«Суммы степеней и числа Бернулли»: решения

Большинство из приведённых решений не являются новыми (однако не все!) Подлинным результатом конференции будет такая версия этого текста, где для каждой задачи будет выбрано наиболее удачное из решений, предложенных на конференции. Вопросы по этому тексту (и не только) приветствуются (по email'у: `dotsenko@mccme.ru`).

1. (**a**) (**b**) Доказательство вполне стандартно. Давайте переформулируем задачу: сколько раз встретится слагаемое $x_1^{a_1}\cdots x_k^{a_k}$ после раскрытия скобок в $(x_1+\cdots+x_k)^n$? Это число совпадает с числом способов разбить n скобок на k групп, чтобы в первой было a_1 скобок, во второй — a_2 скобок, …, в k-ой — a_k скобок. Восстановить детали предлагается читателю.

2. (**a**) (**b**) В случае, когда a — целое число, легко придумать комбинаторную интерпретацию для $[a]^n$ и $[a]_n$: например, $[a]_n$ совпадает с числом способов выбрать председателя, заместителя председателя, …, «заместителя$^{n-1}$ председателя» на собрании, где присутствуют a человек.

Упражнение. Завершите доказательство для целых a, b.

Для общих a, b используйте такой факт: многочлен от a, b обращается в нуль во всех целых точках тогда и только тогда, когда все его коэффициенты обращаются в нуль.

3. Указание: покажите, что и $\binom{n}{k}_q$, и соответствующие коэффициенты в левой части удовлетворяют одному и тому же рекуррентному соотношению.

4. (**a**) Доказательство использует очень важный метод: исчисление конечных разностей (см. [Ге]). Основная идея очень проста: допустим, мы уже знаем многочлен $Q(x)$, такой что $Q(1)=0$ («начальное условие») и $Q(x+1)-Q(x)=x^k$. Тогда $Q(x)=P_k(x)$: $1^k+2^k+\cdots+(n-1)^k=Q(2)-Q(1)+Q(3)-Q(2)+\cdots+Q(n)-Q(n-1)=Q(n)$. Давайте проверим, что такой многочлен степени $k+1$ существует (и единственен). Пусть $Q(x)=q_0+q_1x+\cdots+q_kx^k+q_{k+1}x^{k+1}$. Тогда $Q(x+1)-Q(x)=(k+1)q_{k+1}x^k+(\binom{k+1}{2}q_{k+1}+kq_k)x^{k-1}+\ldots$, поэтому ясно, что коэффициенты q_i можно вычислить один за другим с помощью этих уравнений (такую ситуацию называют «система линейных уравнений с верхнетреугольной матрицей») и набор из $k+2$ чисел $(q_0,\ldots,q_{k+1})$ определяется однозначно (с точностью до свободного члена q_0, определяемого из начального условия).

(**b**)

$$P_1(x)=x(x-1)/2, P_2(x)=x(x-1)(2x-1)/6, P_3(x)=x^2(x-1)^2/4,$$
$$P_4(x)=x(x-1)(2x-1)(3x^2-3x-1)/30, P_5(x)=x^2(x-1)^2(2x^2-2x-1)/12$$

5. Это немедленное следует из определения чисел Бернулли. Приведённое решение демонстрирует возможности метода производящих функций. Пусть

$$\frac{t}{e^t-1}=\sum_{k\geqslant 0}\frac{\widehat{B}_kt^k}{k!}.$$

Тогда ясно, что

$$t=\sum_{k\geqslant 0}\frac{t^{k+1}}{(k+1)!}\sum_{l\geqslant 0}\frac{\widehat{B}_lt^l}{l!}=\sum_{k\geqslant 0}\left(\sum_{i=0}^k\binom{k+1}{i}\widehat{B}_i\right)\frac{t^{k+1}}{(k+1)!},$$

поэтому на $\widehat{B}_k$ и B_k есть одинаковые рекуррентное сотношение и начальное условие, а поэтому эти последовательности совпадают. Дальше доказательство совсем простое: экспоненциальная производящая функция для степенных сумм $S_k(n)$ с фиксированным n — это

$$\sum_{k=0}^{n-1}e^{kt}=\frac{e^{nt}-1}{e^t-1}=\frac{e^{nt}-1}{t}\cdot\frac{t}{e^t-1}=\sum_{k\geqslant 0}\frac{n^{k+1}t^k}{k!}\sum_{l\geqslant 0}\frac{B_lt^l}{l!}=\sum_{k\geqslant 0}\left(\frac{1}{k+1}\sum_{i=0}^k\binom{k+1}{i}B_in^{k+1-i}\right)\frac{t^k}{k!}.$$

6.

n	0	1	2	3	4	5	6	7	8	9
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$\frac{-1}{30}$	0	$\frac{1}{42}$	0	$\frac{-1}{30}$	0

n	10	11	12	13	14	15	16	17	18	19	20
B_n	$\frac{5}{66}$	0	$\frac{-691}{2730}$	0	$\frac{7}{6}$	0	$-\frac{3617}{510}$	0	$\frac{43867}{798}$	0	$-\frac{174611}{330}$

$$5,7,691,3617,43867 \quad \text{– простые числа},\ 6=2\cdot 3,\ 30=2\cdot 3\cdot 5,\ 42=2\cdot 3\cdot 7,\ 66=2\cdot 3\cdot 11,$$
$$2730=2\cdot 3\cdot 5\cdot 7\cdot 13,\ 510=2\cdot 3\cdot 5\cdot 17,\ 798=2\cdot 3\cdot 7\cdot 19,\ 174611=283\cdot 617,\ 330=2\cdot 3\cdot 5\cdot 11.$$

7. (Это решение было предложено Е. Ференс–Сороцким, О. Стыртом и О. Евтифеевой во время конференции; мне оно не было известно до этого. Другие участники проверяли, что функция $f(t)=\dfrac{t}{e^t-1}+\dfrac{t}{2}$

чётна, но на этом пути встречаются проблемы формального обоснования (которые, впрочем, не очень сложно преодолеть).)

Пусть k — наименьшее нечетное число, большее 1, для которого $B_k \neq 0$. $P_k(n) + n^k = P_k(n+1) = P_k(-n)$ — см. решение **9(e)**. Поэтому

$$\frac{1}{k+1}\sum_{i=0}^{k}\binom{k+1}{i}B_i(-n)^{k+1-i} = \frac{1}{k+1}\sum_{i=0}^{k}\binom{k+1}{i}B_i n^{k+1-i} + n^k.$$

Мы предположили, что $B_3 = B_5 = \dots = B_{k-2} = 0$, поэтому большинство слагаемых сокращаются (часть из них — из-за того, что имеют одинаковые знаки, другие — из-за этого предположения) и мы получаем $n^k + 2B_1 n^k + 2B_k n = 0$. Поскольку $B_1 = -\dfrac{1}{2}$, ясно, что $B_k = 0$.

8.

$$P_1(x) = \frac{1}{2}x^2 - \frac{1}{2}x,\quad P_2(x) = \frac{1}{3}x^3 - \frac{1}{2}x^2 + \frac{1}{6}x,\quad P_3(x) = \frac{1}{4}x^4 - \frac{1}{2}x^3 + \frac{1}{4}x^2,\quad P_4(x) = \frac{1}{5}x^5 - \frac{1}{2}x^4 + \frac{1}{3}x^3 - \frac{1}{30}x,$$

$$P_5(x) = \frac{1}{6}x^6 - \frac{1}{2}x^5 + \frac{5}{12}x^4 - \frac{1}{12}x^2,\quad P_6(x) = \frac{1}{7}x^7 - \frac{1}{2}x^6 + \frac{1}{2}x^5 - \frac{1}{6}x^3 + \frac{1}{42}x,\quad P_7(x) = \frac{1}{8}x^8 - \frac{1}{2}x^7 + \frac{7}{12}x^6 - \frac{7}{24}x^4 + \frac{1}{12}x^2,$$

$$P_8(x) = \frac{1}{9}x^9 - \frac{1}{2}x^8 + \frac{2}{3}x^7 - \frac{7}{15}x^5 + \frac{2}{9}x^3 - \frac{1}{30}x,\quad P_9(x) = \frac{1}{10}x^{10} - \frac{1}{2}x^9 + \frac{3}{4}x^8 - \frac{7}{10}x^6 + \frac{1}{2}x^4 - \frac{3}{20}x^2,$$

$$P_{10}(x) = \frac{1}{11}x^{11} - \frac{1}{2}x^{10} + \frac{5}{6}x^9 - x^7 + x^5 - \frac{1}{2}x^3 + \frac{5}{66}x,\quad P_{11}(x) = \frac{1}{12}x^{12} - \frac{1}{2}x^{11} + \frac{11}{12}x^{10} - \frac{11}{8}x^8 + \frac{11}{6}x^6 - \frac{11}{8}x^4 + \frac{5}{12}x^2,$$

$$P_{12}(x) = \frac{1}{13}x^{13} - \frac{1}{2}x^{12} + x^{11} - \frac{11}{6}x^9 + \frac{22}{7}x^7 - \frac{33}{10}x^5 + \frac{5}{3}x^3 - \frac{691}{2730}x,$$

$$P_{13}(x) = \frac{1}{14}x^{14} - \frac{1}{2}x^{13} + \frac{13}{12}x^{12} - \frac{143}{60}x^{10} + \frac{143}{28}x^8 - \frac{143}{20}x^6 + \frac{65}{12}x^4 - \frac{691}{420}x^2,$$

$$P_{14}(x) = \frac{1}{15}x^{15} - \frac{1}{2}x^{14} + \frac{7}{6}x^{13} - \frac{91}{30}x^{11} + \frac{143}{18}x^9 - \frac{143}{10}x^7 + \frac{91}{6}x^5 - \frac{691}{90}x^3 + \frac{7}{6}x,$$

$$P_{15}(x) = \frac{1}{16}x^{16} - \frac{1}{2}x^{15} + \frac{5}{4}x^{14} - \frac{91}{24}x^{12} + \frac{143}{12}x^{10} - \frac{429}{16}x^8 + \frac{455}{12}x^6 - \frac{691}{24}x^4 + \frac{35}{4}x^2,$$

$$P_{16}(x) = \frac{1}{17}x^{17} - \frac{1}{2}x^{16} + \frac{4}{3}x^{15} - \frac{14}{3}x^{13} + \frac{52}{3}x^{11} - \frac{143}{3}x^9 + \frac{260}{3}x^7 - \frac{1382}{15}x^5 + \frac{140}{3}x^3 - \frac{3617}{510}x,$$

$$P_{17}(x) = \frac{1}{18}x^{18} - \frac{1}{2}x^{17} + \frac{17}{12}x^{16} - \frac{17}{3}x^{14} + \frac{221}{9}x^{12} - \frac{2431}{30}x^{10} + \frac{1105}{6}x^8 - \frac{11747}{45}x^6 + \frac{595}{3}x^4 - \frac{3617}{60}x^2,$$

$$P_{18}(x) = \frac{1}{19}x^{19} - \frac{1}{2}x^{18} + \frac{3}{2}x^{17} - \frac{34}{5}x^{15} + 34x^{13} - \frac{663}{5}x^{11} + \frac{1105}{3}x^9 - \frac{23494}{35}x^7 + 714x^5 - \frac{3617}{10}x^3 + \frac{43867}{798}x,$$

$$P_{19}(x) = \frac{1}{20}x^{20} - \frac{1}{2}x^{19} + \frac{19}{12}x^{18} - \frac{323}{40}x^{16} + \frac{323}{7}x^{14} - \frac{4199}{20}x^{12} + \\ + \frac{4199}{6}x^{10} - \frac{223193}{140}x^8 + 2261x^6 - \frac{68723}{40}x^4 + \frac{43867}{84}x^2$$

9. (**a**) $6P_1(x)P_2(x) = 5P_4(x) + P_2(x)$

(**b**) $3P_2(x)P_2(x) = 2P_5(x) + P_3(x)$

(**c**) $12P_2(x)P_3(x) = 7P_6(x) + 5P_4(x)$

(**d**) $2P_3(x)P_3(x) = P_7(x) + P_5(x)$

(**e**) очевидно: обозначим α старший коэффициент данного многочлена $P(x)$ степени k и применим предположение индукции (по степени многочлена) к многочлену $\widehat{P}(x) := P(x) - \alpha P_{k-1}(x)$ (степени не выше $k-1$).

(**f**) (Насколько мне известно, автор этого доказательства — Л. Посицельский. Недавно я выяснил, что формулы для $P_k(x)$ в [Пр] приводят к другому варианту следующей леммы.)

Определим оператор T на многочленах равенством $(TP)(x) := P(1-x)$. Положим $P_0(x) = x - \dfrac{1}{2}$ (!!).

Лемма. $(TP_k)(x) = (-1)^{k+1}P_k(x)$ *для всех* k.

Доказательство. Утверждение очевидно для $k=0$. Пусть $k>0$. Напомним, что $P_k(x+1)-P_k(x)=x^k$, $P_k(1)=0$ (см. решение 4). Мы докажем, что $(-1)^{k+1}(TP_k)(x)$ тоже удовлетворяет этим условиям. А поскольку такой многочлен степени $k+1$ ровно один, то лемма будет доказана. Перепишем первое равенство так: $(-1)^{k+1}P_k(-(-x))-(-1)^{k+1}P_k(1-(-x))=(-x)^k$, т.е. $(y:=-x)$ $y^k=(-1)^{k+1}P_k(-y)-(-1)^{k+1}P_k(1-y)=(-1)^{k+1}(TP_k)(y+1)-(-1)^{k+1}(TP_k)(y)$. $(-1)^{k+1}(TP_k)(1)=0$, поскольку $P_k(0)=0$ (см. формулу (1)), значит, оба равенства имеют место, что и требовалось.

Оставшаяся часть доказательства демонстрирует возможности линейной алгебры. Ясно, что $T(P_kP_l)=T(P_k)T(P_l)=(-1)^{k+l}P_kP_l$. Пусть для многочлена $P_k(x)P_l(x)$ (степени $k+l+2$) имеется такое представление: $P_k(x)P_l(x)=\sum\limits_{j=0}^{k+l+1}b_jP_j(x)$. Ясно, что $\sum\limits_{j=0}^{k+l+1}(-1)^{k+l+1}b_jP_j(x)=(-1)^{k+l}P_k(x)P_l(x)=T(P_kP_l)(x)=\sum\limits_{j=0}^{k+l+1}(-1)^{j+1}b_jP_j(x)$, и поскольку такое представление единственно, понятно, что b_j должны обратиться в нуль при $j\not\equiv k+l+1 \pmod 2$.

(Следующее решение было предложено О. Гольбергом и М. Левиным во время конференции. Оно сходно с приведённым выше решением задачи **7**.)

Заметим, что если $P_k(x)P_l(x)=\sum\limits_{j=0}^{k+l+1}b_jP_j(x)$, то $P_k(x+1)P_l(x+1)-P_k(x)P_l(x)=\sum\limits_{j=0}^{k+l+1}b_jx^j$. Но $P_k(x+1)=P_k(x)+x^k$, поэтому левая часть равна $x^{k+l}+x^kP_l(x)+x^lP_k(x)$. У этого многочлена коэффициенты той же чётности, что и $k+l$ (и не равные $k+l$), пропорциональны числам Бернулли с нечётными номерами, большими 1, и поэтому равны 0 согласно задаче **7**, а коэффициент при x^{k+l} равен $1+2B_1=0$. Поэтому соответствующие коэффициенты b_j равны 0.

Упражнение. (Полный ответ мне неизвестен.) Выразите коэффициенты b_j через числа Бернулли. Таким образом, имеющееся для многочлена $P_k(x)P_l(x)$ представление — это просто набор соотношений на числа Бернулли. Выпишите эти соотношения. Являются ли числа Бернулли единственной последовательностью, удовлетворяющей этим соотношениям?

(**g**) $60P_3(x)P_4(x)=27P_8(x)+35P_6(x)-2P_4(x)$.

10. В дальнейшем мы будем использовать такие обозначения: для рациональных чисел a, b будем писать $a\equiv b \pmod k$ (a сравнимо с b по модулю k), если числитель $a-b$ делится на k. (Наиболее внимательные читатели уже встретили это обозначение чуть выше…)

(**a**) Напомним Основную Теорему Арифметики: (точнее, утверждение, эквивалентное традиционной форме ОТА): если целые числа a,b не делятся на p, то и ab не делится на p. Из этого следует, что умножение всех остатков по модулю p на ненулевой остаток инъективно (т.е. переводит различные остатки в различные). Поэтому ясно, что для каждого ненулевого остатка a существует (единственный) остаток b, такой что $ab-1\equiv 0 \pmod p$ (различных остатков конечное число, поэтому в описанной выше ситуации каждый из них встретится).

(**b**) Используйте указание для доказательства второго утверждения. Мы же докажем первое. Для каждого a, не делящегося на p, остатки чисел $a,2a,\dots,(p-1)a$ образуют полную систему ненулевых остатков по модулю p. Поэтому $1\cdot 2\cdots(p-1)(a^{p-1}-1)=a\cdot 2a\cdots(p-1)a-1\cdot 2\cdots(p-1)\equiv 0 \pmod p$. Сократите $(p-1)!$ (взаимно простое с p число), чтобы завершить доказательство.

11. (**a**) Рассмотрим остаток $\widehat{k}$ числа k по модулю $p-1$. Тогда $a^k-a^{\widehat{k}}\equiv 0 \pmod p$ для любого a (очевидно), поэтому достаточно доказать, что $S_{\widehat{k}}(p)\equiv 0 \pmod p$. Пусть b — ненулевой остаток, такой что $b^{\widehat{k}}-1\not\equiv 0 \pmod p$. Изучим $b^{\widehat{k}}S_{\widehat{k}}(p)$. Поскольку $b,2b,\dots(p-1)b$ образуют полную систему ненулевых остатков, ясно, что $b^{\widehat{k}}S_{\widehat{k}}(p)-S_{\widehat{k}}(p)\equiv 0 \pmod p$. Завершите доказательство по образцу предыдущей задачи.

(**b**) Немедленное следствие задачи **10(b)**: $a^{l(p-1)}-1$ делится на $a^{p-1}-1\equiv 0 \pmod p$…

Определение. Пусть p — простое число. Будем называть рациональное число p-целым, если его знаменатель (в несократимой записи) не делится на p.

12. (Здесь мы следуем [БШ].) Полагая $n=p^r$ в (1), мы получаем

$$\frac{S_{2k}(p^r)}{p^r}-B_{2k}=\frac{1}{2k+1}\sum_{j=0}^{2k-1}\binom{2k+1}{j}B_jp^{r(2k-j)}.$$

Если r достаточно велико, то правая часть (а значит, и левая часть) является p-целым числом. С другой стороны при $m\geqslant 1$

$$S_{2k}(p^{m+1})=\sum_{u=0}^{p^m-1}\sum_{v=0}^{p-1}(u+vp^m)^{2k}\equiv p\sum_{u=0}^{p^m-1}u^{2k}+kp^m\sum_u u^{2k-1}\sum_v v\equiv pS_{2k}(p^m)(p^{m+1}),$$

и поэтому $\dfrac{S_{2k}(p^{m+1})}{p^{m+1}}-\dfrac{S_{2k}(p_m)}{p^m}$ — целое число. Значит, и $\dfrac{S_{2k}(p)}{p}-B_{2k}$ является p-целым числом. Замените

$S_{2k}(p)$ на 0 для $2k \not\equiv 0 \pmod{p-1}$ и $S_{2k}(p)$ на 1 для $2k \equiv 0 \pmod{p-1}$, чтобы доказать такое утверждение (именно оно нам и нужно):

Для любого простого числа q $B_{2k} + \sum_p \frac{1}{p}$ — q-целое число (суммирование происходит по простым p, для которых $2k \equiv 0 \pmod{p-1}$).

Поэтому это (рациональное) число является целым.

13. Легко проверить, что $44 \equiv 0 \pmod{p-1}$ для простого $p \Leftrightarrow p \in \{2, 3, 23\}$. Поэтому знаменатель B_{22} равен 138 и $B_{22} + \frac{1}{2} + \frac{1}{3} + \frac{1}{23}$ — целое число $\Rightarrow B_{22} = 6193 - \frac{1}{2} - \frac{1}{3} - \frac{1}{23} = 6193 - \frac{121}{138} = \frac{854513}{138}$.

14. Большинство участников использовали в решении частный случай теоремы Дирихле: существует бесконечно много простых чисел, сравнимых с 1 по модулю 3. Доказательство достаточно поучительно и заслуживает того, чтобы привести его здесь.

(По мотивам работ М. Левина, О. Гольберга, Р. Кралева, Д. Русева, В. Димитрова. Это достаточно известное рассуждение сугубо элементарно, в отличие от доказательства А. Энтина и Д. Файфмана: они использовали квадратичный закон взаимности.)

Докажем, что для любого простого q существует бесконечно много простых p, сравнимых с 1 по модулю q (для составного q доказательство требует немного больше техники, но в целом аналогично). Пусть таких простых чисел конечное число: $p_1, \ldots, p_k$. Рассмотрим число $m = n^{q-1} + n^{q-2} + \cdots + n + 1 = \frac{n^q - 1}{n-1}$, где $n = 2p_1 \cdots p_k$. Заметим, что наибольший общий делитель (НОД) чисел $n^a - 1$ и $n^b - 1$ равен $n^{\text{НОД}(a,b)} - 1$ (используйте алгоритм Евклида для доказательства). Поэтому $\text{НОД}(m, n^r - 1) = \text{НОД}(m, n-1)$ при $0 < r < q$. Но $\text{НОД}(m, n-1) = \text{НОД}(n^{q-2}(n-1) + 2n^{q-3}(n-1) + \cdots + (q-1)(n-1) + q, n-1) = \text{НОД}(q, n-1)$. Поскольку $n \equiv 2 \pmod q$, $\text{НОД}(n-1, q) = 1$. Значит, $\text{НОД}(m, n^r - 1) = 1$ при $0 < r < q$. Рассмотрим простой делитель p числа m. Тогда $n^{p-1} - 1 \equiv 0 \pmod p$ (см. **10(b)**; ясно, что n не делится на p) и $n^q - 1 \equiv 0 \pmod p$ (очевидно). Значит, $n^r - 1$ не делится на p при $0 < r < q$, и поскольку $\text{НОД}(n^{p-1} - 1, n^q - 1) = n^{\text{НОД}(p-1,q)} - 1$, мы видим, что $\text{НОД}(p-1, q) = q$, т. е. $p \equiv 1 \pmod q$, что приводит к противоречию (конечно, p не совпадает ни с одним из p_i).

Я всё же предпочитаю более элементарные подходы.

Первое решение.

Предположим, что все простые делители числа n сравнимы с 1 по модулю 6 (например, возьмите $n = 7, 7^2, 7^3 \ldots$). Пусть $q \neq 2, 3$ — простой делитель знаменателя B_{2n}. Тогда $q \equiv \pm 1 \pmod 6$ (q —простое), поэтому $q - 1$ делится либо на 6, либо на целое $m \equiv -1 \pmod 3$. Оба варианта вместе со сравнением $2n \equiv 0 \pmod{q-1}$ и предположением о структуре простых делителей n ведут к противоречию, которое и завершает доказательство.

Второе решение.

(Оно было известно мне раньше, но был рад обнаружить его в работе Е. Ференс–Сороцкого, О. Стырта и О. Евтифеевой.)

Для простого p все делители $2p$ — это $1, 2, p, 2p$, поэтому знаменатель B_{2p} равен 6, если $2p + 1$ не является простым числом (именно здесь можно использовать теорему Дирихле: для простого числа p, сравнимого с 1 по модулю 3, $2p + 1$ делится на 3 и не может быть простым числом). Иначе попробуйте $p := 2p + 1$ (а $2p + 1 := 4p + 3$) и т. д. (Составное число *встретится*: например, $2^{p-1}p + 2^{p-1} - 1$ делится на $p \ldots$)

15. (**a**) (**b**) Это решение навеяно работами А. Энтина и Д. Файфмана, О.Гольберга, М. Левина (сравните это с решением в [MC], использующим производящие функции). Главная идея состоит в том, чтобы использовать результат **16**; мы покажем, что для любого простого p число $a^{2n}(a^{2n} - 1)B_{2n}/2n$ является p-целым. Это очевидно для p, при которых $2n$ не делится на $p - 1$ (используйте **12** и **16**). Пусть $2n$ делится на $p - 1$; $2n = (p-1)p^k m$, где m не делится на p. Если a делится на p, то a^{2n} делится на p^{2n} (и делится на p^{k+1}, поскольку $2n \geqslant p^k \geqslant k + 1$, а знаменатель $B_{2n}/2n$ делится в точности на p^{k+1} — см. **12**). Если a не делится на p, то $a^{2n} - 1$ делится на p^{k+1}, поскольку $2n$ делится на $(p-1)p^k = \varphi(p^{k+1})$. (В этом состоит теорема Эйлера: для a, взаимно простого с n имеет место сравнение $a^{\varphi(n)} \equiv 1 \pmod n$, где $\varphi(n)$ — число натуральных чисел, меньших n и взаимно простых с n. Доказательство этого утверждения повторяет доказательство **10(b)**.)

16. (Это решение предложено А. Энтиным и Д. Файфманом. Основное преимущество состоит в том, что это решение легко переписать для задачи **17**. О. Гольберг и М. Левин использовали существование первообразного корня по модулю p^k (для $p \neq 2$); Е. Ференс–Сороцкий, О. Стырт и О. Евтифеева использовали для доказательства результат **15**, который вывели из весьма сложного решения **17**.)

Пусть $1 \leqslant g \leqslant p - 1$ таково, что $g^k - 1$ не делится на p при $0 < k < p - 1$(«g — первообразный корень по модулю p». **Упражнение.** Докажите, что такое g существует — это не очень сложно.)

$$\frac{gt}{e^{gt} - 1} - \frac{t}{e^t - 1} = \sum_{k \geqslant 1} (g^k - 1) B_k \frac{t^k}{k!} = t \sum_{k \geqslant 1} G_k \frac{t^{k-1}}{(k-1)!},$$

где $G_k = (g^k - 1)\dfrac{B_k}{k}$.

Перепишем это в виде $\sum\limits_{k\geqslant 1} G_k \dfrac{t^{k-1}}{(k-1)!} = \dfrac{g}{e^{gt}-1} - \dfrac{1}{e^t-1}$.

Обозначим $u = e^t - 1$.

$$\frac{g}{e^{gt}-1} - \frac{1}{e^t-1} = \frac{g}{(1+u)^g - 1} - \frac{1}{u} = \frac{g}{gu + \sum_{j=2}^{g} c_j u^j} - \frac{1}{u} = \frac{1}{u}\left(\frac{1}{1+\sum_{j=2}^{g} c_j u^{j-1}/g} - 1\right).$$

Заметим, что
$$\frac{1}{1+\sum_{j=2}^{g} c_j u^{j-1}/g} = 1 + \sum_{j\leqslant 1} d_j u^j,$$
где числа d_j — p-целые. Поэтому
$$\sum_{k\geqslant 1} G_k \frac{t^{k-1}}{(k-1)!} = \sum_{r\geqslant 0} a_r (e^t-1)^r = \sum_{r\geqslant 0} a_r \sum_{m=0}^{r} (-1)^{r-m}\binom{r}{m} e^{mt},$$
где все a_r — p-целые. Заменяя все e^{mt} на соответствующие степенные ряды, мы получаем
$$G_k = x_1 + x_2\cdot 2^{k-1} + \ldots x_k\cdot (k-1)^{k-1},$$
где все x_k — p-целые. (Здесь мы используем тот очевидный факт, что разложение в степенной ряд $(e^t-1)^m$ начинается с t^m.) Поэтому G_k — p-целое число для любого k. Вернёмся к решению задачи. B_{2n}/n — p-целое $\Rightarrow B_{2n}$ — p-целое (очевидно). Предположим, что B_{2n} — p-целое число. Это означает, что $2n$ не делится на $p-1$, поэтому $g^{2n}-1$ не делится на p, а потому $B_{2n}/n = \dfrac{2G_{2n}}{g^{2n}-1}$ — p-целое число.

17. (Большая часть работы проделана в приведённом решении **16**.) Запишем
$$G_{2k} = \sum_{m=1}^{2k+p-2} x_m m^{2k-1},$$
где x_m — p-целые (раскройте скобки в $\sum\limits_{r=0}^{2k+p-2} a_r(e^t-1)^r$, не обращая внимания, что в некоторых из этих скобок коэффициент при t^{2k-1} на самом деле нулевой). Понятно, что
$$G_{2k+p-1} = \sum_{m=1}^{2k+p-2} x_m m^{2k+p-2}.$$

Поэтому
$$G_{2k+p-1} - G_{2k} = \sum_{m=1}^{2k+p-2} x_m m^{2k-1}(m^{p-1}-1) \equiv 0 \pmod p.$$
$$G_{2k+p-1} - G_{2k} = g^{2k}(g^{p-1}-1)\frac{B_{2k+p-1}}{2k+p-1} + (g^{2k}-1)\left(\frac{B_{2k+p-1}}{2k+p-1} - \frac{B_{2k}}{2k}\right),$$
и поскольку $g^{2k}(g^{p-1}-1)\dfrac{B_{2k+p-1}}{2k+p-1} \equiv 0 \pmod p$ (используйте **10** и **12**) и $g^{2k}-1$ не делится на p ($2k$ не делится на $p-1$), мы видим, что
$$\frac{B_{2k+p-1}}{2k+p-1} - \frac{B_{2k}}{2k} \equiv 0 \pmod p$$
. Теперь сравнение Куммера доказывается индукцией по $2n-2k$.

18. Пусть иррегулярных простых чисел лишь конечное число: $p_1, \ldots, p_k$. Выберем натуральное n настолько большим, чтобы выполнялось $\left|\dfrac{B_{2m}}{2m}\right| > 1$ (где $m = n(p_1-1)\cdots(p_k-1)$). Ясно, что знаменатель $\dfrac{B_{2m}}{2m}$ делится на p_i при всех $i = 1, \ldots, k$ (используйте **12**), поэтому числитель этого числа должен быть равен ± 1 (согласно нашему предположению, если этот числитель делится на простое p, то p — одно из p_i.). Это противоречит $\left|\dfrac{B_{2m}}{2m}\right| > 1$.

19. (Доказательство И. Гуда (из [Гуд]); другое доказательство ключевого тождества есть в книге [Мак])[1]

[1]О, ужас! И это есть в книге [ГКП].

Обозначим этот свободный член $C(a_1,\dots,a_k)$. Докажем, что $C(a_1,\dots,a_k) = C(a_1-1,a_2,\dots,a_k)+\dots+C(a_1,\cdots,a_k-1)$ (имеют место очевидные начальные условия $C(a_1,\dots,a_{k-1},0) = C(a_1,\dots,a_{k-1})$ и $C(0)=1$). Поскольку мультиномиальные коэффициенты удовлетворяют тем же начальным условиям и рекуррентному соотношению, это докажет гипотезу Дайсона.

Рассмотрим многочлен $f(x)=\sum\limits_{j=1}^{n}\prod\limits_{i\neq j}\dfrac{x_i-x}{x_i-x_j}$. Его степень не превосходит $n-1$ и $f(x_1)=\dots=f(x_n)=1$, поэтому $f(x)\equiv 1$. Значит,

$$1=f(0)=\sum_{j=1}^{n}\prod_{i\neq j}\frac{x_i}{x_i-x_j}=\sum_{j=1}^{n}\prod_{i\neq j}\frac{1}{1-\dfrac{x_j}{x_i}}.$$

Умножив $\prod\limits_{1\leqslant i\neq j\leqslant n}\left(1-\dfrac{x_j}{x_i}\right)^{a_j}$ на это равенство, мы получим упомянутое рекуррентное соотношение.

20. Это простое упражнение по линейной алгебре. Для каждого подпространства выпишем все его (упорядоченные) базисы. Чтобы подсчитать количество подпространств, надо выяснить, сколько всего выписано базисов и сколько базисов соответствует одному подпространству. Количество различных (упорядоченных) наборов k линейно независимых векторов в n-мерном пространстве над полем $\mathbb{F}_q$ вычислить легко, если сообразить, что точек в таком n-мерном пространстве q^n (это особенно очевидно. если представлять себе n-мерное пространство «арифметическим», т. е. пространством n-ок элементов $\mathbb{F}_q$ с покоординатным сложением и умножением на число): есть q^n-1 способов выбрать первый вектор (надо лишь, чтобы он был ненулевым), q^n-q способов выбрать второй вектор (надо, чтобы он не лежал в (одномерной) линейной оболочке первого), q^n-q^2 способов выбрать третий вектор (надо, чтобы он не лежал в (двумерной) линейной оболочке первых двух) и т. д. Искомое число равно, таким образом, $(q^n-1)\cdots(q^n-q^{k-1}) = q^{k(k-1)/2}\dfrac{n!_q}{(n-k)!_q}(q-1)^k$. Сколько базисов выписано для каждого подпространства? Аналогичное рассуждение показывает, что их $q^{k(k-1)/2}k!_q(q-1)^k$. Поэтому различных подпространств

$$\frac{q^{k(k-1)/2}\dfrac{n!_q}{(n-k)!_q}(q-1)^k}{q^{k(k-1)/2}k!_q(q-1)^k}=\frac{n!_q}{k!_q(n-k)!_q}=\binom{n}{k}_q.$$

21. Пусть $y_{2n+1}^{(i)}=\sum\limits_{k\equiv i \pmod{p-1}}\binom{2n+1}{k}$, $i=0,1,\dots,p-2$. Докажем, что все эти $p-1$ последовательностей (занумерованных нечётными числами) периодичны по модулю p. Поскольку $y_{2n+1}^{(i)}=y_{2n-1}^{(i)}+2y_{2n-1}^{(i-1)}+y_{2n-1}^{(i-2)}$ (очевидно), достаточно доказать, что $y_0^{(i)}\equiv y_p^{(i)} \pmod p$ для любого $0<i<p-1$. А это ясно:

$$y_0^{(0)}=1\equiv 1+p=\binom{p}{0}+\binom{p}{p-1}=y_p^{(0)},$$

$$y_0^{(1)}=1\equiv p+1=\binom{p}{1}+\binom{p}{p}=y_p^{(1)},$$

$$y_0^{(i)}=0\equiv\binom{p}{i}=y_p^{(i)},\text{при } i=2,3,\dots,p-2.$$

Осталось заметить, что $y_{2n+1}^{(i)}=\binom{2n+1}{i}$ для любого $i=0,1,\dots,p-2$ при $2n+1\leqslant p-2$, в частности, $y_{2n+1}^{(0)}=1$ для таких n, а значит $y_{2n+1}^{(0)}\equiv 1 \pmod p$ при всех n. Но $y_{2n+1}^{(0)}=1+\sum\limits_{k>0}\binom{2n+1}{k(p-1)}$, поэтому утверждение задачи доказано.

Другое решение основано на таком соображении:

$$S_{2n+1}(p)=\sum_{i=0}^{p-1}i^{2n+1}\equiv\sum_{j=0}^{p-1}(j+1)^{2n+1}=\sum_{j=0}^{p-1}\sum_{k=0}^{2n+1}\binom{2n+1}{k}j^k=p+\sum_{k=1}^{2n+1}\binom{2n+1}{k}S_k(p),$$

и рассуждение в духе задачи **11** даёт цепочку сравнений

$$0\equiv S_{2n+1}(p)\equiv\sum_{k=1}^{p-1}\binom{2n+1}{k}S_k(p)\equiv\sum_{k>0}\binom{2n+1}{k(p-1)}\pmod p,$$

что и требовалось.

22. Указание: пусть $B(x)=\dfrac{t}{e^t-1}+\dfrac{t}{2}$. Проверьте, что $B(x)$ удовлетворяет следующему дифференциальному уравнению: $B^2(x)-B(x)+xB'(x)=\dfrac{x^2}{4}$ и что требуемое рекуррентное соотношение следует из этого уравнения.

23. Все решения этой задачи основаны на прямом вычислении. Мне понравилось следующее решение Е. Ференс–Сороцкого, О. Стырта и О. Евтифеевой.

Заметим, что $f(m,n)=f(n,m)$ и $f(-m,-n)=f(m,n)$. Поскольку $f(m,n)+f(m,-n)=\sum\limits_{0<2j<2k}\dfrac{1}{m^{2j}n^{2k-2j}}$ (слагаемые, содержащие n в нечётной степени, сокращаются, в чётной — удваиваются), то надо доказать, что

$$f(m,n)-f(m,m+n)-f(m+n,n)=f(m,n)+f(m,-n)\Leftrightarrow$$
$$f(m+n,n)+f(m,m+n)+f(m,-n)=0\Leftrightarrow$$
$$f(m+n,n)+f(-m,-m-n)+f(-n,m)=0.$$

Докажем, что для всех a,b,c, для которых $abc\neq 0$ и $a+b+c=0$, выполнено $f(a,-b)+f(b,-c)+f(c,-a)=0$. (После этого надо лишь подставить $a=m+n, b=-n, c=-m$.) Для этого преобразуем выражение для $f(m,n)$ (при $m\neq n$):

$$(n-m)f(m,n)=\frac{1}{mn^{2k-2}}-\frac{1}{n^{2k-1}}+$$
$$\frac{1}{m^{2k-1}}-\frac{1}{m^{2k-2}n}+\frac{1}{2}\sum_{j=2}^{2k-2}\frac{1}{m^jn^{2k-j-1}}-\frac{1}{2}\sum_{j=2}^{2k-2}\frac{1}{m^{j-1}n^{2k-j}}=$$
$$\frac{1}{2mn^{2k-2}}-\frac{1}{2m^{2k-2}n}+\frac{1}{m^{2k-1}}-\frac{1}{n^{2k-1}},$$

откуда

$$f(m,n)=\frac{1}{n-m}\left(\frac{1}{2mn^{2k-2}}-\frac{1}{2m^{2k-2}n}+\frac{1}{m^{2k-1}}-\frac{1}{n^{2k-1}}\right).$$

Завершить доказательство теперь очень просто:

$$f(a,-b)=\frac{1}{c}\left(\frac{1}{2ab^{2k-2}}+\frac{1}{2a^{2k-2}b}+\frac{1}{a^{2k-1}}+\frac{1}{b^{2k-1}}\right),$$

$$f(b,-c)=\frac{1}{a}\left(\frac{1}{2bc^{2k-2}}+\frac{1}{2b^{2k-2}c}+\frac{1}{b^{2k-1}}+\frac{1}{c^{2k-1}}\right),$$

$$f(c,-a)=\frac{1}{b}\left(\frac{1}{2ca^{2k-2}}+\frac{1}{2c^{2k-2}a}+\frac{1}{c^{2k-1}}+\frac{1}{a^{2k-1}}\right),$$

$$f(a,-b)+f(b,-c)+f(c,-a)=$$
$$\frac{1}{a^{2k-2}}\left(\frac{1}{ab}+\frac{1}{bc}+\frac{1}{ca}\right)+\frac{1}{b^{2k-2}}\left(\frac{1}{ab}+\frac{1}{bc}+\frac{1}{ca}\right)+\frac{1}{c^{2k-2}}\left(\frac{1}{ab}+\frac{1}{bc}+\frac{1}{ca}\right)=$$
$$\left(\frac{1}{a^{2k-2}}+\frac{1}{b^{2k-2}}+\frac{1}{c^{2k-2}}\right)\left(\frac{1}{ab}+\frac{1}{bc}+\frac{1}{ca}\right)=$$
$$\left(\frac{1}{a^{2k-2}}+\frac{1}{b^{2k-2}}+\frac{1}{c^{2k-2}}\right)\left(\frac{a+b+c}{abc}\right)=0.$$

24. Просуммируем равенства предыдущей задачи по всем натуральным m,n. Заметим, что

$$\sum_{m,n}\frac{1}{m^{2j}n^{2k-2j}}=\zeta(2j)\zeta(2k-2j),$$

$$\sum_{m,n}f(m,m+n)=\sum_{m<n}f(m,n),$$

$$\sum_{m,n}f(m+n,n)=\sum_{m>n}f(m,n),$$

поэтому

$$\left(k+\frac{1}{2}\right)\zeta(2k)=\sum_{m=n}f(m,n)=\sum_{m,n}f(m,n)-\sum_{m<n}f(m,n)-\sum_{m>n}f(m,n)=$$

$$\sum_{m,n}\left(f(m,n)-f(m,m+n)-f(m+n,n)\right)=\sum_{0<2j<2k}\sum_{m,n}\frac{1}{m^{2j}n^{2k-2j}}=\sum_{0<2j<2k}\zeta(2j)\zeta(2k-2j),$$

что даёт

$$\frac{2k-1}{2}\zeta(2k)=\sum_{j=0}^{k}\zeta(2j)\zeta(2k-2j).$$

Осталось сопоставить это рекуррентное соотношение с рекуррентным соотношением задачи **22** и получить классическую формулу

$$\zeta(2k)=(-1)^{k-1}\frac{(2\pi)^{2k}B_{2k}}{2(2k)!}.$$

Замечание. Из этой формулы, в частности, легко следует оценка роста чисел Бернулли, использованная в задаче **18**.

25. Приведём здесь несколько объяснений разной степени убедительности.

- («Далеко идущее объяснение».)

$$\sum_{k\geqslant 0}\frac{B_k}{k!}t^k=\frac{t}{e^t-1}=-t\cdot\frac{1}{1-e^t}=-t\cdot(1+e^t+e^{2t}+\dots)=$$

$$-t\cdot\left(1+\sum_{n\geqslant 0}\frac{t^n}{n!}\sum_{k\geqslant 1}k^n\right)=-t-\sum_{n\geqslant 1}\frac{t^n}{n!}\left(n\sum_{k\geqslant 1}k^{n-1}\right).$$

  Сравним коэффициенты при одинаковых степенях t:

  при t^n $(n>1)$: $-n\sum_{k\geqslant 1}k^{n-1}=B_n$, откуда $\zeta(1-n)=-\dfrac{B_n}{n}$;

  при t^1: $-\sum_{k\geqslant 1}1-1=-\dfrac{1}{2}$, откуда $\zeta(0)=-\dfrac{1}{2}$

  (при t^0: $1=0$, откуда…).

- (Это объяснение предложили А. Энтин и Д. Файфман.) Определим многочлены Бернулли $B_n(x)$ равенством $B_n(x)=nP_{n-1}(x)+B_n$. Тогда $P_{n-1}(x)=\dfrac{B_n(x)-B_n}{n}$,

$$k^{n-1}=P_{n-1}(k+1)-P_{n-1}(k)=\frac{B_n(k+1)-B_n}{n}-\frac{B_n(k)-B_n}{n}=\frac{B_n(k+1)-B_n(k)}{n},$$

$$\sum_{k\geqslant 1}k^{n-1}=\frac{1}{n}\sum_{k\geqslant 1}\left(B_n(k+1)-B_n(k)\right)=-\frac{B_n(1)}{n}=-\frac{nP_{n-1}(1)+B_n}{n}=-\frac{B_n}{n}.$$

  (Проблема здесь в том, что определяя разными способами многочлены Бернулли, можно получить любой ответ. Конечно, для А. Энтина и Д. Файфмана было очевидно преимущество многочленов Бернулли, т. к. они успешно использовали разложение этих многочленов в ряды Фурье при решении задачи **24**…)

- («Объяснение в духе Абеля»(соответствующий метод суммирования рядов приписывается Абелю).) Легко проверить, что имеют место равенства (формальных рядов):

$$1-2x+3x^2-4x^3+\dots=\frac{1}{(1+x)^2},\quad 1^2-2^2x+3^2x^2-4^2x^3+\dots=\frac{1-x}{(1+x)^3}.$$

  Значит,

$$1+2+\dots-4(1+2+\dots)=1-2+3-4+\dots=1-2x+3x^2-4x^3+\dots\Big|_{x=1}=\left.\frac{1}{(1+x)^2}\right|_{x=1}=\frac{1}{4},$$

$$1^2+2^2+\dots-8(1^2+2^2+\dots)=1^2-2^2+3^2-4^2+\dots=1^2-2^2x+3^2x^2-4^2x^3+\dots\Big|_{x=1}=\left.\frac{1-x}{(1+x)^3}\right|_{x=1}=0,$$

откуда $1+2+\dots=-\frac{1}{12}$, $1^2+2^2+\dots=0$.

Упражнение. (Предупреждение: это упражнение — сложное.) Придумайте аналогичное объяснение в общем случае.

26. (Здесь приводится рассуждение, которое содержит решения большинства задач про числители и знаменатели чисел Бернулли. Его не придумал ни один участник конференции. Другое решение можно найти в [Ко], правда, чтобы его освоить, надо предварительно прочитать (там же) про p-адическое интегрирование.)

Обозначим σ_{2m} наименьшее натуральное число, для которого все числа $\frac{1}{2m+1}B_k p^{\sigma_{2m}}$ являются p-целыми ($0\leqslant k\leqslant 2m-1$). Тогда

$$S_{2m}(p^r)-p^rB_{2m}\equiv 0 \pmod{p^{2r-\sigma_{2m}}} \qquad (*)$$

. Пусть r достаточно велико, например, $r>\max(\sigma_{2m}+2m+N,\sigma_{2n}+2n+N)$. Рассмотрим целое a (его выбор будет уточнён позже), не делящееся на p. Для $i=1,\dots,p^r-1$ обозначим $b_i(r)$ остаток ia по модулю p^r: $ia=b_i(r)+p^rq_i(r)$, $0<b_i(r)<p^r$. Тогда

$$i^{2m}a^{2m}\equiv b_i(r)^{2m}+2mb_i(r)^{2m-1}q_i(r)p^r \pmod{p^{2r}}.$$

Суммируя по $i=1,\dots,p^r-1$, получаем

$$a^{2m}S_{2m}(p^r)\equiv S_{2m}(p^r)+2mp^r\left(\sum_{i=1}^{p^r-1}b_i(r)^{2m-1}q_i(r)\right) \pmod{p^{2r}},$$

что можно записать в виде

$$(a^{2m}-1)S_{2m}(p^r)\equiv 2mp^r\left(\sum_{i=1}^{p^r-1}b_i(r)^{2m-1}q_i(r)\right) \pmod{p^{2r}}.$$

Из сравнения (*) следует

$$(a^{2m}-1)p^rB_{2m}\equiv 2mp^r\left(\sum_{i=1}^{p^r-1}b_i(r)^{2m-1}q_i(r)\right) \pmod{p^{2r-\sigma_{2m}}},$$

откуда

$$(a^{2m}-1)B_{2m}\equiv 2m\left(\sum_{i=1}^{p^r-1}b_i(r)^{2m-1}q_i(r)\right) \pmod{p^{r-\sigma_{2m}}}.$$

Поскольку $p^{2m}>2m$ (очевидно), то ясно, что

$$(a^{2m}-1)\frac{B_{2m}}{2m}\equiv \sum_{i=1}^{p^r-1}b_i(r)^{2m-1}q_i(r) \pmod{p^{r-\sigma_{2m}-2m}}. \qquad (**)$$

Выделим из суммы в правой части сумму $b_i(r)$, не делящихся на p. Обозначим эту сумму Σ_{2m}. Ближайшей нашей целью будет разобраться с оставшейся частью суммы в правой части: $\sum\limits_{i=1}^{p^{r-1}-1}b_{pi}(r)^{2m-1}q_{pi}(r)$. Обозначим $c_i=\frac{b_{pi}(r)}{p}$ ($i=1,\dots,p^{r-1}-1$). Очевидно, что $c_i=b_i(r-1)$, $q_{pi}(r)=q_i(r-1)$. Запишем сравнение (**) с заменой r на $r-1$:

$$(a^{2m}-1)\frac{B_{2m}}{2m}\equiv \sum_{i=1}^{p^{r-1}-1}b_i(r-1)^{2m-1}q_i(r-1) \pmod{p^{r-1-\sigma_{2m}-2m}}.$$

Но легко видеть, что

$$\sum_{i=1}^{p^{r-1}-1}b_i(r-1)^{2m-1}q_i(r-1)=\sum_{i=1}^{p^{r-1}-1}c_i^{2m-1}q_i(r-1)=\frac{1}{p^{2m-1}}\sum_{i=1}^{p^{r-1}-1}b_{pi}(r)^{2m-1}q_{pi}(r).$$

Поэтому
$$p^{2m-1}(a^{2m}-1)\frac{B_{2m}}{2m} \equiv \sum_{i=1}^{p^{r-1}-1} b_{pi}(r)^{2m-1} q_{pi}(r) \pmod{p^{r-\sigma_{2m}-2m}}$$
(очевидно, что $2m-1 \geqslant 1$). Подстановка этого в сравнение (**) даёт
$$(a^{2m}-1)\frac{B_{2m}}{2m} \equiv \Sigma_{2m} + \sum_{i=1}^{p^{r-1}-1} b_{pi}(r)^{2m-1} q_{pi}(r) \equiv \Sigma_{2m} + p^{2m-1}(a^{2m}-1)\frac{B_{2m}}{2m} \pmod{p^{r-\sigma_{2m}-2m}},$$
что можно переписать в удобном виде
$$(a^{2m}-1)(1-p^{2m-1})\frac{B_{2m}}{2m} \equiv \Sigma_{2m} \pmod{p^{r-\sigma_{2m}-2m}},$$
откуда (напомним, что r достаточно велико)
$$(a^{2m}-1)(1-p^{2m-1})\frac{B_{2m}}{2m} \equiv \Sigma_{2m} \pmod{p^{N+1}}$$
и точно так же
$$(a^{2n}-1)(1-p^{2n-1})\frac{B_{2n}}{2n} \equiv \Sigma_{2n} \pmod{p^{N+1}}.$$
Поскольку $2m-2n$ делится на $p^{N+1}-p^N=\varphi(p^{N+1})$ по условию, а числа $b_i(r)$ (те, что собраны в Σ_{2m} и Σ_{2n}) не делятся на p, то из теоремы Эйлера следует, что
$$(a^{2n}-1)(1-p^{2n-1})\frac{B_{2n}}{2n} \equiv \Sigma_{2n} \equiv \Sigma_{2m} \equiv (a^{2m}-1)(1-p^{2m-1})\frac{B_{2m}}{2m} \pmod{p^{N+1}},$$
откуда (a тоже не делится на p)
$$(a^{2n}-1)\left((1-p^{2n-1})\frac{B_{2n}}{2n} - (1-p^{2m-1})\frac{B_{2m}}{2m}\right) \equiv 0 \pmod{p^{N+1}}.$$
Осталось лишь выбрать a таким, что $a^{2n}-1$ не делится на p, что возможно, т. к. $2n$ не делится на $p-1$.

Литература

[БШ] З. И. Боревич, И. Р. Шафаревич. Теория чисел. Москва, Наука, 1985.

[Ге] А. О. Гельфонд. Исчисление конечных разностей. Москва-Ленинград, ГИТТЛ, 1952.

[Гуд] I. J. Good. A short proof of a conjecture of Dyson. J. Math. Phys., 11, 1970.

[ГКП] Р. Л. Грэхем, Д. Е. Кнут, О. Паташник. Конкретная математика. Москва, Мир, 1998.

[Ко] Н. Коблиц. P-адические числа, p-адический анализ и дзета-функции. Москва, Мир, 1982.

[Мак] И. Г. Макдональд. Симметрические функции и многочлены Холла. Москва, Мир, 1985.

[МС] Д. Милнор, Д. Сташефф. Характеристические классы. Москва, Мир, 1979.

[Пр] В. В. Прасолов. Задачи и теоремы линейной алгебры. Москва, Наука, 1996.