sum_{k=1}^{p-1}\Big(\frac{1}{k} + \frac{1}{p-k}\Big) = 2p\sum_{k=1}^{p-1} \frac{1}{k(p-k)}$. Наконец, как мы знаем из предыдущей задачи,

$$C_{2p-1}^{p-1} \equiv 1 - p^2\sum_{i=1}^{p-1} \frac{1}{i(p-i)} + 4p^2 \sum_{\substack{i,j=1\\ i<j}}^{p-1} \frac{1}{ij} \pmod{p^4}.$$

Таким образом, утверждение 1) эквивалентно сравнению

$$\sum_{i=1}^{p-1} \frac{1}{i(p-i)} \equiv 4 \sum_{\substack{i,j=1\\ i<j}}^{p-1} \frac{1}{ij} \pmod{p^2}. \tag{8}$$

Преобразуем выражение в правой части:

$$4 \sum_{\substack{i,j=1\\ i<j}}^{p-1} \frac{1}{ij} = 2\Big(\sum_{k=1}^{p-1} \frac{1}{i}\Big)^2 - 2\sum_{k=1}^{p-1} \frac{1}{k^2} \equiv 2\Big(\sum_{k=1}^{p-1} \frac{1}{i}\Big)^2 + 2\sum_{k=1}^{p-1} \frac{1}{k(p-k)}.$$

Сумма в скобке делится на p, ее квадрат делится на p^2 и это слагаемое можно отбросить. Подставляя в (8), получаем, что и первое утверждение равносильно сравнению $\displaystyle\sum_{k=1}^{p-1} \frac{1}{k(p-k)} \equiv 0 \pmod{p^2}$.

4.6. а) Р е ш е н и е 1 ([5, предложение 2.12]). Индукция по n. Раскроем скобки в равенстве

$$(a+b)^{pn} = (a+b)^{p(n-1)}(a+b)^p$$

Приравняем коэффициенты при $a^{pm}b^{p(n-m)}$:

$$C_{pn}^{pm} = C_{p(n-1)}^{pm} C_p^0 + C_{p(n-1)}^{pm-1} C_p^1 + \ldots + C_{p(n-1)}^{pm-p+1} C_p^{p-1} + C_{p(n-1)}^{pm-p} C_p^p\,.$$

В правой части все слагаемые, кроме крайних, делятся на p^2, потому что каждый биномиальный коэффициент в них делится на p по теореме Люка. Следовательно,

$$C_{pn}^{pm} \equiv C_{p(n-1)}^{pm} + C_{p(n-1)}^{p(m-1)} \pmod{p^2}.$$

По предположению индукции

$$C_{p(n-1)}^{pm} + C_{p(n-1)}^{p(m-1)} \equiv C_{n-1}^m + C_{n-1}^{m-1} \equiv C_n^m \pmod{p^2}.$$

Р е ш е н и е 2 ([Д]). Докажем, что $C_{kp}^{mp} \equiv C_k^m \pmod{p^2}$ индукцией по m.

База $m = 1$. Требуется проверить, что $C_{pk}^p - C_k^1 \equiv 0 \pmod{p^2}$. Преобразуем эту разность:

$$C_{pk}^p - C_k^1 = \frac{pk(pk-1)\dots(pk-p+1)}{p!} - k = \left(\frac{(pk-1)(pk-1)\dots(pk-p+1)}{(p-1)!} - 1\right). \tag{9}$$

В числителе большой дроби четное число сомножителей. Разобьем их на пары:

$$(pk-i)(pk-p+i) \equiv pi^2 - i^2 \pmod{p^2}.$$

Как видим, по модулю p^2 произведение чисел в парах не зависит от k. Поэтому вычисление разности (9) по модулю p^2 дает одинаковый результат при всех k. Но при $k = 1$ вычисляемое выражение равно 0.

Переход. Пусть $C_{kp}^{(m-1)p} \equiv C_k^{m-1} \pmod{p^2}$.

$$C_{kp}^{mp} = C_{kp}^{(m-1)p} \cdot \frac{(p(k-m)+1)(p(k-m)+1)\dots(p(k-m)+p)}{pm(pm-1)\dots(pm-p+1)} =$$
$$= C_{kp}^{(m-1)p} \cdot \frac{(p(k-m)+1)(p(k-m)+1)\dots(p(k-m)+p-1)}{(pm-1)\dots(pm-p+1)} \cdot \frac{k-m+1}{m} \tag{10}$$

Отметим, что обе дроби корректно определены по модулю p^2. Как и в доказательстве базы, выражение в числителе большой дроби по модулю p^2 не зависит от k. Тогда для вычисления большой дроби можно взять $k = 0$, и мы сразу получим, что по модулю p^2 дробь равна 0. Пользуясь этим соображением и предположением индукции, мы можем заменить правую часть (10) на

$$\equiv C_k^{m-1} \cdot \frac{k-m+1}{m} = C_k^m \pmod{p^2}.$$

b) Р е ш е н и е 1 (комбинаторное). Как и рекомендуется в [1], рассматриваем выборки kp предметов из общего количества pn предметов. Полагаем, что исходное множество предметов разбито на блоки по p штук. Количество блочных выборок равно C_n^k. Таким образом, остается проверить, что количество неблочных выборок делится на p^3. Как объясняется в статье, количество неблочных выборок с тремя и более блоками делится на p^3. Так как при $k > 1$ любая неблочная выборка содержит не менее трех блоков, то в этом случае все доказано. Остается разобрать случай, когда $k = 1$ и мы подсчитываем количество неблочных выборок p предметов из из общего множества в $2p$ предметов. Это количество равно $C_{2p}^p - 2$, что по теореме Волстенхолма делится на p^3.

Р е ш е н и е 2. Напишем формулу для биномиального коэффициента $C_a^b = \frac{a(a-1)\dots(a-b+1)}{b(b-1)\dots1}$, разбив числитель и знаменатель на блоки из p сомножителей, после чего сократим первые множители в каждом блоке, а частные соберем в отдельное выражение:

$$C_{mp}^{kp} = \frac{m\not{p}\cdot(mp-1)\dots\big(mp-(p-1)\big)}{k\not{p}\cdot(kp-1)\dots\big(kp-(p-1)\big)} \cdot \frac{(m-1)\not{p}\cdot\big((m-1)p-1\big)\dots\big((m-1)p-(p-1)\big)}{(k-1)\not{p}\cdot\big((k-1)p-1\big)\dots\big((k-1)p-(p-1)\big)} \cdot \dots \times$$
$$\times \frac{(m-k+1)\not{p}\cdot\big((m-k+1)p-1\big)\dots\big((m-k+1)p-(p-1)\big)}{\not{p}\cdot(p-1)\dots1} =$$
$$= C_m^k \cdot \frac{(mp-1)\dots\big(mp-(p-1)\big)}{(kp-1)\dots\big(kp-(p-1)\big)} \cdot \dots \cdot \frac{\big((m-k+1)p-1\big)\dots\big((m-k+1)p-(p-1)\big)}{(p-1)\dots1}.$$

Осталось проверить, что произведение дробей дает остаток 1 при делении на p^3. Для этого достаточно проверить сравнение

$$\frac{(np-1)\dots\big(np-(p-1)\big)}{(rp-1)\dots\big(rp-(p-1)\big)} \equiv 1 \pmod{p^3}$$

или, лучше, вот такое сравнение

$$\frac{(np-1)\dots\big(np-(p-1)\big)}{(p-1)!} \equiv \frac{(rp-1)\dots\big(rp-(p-1)\big)}{(p-1)!} \pmod{p^3}.$$

Это верно, так как обе части сравнимы с 1 по модулю p^3, что устанавливается аналогично доказательству теоремы Волстенхолма.

4.7. a) [5, теорема 2.14]. Преобразуем разность

$$C_{p^2}^p - C_p^1 = \frac{p^2(p^2-1)\dots(p^2-(p-1))}{1\cdot 2\cdot\ldots\cdot(p-1)p} - p = \frac{p}{(p-1)!}\Big((1-p^2)(2-p^2)\dots((p-1)-p^2) - 1\cdot 2\cdot\ldots\cdot(p-1)\Big).$$

Осталось проверить, что

$$(1-p^2)(2-p^2)\dots((p-1)-p^2) \equiv 1\cdot 2\cdot\ldots\cdot(p-1) \pmod{p^4}.$$

Раскроем скобки в левой части:

$$(1-p^2)(2-p^2)\dots((p-1)-p^2) = 1\cdot 2\cdot\ldots\cdot(p-1) + p^2\Big(1+\frac{1}{2}+\ldots+\frac{1}{p-1}\Big)(p-1)! + \text{члены делящиеся на } p^4.$$

По утверждению задачи 4.1 второе слагаемое делится на p^4.

b) Как нетрудно видеть, $C_{p^{s+1}}^p = p^s \cdot C_{p^{s+1}-1}^{p-1}$, поэтому достаточно проверить, что $C_{p^{s+1}-1}^{p-1} \equiv 1 \pmod{p^{s+3}}$.

$$C_{p^{s+1}-1}^{p-1} = \frac{(p^{s+1}-1)(p^{s+1}-2)\dots(p^{s+1}-(p-1))}{1\cdot 2\cdots(p-1)} = \left(\frac{p^{s+1}}{1}-1\right)\left(\frac{p^{s+1}}{2}-1\right)\dots\left(\frac{p^{s+1}}{p-1}-1\right) \equiv$$
$$\equiv (-1)^{p-1} + p^{s+1}\Big(1+\frac{1}{2}+\ldots+\frac{1}{p-1}\Big) \pmod{p^{s+3}}.$$

Это и есть то, что требуется, поскольку $(-1)^{p-1} = 1$ и $1+\frac{1}{2}+\ldots+\frac{1}{p-1} \equiv 0 \mod p^2$.

В статье [14] доказывается чуть более общий факт.

4.8. Задача из статьи Винберга [1], решение [T].

$$C_{p^3}^{p^2} - C_{p^2}^p = p\left(C_{p^3-1}^{p^2-1} - C_{p^2-1}^{p-1}\right) =$$
$$= p\left(\left(\frac{p^3}{1}-1\right)\left(\frac{p^3}{2}-1\right)\dots\left(\frac{p^3}{p^2-1}-1\right) - \left(\frac{p^2}{1}-1\right)\left(\frac{p^2}{2}-1\right)\dots\left(\frac{p^2}{p-1}-1\right)\right) =$$
$$= p\Big(\frac{p^2}{1}-1\Big)\Big(\frac{p^2}{2}-1\Big)\dots\Big(\frac{p^2}{p-1}-1\Big)\left(\prod_{\substack{k=1\\ p\nmid k}}^{p^2-1}\left(\frac{p^3}{k}-1\right)-1\right).$$

Достаточно проверить, что выражение в последней скобке делится на p^7. Преобразуем произведение

$$\prod_{\substack{k=1\\ p\nmid k}}^{p^2-1}\left(\frac{p^3}{k}-1\right) = \prod_{\substack{k=1\\ p\nmid k}}^{\frac{p^2-1}{2}}\left(\frac{p^3}{k}-1\right)\left(\frac{p^3}{p^2-k}-1\right) = \prod_{\substack{k=1\\ p\nmid k}}^{\frac{p^2-1}{2}}\left(\frac{p^6-p^5}{k(p^2-k)}+1\right) \equiv 1+p^5(p-1)\sum_{\substack{k=1\\ p\nmid k}}^{\frac{p^2-1}{2}}\frac{1}{k(p^2-k)} \pmod{p^7}.$$

Осталось проверить, что последняя сумма делится на p^2. Это так, поскольку по задаче 4.3a)

$$\sum_{\substack{k=1\\ p\nmid k}}^{\frac{p^2-1}{2}}\frac{1}{k(p^2-k)} \equiv -\sum_{\substack{k=1\\ p\nmid k}}^{\frac{p^2-1}{2}}\frac{1}{k^2} \equiv 0 \pmod{p^2}.$$

4.9. Это [6, теорема 5]. Более общий факт доказан в [7].

Р е ш е н и е 1 ([5, предложение 2.19]). Воспользуемся тем, что разность $C_{2^{k+1}}^{2^k} - C_{2^k}^{2^{k-1}}$ равна коэффициенту при x^{2^k} в многочлене

$$(1+x)^{2^{k+1}} - (1-x^2)^{2^k} = (1+x)^{2^k}\Big((1+x)^{2^k} - (1-x)^{2^k}\Big) =$$
$$= \Big(1 + C_{2^k}^1 x + C_{2^k}^2 x^2 + \ldots + x^{2^k}\Big)\cdot 2\Big(C_{2^k}^1 x + C_{2^k}^3 x^3 + \ldots + C_{2^k}^{2^k-1} x^{2^k-1}\Big).$$

Поскольку второй многочлен содержит только множители нечетной степени, коэффициент при x^{2^k} в произведении равен

$$2\Big(C_{2^k}^1 C_{2^k}^{2^k-1} + C_{2^k}^3 C_{2^k}^{2^k-3} + \ldots + C_{2^k}^{2^k-1} C_{2^k}^1\Big).$$

По утверждению задачи 3.5 б) каждый биномиальный коэффициент в этом выражении делится на 2^k, кроме того, каждое слагаемое в сумме встречается 2 раза, а перед суммой стоит коэффициент 2. В итоге все выражение делится на 2^{2k+2}.

Решение 2 ([CSTTVZ]). Так как $C_{2^{n+1}}^{2^n} = 2C_{2^{n+1}-1}^{2^n-1}$, достаточно доказать соотношение

$$C_{2^{n+1}-1}^{2^n-1} \equiv C_{2^n-1}^{2^{n-1}-1} \pmod{2^{2n+1}}.$$

Аналогично (3) получаем

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

Достаточно проверить, что

$$L = \left(\frac{2^{n+1}}{1} - 1\right)\left(\frac{2^{n+1}}{3} - 1\right)\ldots\left(\frac{2^{n+1}}{2^n-1} - 1\right) \equiv 1 \pmod{2^{2n+1}}.$$

Это так, поскольку

$$L \equiv (-1)^{2^{n-1}} - 2^{n+1}\left(\frac{1}{1} + \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2^n-1}\right) \equiv$$
$$\equiv 1 - 2^{n+1}\left(\frac{2^n}{1\cdot(2^n-1)} + \frac{2^n}{3\cdot(2^n-3)} + \ldots + \frac{2^n}{(2^{n-1}-1)(2^{n-1}+1)}\right) \equiv 1 \pmod{2^{2n+1}}.$$

4.10. Это теорема Морли [26].

Решение 1 (авторское решение из статьи 1895 года). Оно лишь чуть-чуть выходит за рамки школьной программы.

Возьмем формулу, с помощью которой $\cos^{2n+1} x$ выражается через косинусы кратных углов,[1] или, как говорили в те времена, запишем $\cos^{2n+1} x$ в виде, удобном для интегрирования:

$$2^{2n}\cos^{2n+1}x = \cos(2n{+}1)x + (2n{+}1)\cos(2n{-}1)x + \frac{(2n{+}1)\cdot 2n}{1\cdot 2}\cos(2n{-}3)x + \ldots + \frac{(2n{+}1)\cdot 2n\ldots(n{+}2)}{n!}\cos x.$$

Ну, а раз этот вид удобен для интегрирования, то и проинтегрируем обе части[2] по промежутку $[0, \frac{\pi}{2}]$:

$$2^{2n}\int \cos^{2n+1} x\,dx = \frac{\sin(2n+1)x}{2n+1} + \frac{2n+1}{2n-1}\sin(2n-1)x + \ldots,$$
$$2^{2n}\int_0^{\pi/2} \cos^{2n+1} x\,dx = (-)^n\left(\frac{1}{2n+1} - \frac{2n+1}{2n-1} + \ldots\right).$$

Но любой первокурсник знает, что куда проще этот интеграл вычисляется с помощью формулы понижения, для получения которой нужно всего лишь проинтегрировать по частям:

$$I_{2n+1} = \int_0^{\pi/2} \cos^{2n+1} x\,dx = \int_0^{\pi/2} \cos^{2n} x\cos x\,dx = \cos^{2n} x\sin x\,\Big|_0^{\pi/2} + 2n\int_0^{\pi/2} \cos^{2n-1} x\sin^2 x\,dx =$$
$$= 0 + 2n\int_0^{\pi/2} \cos^{2n-1} x(1-\cos^2 x)\,dx = 2n\cdot I_{2n-1} - 2n\cdot I_{2n+1},$$

[1] Читатель, интересующийся вопросом "где мы ее возьмем" и не удовлетворенный ответом "в справочнике", может просто воспользоваться формулой Эйлера $\cos\varphi = \frac{1}{2}(e^{i\varphi} + e^{-i\varphi})$ и возвести правую часть в степень $2n+1$ по формуле бинома.

[2] Когда мы учим правила умножения, мы запоминаем формулу "минус на минус будет плюс". В этой формуле мы перемножаем знаки. Значит, если нам нужно перемножить n минусов, кажется вполне уместной запись $(-)^n$. Поэтому мы оставляем старомодное обозначение $(-)^n$, как у автора, вместо современного $(-1)^n$.

откуда находим, что $I_{2n+1} = \dfrac{2n}{2n+1}\cdot I_{2n-1}$. Учитывая что $I_1 = 1$, применяя эту формулу n раз подряд, находим, что

$$\int\limits_0^{\pi/2} \cos^{2n+1} x\,dx = \frac{2n\cdot(2n-2)\dots 2}{(2n+1)(2n-1)\dots 3}\,.$$

Приравнивая эти два способа подсчета интеграла, мы получаем тождество

$$2^{2n}\frac{2n\cdot(2n-2)\dots 2}{(2n+1)(2n-1)\dots 3} = (-)^n\left(\frac{1}{2n+1} - \frac{2n+1}{2n-1} + \dots + \frac{(2n+1)\cdot 2n\dots(n+2)}{n!}\right).$$

Если взять $p = 2n+1$ — простое число, то домножая на p, мы сразу получаем требуемое сравнение

$$2^{2n}\frac{2n\cdot(2n-2)\dots 2}{(2n-1)(2n-3)\dots 3} \equiv (-)^n \pmod{p^2}\,.$$

Р е ш е н и е 2 ([CSTTVZ]). Введем несколько обозначений. Пусть

$$A = \sum_{i=1}^{\frac{p-1}{2}}\frac{1}{i}, \qquad B = \sum_{1\leqslant i<j\leqslant\frac{p-1}{2}}\frac{1}{ij}, \qquad C = \sum_{\substack{1\leqslant i\leqslant p-1\\ i \text{ нечетно}}}\frac{1}{i}.$$

Очевидно, $A^2 = \sum\limits_{i=1}^{\frac{p-1}{2}}\frac{1}{i^2} + 2B \equiv 2B \pmod p$ по задаче 4.3b). Итак, $A^2 \equiv 2B \pmod p$. Далее,

$$2C + A = \sum_{\substack{1\leqslant i\leqslant p-1\\ i \text{ нечетно}}}\frac{2}{i} + \sum_{i=1}^{\frac{p-1}{2}}\frac{2}{2i} = \sum_{i=1}^{p-1}\frac{2}{i} \equiv 0 \pmod{p^2}.$$

Таким образом, $C \equiv -\frac{1}{2}A \pmod{p^2}$.

Теперь преобразуем по модулю p^3 правую и левую части доказываемого сравнения. Левая часть:

$$(-1)^{\frac{p-1}{2}}C_{p-1}^{\frac{p-1}{2}} \equiv \left(1-\frac{p}{1}\right)\left(1-\frac{p}{2}\right)\dots\left(1-\frac{p}{\frac{p-1}{2}}\right) \equiv 1 - pA + p^2B \equiv 1 - pA + \frac{1}{2}p^2A^2 \pmod{p^3}.$$

Для преобразования правой части заметим, что

$$2^{p-1} = \frac{2\cdot 4\cdots(p-1)}{1\cdot 2\cdots\frac{p-1}{2}}\cdot\frac{(p+1)\cdots(2p-2)}{\frac{p+1}{2}\cdots(p-1)} = \frac{(p+1)\cdots(2p-2)}{1\cdot 3\cdot 5\cdots(p-2)} =$$
$$= \left(\frac{p}{1}+1\right)\left(\frac{p}{3}+1\right)\dots\left(\frac{p}{p-1}+1\right) \equiv 1 + pC + \frac{1}{2}p^2C^2 \equiv 1 - \frac{1}{2}pA + \frac{1}{8}p^2A^2 \pmod{p^3}\,.$$

Отсюда получаем

$$4^{p-1} \equiv \left(1 - \frac{1}{2}pA + \frac{1}{8}p^2A^2\right)^2 \equiv 1 - pA + \frac{1}{4}p^2A^2 + 2\cdot\frac{1}{8}P^2A^2 = 1 - pA + \frac{1}{2}p^2A^2 \pmod{p^3}.$$

Таким образом, левая часть эквивалентна правой.

4.11. Мы взяли утверждение в [10].

$$\sum_{k=1}^{p-1}\frac{1}{mp+k} = \frac{1}{2}\sum_{k=1}^{p-1}\left(\frac{1}{mp+k} + \frac{1}{mp+p-k}\right) =$$
$$= p\cdot\frac{2m+1}{2}\cdot\sum_{k=1}^{p-1}\frac{1}{(mp+k)(mp+p-k)} \equiv -p\cdot\frac{2m+1}{2}\cdot\sum_{k=1}^{p-1}\frac{1}{k^2} \equiv 0 \pmod{p^2}.$$

4.12. Мы взяли утверждение в [8]. Так как $2pq-1 = (2q-1)p+p-1$, у числа $2pq-1$ последняя цифра p-ичной записи — это $p-1$, а остальные цифры образуют запись числа $2q-1$. Аналогично в записи числа $pq-1$ последняя цифра — $p-1$, а остальные цифры образуют запись числа $q-1$. По теореме Люка $C_{2pq-1}^{pq-1} \equiv C_{2q-1}^{q-1}C_{p-1}^{p-1} \equiv C_{2q-1}^{q-1} \pmod p$. С другой стороны, очевидно, что так как $C_{2pq-1}^{pq-1} \equiv 1 \pmod{pq}$, то $C_{2pq-1}^{pq-1} \equiv 1 \pmod p$. Таким образом, $C_{2q-1}^{q-1} \equiv 1 \pmod p$. Аналогично $C_{2p-1}^{p-1} \equiv 1 \pmod q$.

В обратную сторону утверждение очевидно.

5 Суммы биномиальных коэффициентов

5.1. a) Это сразу следует из результата задачи 1.3. Если Δ_0^0 — это треугольник из трех первых строк 3-арифметического треугольника Паскаля, то, как нетрудно видеть сумма центральных коэффициентов в нем делится на 3. При произвольном a изучаемая сумма содержит элементы нескольких центральных треугольников, кратных Δ_0^0. Поэтому сумма тоже делится на 3.

Другое решение ([CSTTVZ]) получится, если мы воспользуемся тождеством $C_{2k}^k = \sum\limits_{i=0}^{k} {C_k^i}^2$. Тогда $\sum\limits_{k=0}^{3^a-1} C_{2k}^k = \sum\limits_{k=0}^{3^a-1}\sum\limits_{i=0}^{k} {C_k^i}^2$. Поскольку $1^2 = 2^2 = 1$, $0^2 = 0$ по модулю 3, последняя сумма равна по модулю 3 количеству ненулевых элементов в первых 3^a строках треугольника Паскаля. Это количество подсчитано в задаче 2.1a), оно делится на 3.

b) Приводим решение [Д]. Нужная нам сумма является коэффициентом при x^{3^a-1} многочлена

$$x^{3^a-1}\left(1+\frac{(x+1)^2}{x}+\frac{(x+1)^4}{x^2}+\ldots+\frac{(x+1)^{2(3^a-1)}}{x^{3^a-1}}\right)=\frac{\frac{(x+1)^{2\cdot 3^a}}{x^{3^a}}-1}{\frac{(x+1)^2}{x}-1}\cdot x^{3^a-1}=\frac{(x+1)^{2\cdot 3^a}-x^{3^a}}{x^2+x+1}=$$
$$=\frac{x^{2\cdot 3^a}+C_{2\cdot 3^a}^1\cdot x^{2\cdot 3^a-1}+C_{2\cdot 3^a}^2\cdot x^{2\cdot 3^a-2}+\ldots+1-x^{3^a}}{x^3-1}\cdot(x-1)\,.$$

Чтобы найти нужный коэффициент, достаточно поделить числитель на знаменатель “в столбик”, и потом домножить результат на $(x-1)$. Таким образом, не нужно даже доводить деление до конца, достаточно довести его до нахождения коэффициента при x^{3^a-2}, кроме того, напомним, результат нас интересует лишь по модулю 3^a. Отметим, что при $b \not\vdots 3$ все биномиальные коэффициенты $C_{2\cdot 3^a}^b$ делятся на 3^a по теореме Куммера. Сгруппируем слагаемые с этими коэффициентами и будем делить их сумму на x^3-1 отдельно. Очевидно, все коэффициенты частного будут тоже делиться на 3^a, поэтому все эти слагаемые можно отбросить. Остается выражение

$$\frac{x^{2\cdot 3^a}+C_{2\cdot 3^a}^3\cdot x^{2\cdot 3^a-3}+C_{2\cdot 3^a}^6\cdot x^{2\cdot 3^a-6}+\ldots+1-x^{3^a}}{x^3-1}\cdot(x-1).$$

Здесь все показатели в числителе делятся на 3, после деления на x^3-1 все показатели частного тоже будут делиться на 3, а когда мы домножим частное на $x-1$, у нас не появится ни одного показателя вида $3k+2$. Таким образом, искомый коэффициент по модулю 3^a равен 0.

5.2. Задача была опубликована в Monthly [25]. Так как

$$C_{2n+2}^{n+1}-4C_{2n}^n=2\cdot\frac{2n+1}{n+1}C_{2n}^n-4C_{2n}^n=-2C_n\,,$$

то $C_n \equiv C_{2n+2}^{n+1}-C_{2n}^n \pmod 3$. Поэтому сумма по модулю 3 является телескопической,

$$\sum_{k=1}^{n} C_k \equiv \left(C_{2n+2}^{n+1}-C_{2n}^n\right)+\left(C_{2n}^n-C_{2n-2}^{n-1}+\ldots\right)=C_{2n+2}^{n+1}+1 \pmod 3.$$

Таким образом, по теореме Куммера нам остается выяснить, в каком случае сложение числа $(n+1)$ с самим собой в троичной системе счисления приводит к появлению хотя бы одного переноса. Очевидно, это может быть в том и только том случае, когда в записи $n+1$ есть хотя бы одна двойка.

5.3. Это задача A5 Putnam Mathematical Competition, 1998. Поскольку $\frac{1}{p}C_p^n \equiv \frac{(-1)^{n-1}}{n} \pmod p$, получаем, что

$$\sum_{n=1}^{k}\frac{1}{p}C_p^n \equiv \sum_{n=1}^{k}\frac{(-1)^{n-1}}{n}=\sum_{n=1}^{k}\frac{1}{n}-2\sum_{n=1}^{[k/2]}\frac{1}{2n}\equiv\sum_{n=1}^{k}\frac{1}{n}+\sum_{n=p-[\frac{k}{2}]}^{p-1}\frac{1}{n}\overset{*}{=}\sum_{n=1}^{p-1}\frac{1}{n}\equiv 0 \pmod p.$$

В сумме, расположенной непосредственно слева от равенства, помеченного звездочкой, на самом деле суммирование ведется от $n = k + 1$ (в этом нетрудно убедиться: при $p = 6r + 1$ имеем $k = 4r$ и $p - [\frac{k}{2}] = 4r + 1 = k + 1$, аналогично при $p = 6r + 5$).

5.4. Это утверждение из [11]. Решение [CSTTVZ]. Индукция по n. База тривиальна. Докажем переход от $n' = n - (p - 1)$ к n. Пусть $q = \frac{n}{p-1}$. Так как

$$C_{n'+p-1}^{x(p-1)} = \sum_{i=0}^{p-1} C_{p-1}^{i} C_{n'}^{x(p-1)-i},$$

мы можем записать изучаемую сумму в виде

$$C_n^{p-1} + C_n^{2(p-1)} + C_n^{3(p-1)} + \ldots = \sum_{x=1}^{q} \sum_{i=0}^{p-1} C_{p-1}^{i} C_{n'}^{x(p-1)-i} = \sum_{i=0}^{p-1} \left(C_{p-1}^{i} \sum_{x=1}^{q} C_{n'}^{x(p-1)-i} \right) \tag{11}$$

По утверждению задачи 1.1 а) $C_{p-1}^{i} \equiv (-1)^i \pmod p$, пусть $C_{p-1}^{i} = ap + (-1)^i$. По утверждению задачи 1.6 при $i = 0, 1, \ldots, p-2$ выполнено сравнение $\sum\limits_{x=1}^{q} C_{n'}^{x(p-1)-i} \equiv C_{p-1}^{i} \equiv (-1)^i \pmod p$; пусть $\sum\limits_{x=1}^{q} C_{n'}^{x(p-1)-i} = bp + (-1)^i$. Тогда

$$C_{p-1}^{i} \sum_{x=1}^{q} C_{n'}^{x(p-1)-i} = \big(ap + (-1)^i\big)\big(bp + (-1)^i\big) \equiv 1 + (-1)^i(ap + bp) =$$
$$= 1 + (-1)^i \left(C_{p-1}^{i} + \sum_{x=1}^{q} C_{n'}^{x(p-1)-i} - 2 \cdot (-1)^i \right) = (-1)^i \left(C_{p-1}^{i} + \sum_{x=1}^{q} C_{n'}^{x(p-1)-i} \right) - 1 \pmod{p^2}.$$

Напомним, что это преобразование верно при $0 \leqslant i \leqslant p - 2$. Мы можем продолжить равенство (11), выделив отдельное слагаемое для $i = p - 1$:

$$\sum_{i=0}^{p-1} \left(C_{p-1}^{i} \sum_{x=1}^{q} C_{n'}^{x(p-1)-i} \right) \equiv \sum_{i=0}^{p-2} \left((-1)^i \left(C_{p-1}^{i} + \sum_{x=1}^{q} C_{n'}^{x(p-1)-i} \right) - 1 \right) + \sum_{x=0}^{q-1} C_{n'}^{x(p-1)} =$$
$$= \sum_{i=0}^{p-2} (-1)^i C_{p-1}^{i} + \sum_{i=0}^{p-2} \left((-1)^i \sum_{x=1}^{q} C_{n'}^{x(p-1)-i} \right) - (p-1) + C_{n'}^{0} + \sum_{x=1}^{q-1} C_{n'}^{x(p-1)}.$$

Здесь первая сумма равна -1, так как знакопеременная сумма $C_{p-1}^{0} - C_{p-1}^{1} + C_{p-1}^{2} + \ldots$ равна 0. По той же причине вторая (двойная) сумма вместе со слагаемым $C_{n'}^{0}$ равна 0. Последняя же сумма по предположению индукции равна $1 + p(n' + 1)$. Итого все выражение равно $-1 + 0 - p + 1 + 1 + p(n' + 1) = 1 + pn'$. Это как раз то, что требуется, поскольку $1 + p(n + 1) = 1 + p(n' + p - 1 + 1) \equiv 1 + pn' \pmod{p^2}$.

5.5. Это результат Флека, 1913 г., мы узнали о нем из [18]. Решение [CSTTVZ].

При $p = 2$ сумма не знакопеременная и результат очевиден. Далее считаем, что p нечетно. Индукция по q. База следует из утверждения задачи 2.5 а). Докажем переход от $n' = n - (p-1)$ к n. Ниже выражение $\sum_x$ обозначает суммирование по x в естественных границах (т. е. в границах для которых определены биномиальные коэффициенты под знаком суммирования).

$$\pm \sum_{m:m \equiv j \pmod p} (-1)^m C_n^m = \sum_x (-1)^x C_{n'+p-1}^{xp+j} = \sum_x (-1)^x \sum_{i=0}^{p-1} C_{p-1}^{i} C_{n'}^{xp+j-i} = \sum_{i=0}^{p-1} C_{p-1}^{i} \sum_x (-1)^x C_{n'}^{xp+j-i}$$

По предположению индукции $\sum\limits_x (-1)^x C_{n'}^{xp+j-i}$ делится на p^{q-1}, по утверждению задачи 1.1 а) $C_{p-1}^{i} \equiv (-1)^i \pmod p$, следовательно,

$$\sum_{i=0}^{p-1} C_{p-1}^{i} \sum_x (-1)^x C_{n'}^{xp+j-i} \equiv \sum_{i=0}^{p-1} (-1)^i \sum_x (-1)^x C_{n'}^{xp+j-i} \pmod{p^q}.$$

Внимательно посмотрев на последнюю двойную сумму, можно заметить, что это она равна $C_{n'}^{0} - C_{n'}^{1} + C_{n'}^{2} - C_{n'}^{3} + \ldots = 0$.

5.6. Это результат Баскарана (1965 г.), мы взяли его в [18], решение [CSTTVZ].

Обозначим

$$f(n,j) = C_n^j - C_n^{j+(p-1)} + C_n^{j+2(p-1)} - C_n^{j+3(p-1)} + \dots$$

Индукция по n. База $n = p+1$ тривиальна, отметим лишь, что $C_{p+1}^i \equiv 1 \pmod p$ при $i = 0, 1, p, p+1$, а в остальных случаях этот биномиальный коэффициент делится на p. Докажем индукционный переход от $n' = n - (p+1)$ к n. Благодаря сделанному замечанию,

$$C_{n'+(p+1)}^{j+(p-1)k} = \sum_{i=0}^{p+1} C_{n'}^{j+(p-1)k-i} C_{p+1}^i \equiv \sum_{i\in\{0,1,p,p+1\}} C_{n'}^{j+(p-1)k-i} =$$

$$= C_{n'}^{j+(p-1)k} + \underline{C_{n'}^{j-1+(p-1)k} + C_{n'}^{j-1+(p-1)(k-1)}} + C_{n'}^{j-2+(p-1)(k-1)} \pmod p .$$

Поскольку $f(n,j) = \sum_k (-1)^k C_n^{j+k(p-1)}$ — знакочередующаяся сумма, при суммировании по k подчеркнутые выражения сократятся в типовом слагаемом (а несократившиеся выражения в крайних слагаемых равны 0 по причине некорректности биномиального коэффициента). Таким образом, мы получаем соотношения

$$f(n,j) \equiv f(n',j) - f(n',j-2) \quad \text{при } j > 1 , \qquad f(n,1) \equiv f(n',1) + f(n',p-2) .$$

Теперь часть "только тогда" доказываемого утверждения сразу следует из индукционного предположения, а часть "тогда" в общем-то тоже: если $f(n,j) \equiv 0 \pmod p$ при $j = 1, 3, \dots, p-2$, то

$$f(n',p-2) \equiv f(n',p-4) \equiv \dots \equiv f(n',1) \equiv -f(n',p-2) ,$$

откуда $f(n',j) \equiv 0 \pmod p$ при всех нужных j и тогда $n' \vdots (p+1)$, а тогда и $n \vdots (p+1)$.

Ссылки

Авторы многих приведенных решений — участники конференции, в таких решениях мы ставили ссылки:

[Д] Максим Дидин;
[K] Дмитрий Креков;
[J] Jastin Lim Kai Ze;
[T] Teh Zhao Yang Anzo;
[CSTTVZ] Ćevid Domagoj, Stokić Maksim, Tanasijeviić Ivan, Trifunović Petar, Vukorepa Borna, Žikelić Đorđe

Литература

[1] *Винберг Э. Б.* Удивительные свойства биномиальных коэффициентов. // Мат. просвещение. Третья серия. Вып. 12. 2008

[2] *Гашков С.Б., Чубариков В.Н.* Арифметика. Алгоритмы. Сложность вычислений. М.: Высш. шк., 2000.

[3] *Дынкин Е.Б., Успенский В.А.* Математические беседы. 2-е изд. М.: ФИЗМАТЛИТ, 2004.

[4] Петербургские математические олимпиады, 1961–1993. СПб: Лань, 2007.

[5] *Табачников С.Л., Фукс Д.Б.* Математический дивертисмент. 30 лекций по классической математике. М.: МЦНМО, 2011.

[6] *Фукс Д.Б., Фукс М.Б.* Арифметика биномиальных коэффициентов // Квант. 1970. №6. С. 17–25.

[7] *Ширшов А.И.* Об одном свойстве биномиальных коэффициентов // Квант. 1971. №10. С. 16–20.

[8] *Cai T.X., Granville A.* On the residues of binomial coefficients and their products modulo prime powers /!/ Acta

[9] *Calkin N. J.* Factors of sums of powers of binomial coefficients // Acta Arith. 1998. Vol. 86. P. 17–26.

[10] *Carlitz L.* A note of Wolstenholme's theorem // Amer. Math. Monthly. 1954. Vol. 61. № 3. P. 174–176.

[11] *Dimitrov V., Chapman R.* Binomial coefficient identity: 11118 // Amer. Math. Monthly. 2006. Vol. 113. № 7. P. 657–658.

[12] *Everett W.* Subprime factorization and the numbers of binomial coefficients exactly divided by powers of a prime // Integers. 2011. Vol. 11. # A63. `http://www.integers-ejcnt.org/vol11.html`

[13] *Fine N.* Binomial coefficient modulo a prime // Amer. Math. Monthly. 1947. Vol. 54. № 10. Part 1. P. 589–592.

[14] *Gardiner A.* Four problems on prime power divisibility // Amer. Math. Monthly. 1988. Vol. 95. № 10. P. 926–931.

[15] *Gauss K.* Disquisitiones arithmeticae. 1801. Art. 78.

[16] *Gessel I.* Wolstenholme revisited // Amer. Math. Monthly. 1998. Vol. 105. № 7. P. 657–658.

[17] *Granville A.* Arithmetic properties of binomial coefficients. Доступно по адресу `http://www.dms.umontreal.ca/~andrew/Binomial/`

[18] *Granville A.* Binomial coefficients modulo prime powers.

[19] *Granville A.* Zaphod Beeblebrox's Brian and the Fifty-ninth Row of Pascal's Triangle // Amer. Math. Monthly. 1992. Vol. 99. № 4. P. 318–331.

[20] *Granville A.* Correction to: Zaphod Beeblebrox's Brian and the Fifty-ninth Row of Pascal's Triangle // Amer. Math. Monthly. 1997. Vol. 104. № 9. P. 848–851.

[21] *Hinz A.* Pascal's triangle and tower of Hanoi // Amer. Math. Monthly. 1992. Vol. 99. № 6. P. 538–544.

[22] *Loveless A.* A congruence for products of binomial coefficients modulo a composite // Integers: electronic journal of comb. number theory 7 (2007) # A44

[23] *McIntosh R.* On the converse of Wolstenhome's theorem // Acta Arithmetica. 1995. Vol. 61. №4. P. 381–388.

[24] *Meštrović R.* On the mod p^7 determination of $\binom{2p-1}{p-1}$ // `http://arxiv.org/pdf/1108.1174v1.pdf`

[25] *More Y., Chapman R.* The sum of Catalan numbers, modulo 3: 11165 // Amer. Math. Monthly. 2007. Vol. 114. № 5. P. 454–455.

[26] *Morley F.* Note on the congruences $2^{4n} \equiv (-)^n(2n)!/(n!^2)$, where $2n+1$ is a prime // Annals of Math. 1894-1895. Vol. 9. №1. P. 168–170.

[27] *Roberts J.* On binomial coefficient residues // Canad J. Math. 1957. Vol. 9. P. 363–370.

[28] Sun Z.-W., Wan D. On Fleck quotients // `arXxiv:math.0603462v3`