Solutions for «Power Sums and Bernoulli Numbers»

Most of the solutions below were known to the jury before — but not all! Later I hope to choose the best solutions for all problems from the submitted works — that will be in fact the result of the conference. You are encouraged to ask questions (by email: `dotsenko@mccme.ru`).

1. (**a**) (**b**) The proof is standard. Let us formulate an equivalent question: how many times does the term $x_1^{a_1}\cdots x_k^{a_k}$ occur in $(x_1+\cdots+x_k)^n$? This number is equal to the number of ways to split n given brackets into k groups: first group containing a_1 brackets, second one containing a_2 of them, ... , kth one containing a_k of them. Details are left to the reader.

2. (**a**) (**b**) One can easily find a simple combinatorial interpretation for $[a]^n$ and $[a]_n$ for an integer a: for example, $[a]_n$ is the number of ways to choose a chairman, a deputy chairman, ... , a «deputy^{n-1} chairman» in a committee of a persons.

Exercise. Conclude the proof for integers a, b.

For general a, b use the following fact: a polynomial in a, b vanishes in all integer points if and only all its coefficients are equal to 0.

3. Hint: show that both $\binom{n}{k}_q$ and the coefficients of the left-hand side satisfy the same recurrence relation.

4. (**a**) The proof involves a very important method: calculus of finite differences (see [Ge]). The main idea is very simple: imagine that you know a polynomial $Q(x)$ such that $Q(1)=0$ («initial condition») and $Q(x+1)-Q(x)=x^k$. Then $Q(x)=P_k(x)$: $1^k+2^k+\cdots+(n-1)^k=Q(2)-Q(1)+Q(3)-Q(2)+\cdots+Q(n)-Q(n-1)=Q(n)$. Let us show that such a polynomial of degree $k+1$ exists (and is unique). Let $Q(x)=q_0+q_1x+\cdots+q_kx^k+q_{k+1}x^{k+1}$. Then $Q(x+1)-Q(x)=(k+1)q_{k+1}x^k+(\binom{k+1}{2}q_{k+1}+kq_k)x^{k-1}+\ldots$, so it is clear that q_i can be easily found one by one from these equations (such a situation is called «a system of linear equations with an upper triangular matrix») and the $k+2$-tuple $(q_0,\ldots,q_{k+1})$ is unique (it is determined up to the constant term q_0, which is obtained from the initial condition).

(**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. This immediately follows from the definition of the Bernoulli numbers. Let us illustrate how powerful the method of generating functions is. Let

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

Then it is clear that

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

so $\widehat{B}_k$ and B_k satisfy the same recurrence relation and initial condition and thus coincide. The rest of the proof is very simple: the exponential generating function for the power sums $S_k(n)$ with fixed n is

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

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	$-\frac{174611}{330}$

$$5, 7, 691, 3617, 43867 \text{ are prime},\ \ 6=2\cdot 3,\ \ 30=2\cdot 3\cdot 5,\ \ 42=2\cdot 3\cdot 7,\ \ 66=2\cdot 3\cdot 11,\ \ 2730=2\cdot 3\cdot 5\cdot 7\cdot 13,$$

$$510=2\cdot 3\cdot 5\cdot 17,\ 798=2\cdot 3\cdot 7\cdot 19,\ \ 174611=283\cdot 617,\ \ 330=2\cdot 3\cdot 5\cdot 11.$$

7. (This solution was suggested by E. Ferens–Sorotskij, O. Styrt and O. Evtifeeva during the conference; I did not know it before. Other participants checked that the function $f(t)=\dfrac{t}{e^t-1}+\dfrac{t}{2}$ is even, but the correct explanation meets some difficulties...)

Let k be the minimal odd number greater than 1 such that $B_k \neq 0$. $P_k(n) + n^k = P_k(n+1) = P_k(-n)$ — see solution for **9(e)** for details. This means that

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

By our hypothesis, $B_3 = B_5 = \cdots = B_{k-2} = 0$, therefore almost all terms cancel and we have $n^k + 2B_1 n^k + 2B_k n = 0$. Since $B_1 = -\dfrac{1}{2}$, we see that $B_k = 0$.

8.

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

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

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

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

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

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

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

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

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

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

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

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

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**) is obvious: denote by α the leading coefficient of the given polynomial $P(x)$ of degree k and apply the inductive hypothesis to the polynomial $\widehat{P}(x) := P(x) - \alpha P_{k-1}(x)$ (of degree less than k).

(**f**) (This proof is, as far as I know, due to L.Positselskij. Recently I found out that the collection of formulae for $P_k(x)$ in [Pr] leads to another variant of the following lemma.)

Define an operation T on polynomials by $(TP)(x) := P(1-x)$. Assign $P_0(x) = x - \dfrac{1}{2}$ (!!).

Lemma. $(TP_k)(x) = (-1)^{k+1}P_k(x)$ *for all* k.

Proof. It is obvious for $k = 0$. Assume that $k > 0$. Recall that $P_k(x+1) - P_k(x) = x^k$, $P_k(1) = 0$ (see the solution for 4), $P_k(0) = 0$ (use explicit formula (1)). This means that $(-1)^{k+1}P_k(-(-x)) - (-1)^{k+1}P_k(1-(-x)) = (-x)^k$, i.e., $(y := -x)$

$$y^k = (-1)^{k+1}P_k(-y) - (-1)^{k+1}P_k(1-y) = (-1)^{k+1}(TP_k)(y+1) - (-1)^{k+1}(TP_k)(y).$$

$(-1)^{k+1}(TP_k)(1) = 0$ because $P_k(x)$ vanishes at zero, hence $(-1)^{k+1}TP_k(x)$ satisfies the same conditions and the uniqueness of P_k completes the proof. $\square$

The rest of the proof shows the power of linear algebra. It is clear that $T(P_kP_l) = T(P_k)T(P_l) = (-1)^{k+l}P_kP_l$. Let $P_k(x)P_l(x)$ (a polynomial of degree $k+l+2$) have the following expansion in P_j's: $P_k(x)P_l(x) = \sum_{j=0}^{k+l+1} b_jP_j(x)$. It follows that $\sum_{j=0}^{k+l+1}(-1)^{k+l+1}b_jP_j(x) = (-1)^{k+l}P_k(x)P_l(x) = T(P_kP_l)(x) = \sum_{j=0}^{k+l+1}(-1)^{j+1}b_jP_j(x)$ and since such an expansion is unique we see that b_j must vanish for $j \not\equiv k+l+1 \pmod 2$.

(The following solution was submitted by O. Golberg and M. Levin during the conference. It looks like the above solution for **7**.)

Let us notice that if $P_k(x)P_l(x) = \sum_{j=0}^{k+l+1} b_jP_j(x)$, then $P_k(x+1)P_l(x+1) - P_k(x)P_l(x) = \sum_{j=0}^{k+l+1} b_jx^j$. But $P_k(x+1) = P_k(x) + x^k$, therefore the left-hand side equals $x^{k+l} + x^kP_l(x) + x^lP_k(x)$. The x^j's coefficients (with $j \equiv k+l \pmod 2$, $j < k+l$) of this polynomial are ¡proportional¿ to the Bernoulli numbers B_k with odd k and hence they are equal to zero according to **7**, and x^{k+l}'s coefficient equals $1 + 2B_1 = 0$. Therefore the corresponding b_j are equal to zero.

Exercise. (I do not know the complete answer.) Calculate the coefficients b_j (it is clear that the answer involves Bernoulli numbers). Therefore the representation for $P_k(x)P_l(x)$ is just a set of equations on Bernoulli numbers. Write out these equations. Is $\{B_n\}$ the unique sequence satisfying these equations?

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

10. Let us introduce the notation: for rational a, b we write $a \equiv b \pmod k$ (a is congruent to b modulo k) if the numerator of $a - b$ is divisible by k. (Most concentrated readers noticed this notation above...)

(**a**) Recall the Fundamental Theorem of Arithmetic (speaking more precisely, this statement is equivalent to the traditional form of FTA): if integers $a, b \not\equiv 0(p)$ then $ab \not\equiv 0(p)$. This implies that multiplication by a non-zero remainder modulo p is injective (i.e., maps different remainders into different ones). Therefore it is obvious that for each non-zero remainder a there exists (a unique) remainder b such that $ab - 1 \equiv 0(p)$ (there are only finitely many remainders, so the above means that each of them will occur).

(**b**) One may use the hint in order to prove the second statement. Let us deal with the first one. For each a not divisible by p the remainders of $a, 2a, \ldots, (p-1)a$ form the complete system of non-zero remainders modulo p. Hence $1\cdot 2\cdots(p-1)(a^{p-1}-1) = a\cdot 2a\cdots(p-1)a - 1\cdot 2\cdots(p-1) \equiv 0(p)$. Cancel $(p-1)!$ (it is relatively prime to p) to conclude the proof.

11. (**a**) Consider the remainder $\widehat{k}$ of k modulo $p-1$. Then $a^k - a^{\widehat{k}} \equiv 0(p)$ for all a (it is obvious), so let us show that $S_{\widehat{k}}(p) \equiv 0(p)$. Let b be a non-zero remainder such that $b^{\widehat{k}} - 1 \not\equiv 0(p)$. Examine $b^{\widehat{k}}S_{\widehat{k}}(p)$. Since $b, 2b, \ldots (p-1)b$ form the complete system of non-zero remainders, we see that $b^{\widehat{k}}S_{\widehat{k}}(p) - S_{\widehat{k}}(p) \equiv 0(p)$. To conclude the proof, proceed as above.

(**b**) is a straightforward corollary of **10(b)**: $a^{l(p-1)} - 1$ is divisible by $a^{p-1} - 1 \equiv 0(p)\ldots$

Definition. Let p be a prime. Let us call a rational number a p-integer if its denominator is not divisible by p.

12. (Here we follow [BSh].) Setting $n = p^r$ in (1), we see that

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

If r is large enough the right-hand side (and the left-hand side as well) is a p-integer. On the other hand for $m \geqslant 1$

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

and this implies that $\dfrac{S_{2k}(p^{m+1})}{p^{m+1}} - \dfrac{S_{2k}(p_m)}{p^m}$ is an integer. Thus $\dfrac{S_{2k}(p)}{p} - B_{2k}$ is a p-integer as well. One may replace $S_{2k}(p)$ by 0 for $2k \not\equiv 0(p-1)$ and $S_{2k}(p)$ by 1 for $2k \equiv 0(p-1)$ to obtain the following statement (which is just what we need):

For any prime number q $B_{2k} + \sum_p \frac{1}{p}$ is a q-integer (here the summation is taken over primes p such that $2k \equiv 0(p-1)$).

Hence this (rational) number is an integer.

13. One may check that $44 \equiv 0(p-1)$ for a prime $p \Leftrightarrow p \in \{2, 3, 23\}$. Hence the denominator of B_{22} is 138 and $B_{22} + \frac{1}{2} + \frac{1}{3} + \frac{1}{23}$ is an integer $\Rightarrow B_{22} = 6193 - \frac{1}{2} - \frac{1}{3} - \frac{1}{23} = 6193 - \frac{121}{138} = \frac{854513}{138}$.

14. Most of the participants used here the following version of the Dirichlet theorem: there is infinitely many primes having remainder 1 modulo 3. The proof of this fact is interesting enough to be written down here.

(Based on the works submitted by M. Levin, O. Golberg, R. Kralev, D. Rusev, V. Dimitrov. This elementary proof is well known. A. Entin and D. Faifman used the quadratic reciprocity law in their proof.)

Let us prove that for all primes q there exist infinitely many primes p having remainder 1 modulo q (one may rewrite this proof for a composite q; it is similar, but slightly more technical). Assume that there are only finitely many such primes: $p_1, \dots, p_k$. Consider the number $m = n^{q-1} + n^{q-2} + \dots + n + 1 = \dfrac{n^q - 1}{n-1}$, where $n = 2p_1 \cdots p_k$. Let us notice that the greatest common divisor (gcd) of $n^a - 1$ and $n^b - 1$ equals $n^{\gcd(a,b)} - 1$ (use Euclid's algorithm). It follows that $\gcd(m, n^r - 1) = \gcd(m, n-1)$ for $0 < r < q$. But $\gcd(m, n-1) = \gcd(n^{q-2}(n-1) + 2n^{q-3}(n-1) + \dots + (q-1)(n-1) + q, n-1) = \gcd(q, n-1)$. As $n \equiv 2 \pmod q$, $\gcd(n-1, q) = 1$. This means that $\gcd(m, n^r - 1) = 1$ for $0 < r < q$. Let p be a prime divisor of m. Then $n^{p-1} - 1 \equiv 0 \pmod p$ (use **10(b)**; it is clear that n is not divisible by p) and $n^q - 1 \equiv 0 \pmod p$ (it is obvious). Hence $n^r - 1$ is not divisible by p for $0 < r < q$, and since $\gcd(n^{p-1} - 1, n^q - 1) = n^{\gcd(p-1,q)} - 1$, we see that $\gcd(p-1, q) = q$, i. e., $p \equiv 1 \pmod q$, and the contradiction concludes the proof (p is not equal to any of p_i).

Still I prefer solutions which avoid such strong machinery…

First solution.

Suppose that for any prime p such that n is divisible by p p is congruent to 1 modulo 6 (for example, take $n = 7, 7^2, 7^3 \dots$). Let $q \neq 2, 3$ be a prime divisor of B_{2n}'s denominator. It follows that $q \equiv \pm 1 (6)$, so $q - 1$ is divisible either by 6 or by an integer $m \equiv -1 (3)$. Both cases together with the equivalence $2n \equiv 0 (q-1)$ and the assumption about prime divisors of n lead to contradiction which concludes the proof.

Second solution.

(It was known to me before, but I was glad to see it in the text submitted by E. Ferens–Sorotskij, O. Styrt and O. Evtifeeva.)

For a prime p all divisors of $2p$ are $1, 2, p, 2p$, so the denominator of B_{2p} is equal to 6 unless $2p + 1$ is a prime number (here you may use Dirichlet theorem: for a prime p having remainder 1 modulo 3 the number $2p + 1$ is divisible by 3 and hence is composite). Otherwise try $p := 2p + 1$(and $2p + 1 := 4p + 3$) etc. (There *will* occur a composite number: for example, $2^{p-1} p + 2^{p-1} - 1$ is divisible by $p \dots$)

15. (**a**) (**b**) Let us follow the solutions suggested by A. Entin and D. Faifman, O.Golberg, M. Levin (compare this to the one in [MS], which involves generating functions). The idea is to draw on the result of **16**: we will show that for each prime p the number $a^{2n}(a^{2n} - 1) B_{2n}/2n$ is a p-integer. It is obvious for p such that $2n$ is not divisible by $p - 1$ (use **12** and **16**). Suppose that $2n$ is divisible by $p - 1$; $2n = (p-1)p^k m$, where m is not divisible by p. For a divisible by p its power a^{2n} is divisible by p^{2n} (it is divisible by p^{k+1} because $2n \geqslant p^k \geqslant k + 1$, and the denominator of $B_{2n}/2n$ is divisible by exactly p^{k+1} — see **12**). For a not divisible by p the number $a^{2n} - 1$ is divisible by p^{k+1} because $2n$ is divisible by $p^{k+1} - p^k = \varphi(p^{k+1})$. (Here we use Euler's theorem: for a relatively prime to n there holds an equivalence $a^{\varphi(n)} \equiv 1(n)$, where $\varphi(n)$ denotes the number of integers less than n and relatively prime to n. The proof is similar to the proof of **10(b)**.)

16. (This solution was suggested by A. Entin and D. Faifman. The main advantage of this approach is that one may easily rewrite it for **17**. O. Golberg and M. Levin used the existence of a primitive root modulo p^k (for $p \neq 2$); E. Ferens–Sorotskij, O. Styrt and O. Evtifeeva deduced it from **15**, which was deduced from a very complicated solution of **17**.)

Let $1 \leqslant g \leqslant p - 1$ be such that $g^k - 1$ is not divisible by p for $0 < k < p - 1$(«g is a primitive root modulo p». **Exercise.** Prove that there exists such a g — it is not very difficult.)

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

where $G_k = (g^k - 1)\dfrac{B_k}{k}$. $\sum\limits_{k \geqslant 1} G_k \dfrac{t^{k-1}}{(k-1)!} = \dfrac{g}{e^{gt} - 1} - \dfrac{1}{e^t - 1}$.

Denote $e^t - 1$ by u.

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

Let us notice that

$$\frac{1}{1 + \sum_{j=2}^{g} c_j u^{j-1}/g} = 1 + \sum_{j \leqslant 1} d_j u^j,$$

where the denominators of d_j are not divisible by p. Therefore

$$\sum_{k \geqslant 1} G_k \frac{t^{k-1}}{(k-1)!} = \sum_{r \geqslant 0} a_r (e^t - 1)^r = \sum_{r \geqslant 0} a_r \sum_{m=0}^{r} (-1)^{r-m} \binom{r}{m} e^{mt},$$

where all a_r are p-integers. Replacing all e^{mt} by the corresponding power series gives us

$$G_k = x_1 + x_2 \cdot 2^{k-1} + \dots x_k \cdot (k-1)^{k-1},$$

where x_k are p-integers. (Here we use the fact that the power series expansion for $(e^t-1)^m$ starts from t^m.) Therefore G_k is a p-integer for all k. Let us return to the solution. B_{2n}/n is a p-integer $\Rightarrow$ B_{2n} is a p-integer (it is obvious). Suppose that B_{2n} is a p-integer. This means that $2n$ is not divisible by $p-1$, so $g^{2n}-1$ is not divisible by p and thus $\dfrac{B_{2n}}{n} = \dfrac{2G_{2n}}{g^{2n}-1}$ is a p-integer.

17. (Most of the work was done in the above solution for **16**.) Write

$$G_{2k} = \sum_{m=1}^{2k+p-2} x_m m^{2k-1},$$

where x_m are p-integers (expand the sum $\sum\limits_{r=0}^{2k+p-2} a_r(e^t-1)^r$). Then it is clear that

$$G_{2k+p-1} = \sum_{m=1}^{2k+p-2} x_m m^{2k+p-2}$$

(the proof is similar to the one above). Thus

$$G_{2k+p-1} - G_{2k} = \sum_{m=1}^{2k+p-2} x_m m^{2k-1}(m^{p-1}-1),$$

so its numerator is divisible by p.

$$G_{2k+p-1} - G_{2k} = g^{2k}(g^{p-1}-1)\frac{B_{2k+p-1}}{2k+p-1} + (g^{2k}-1)\left(\frac{B_{2k+p-1}}{2k+p-1} - \frac{B_{2k}}{2k}\right),$$

and since the numerator of $g^{2k}(g^{p-1}-1)\dfrac{B_{2k+p-1}}{2k+p-1}$ is divisible by p (use **10** and **12**) and $g^{2k}-1$ is not divisible by p ($2k$ is not divisible by $p-1$), we see that the numerator of $\left(\dfrac{B_{2k+p-1}}{2k+p-1} - \dfrac{B_{2k}}{2k}\right)$ is divisible by p. Now one may obtain Kummer's congruence simply by induction.

18. Suppose that there are only finitely many irregular primes: $p_1, \dots, p_k$. Choose an integer n large enough to have $\left|\dfrac{B_{2m}}{2m}\right| > 1$ ($m = n(p_1-1)\cdots(p_k-1)$). It is clear that the denominator of $\dfrac{B_{2m}}{2m}$ is divisible by p_i for all $i = 1, \dots, k$ (use **12** and **16**), so its numerator is equal to ± 1 (by our hypothesis, if it is divisible by a prime p, then p is one of p_i's). This contradicts $\left|\dfrac{B_{2m}}{2m}\right| > 1$.

19. (By I. Good (see [Go]); another proof of the main identity you can find in [Mac])[1]

Denote this constant term by $C(a_1, \dots, a_k)$. Let us show that $C(a_1, \dots, a_k) = C(a_1-1, a_2, \dots, a_k) + \dots + C(a_1, \cdots, a_k-1)$ (there are obvious initial conditions $C(a_1, \dots, a_{k-1}, 0) = C(a_1, \dots, a_{k-1})$ and $C(0) = 1$). Since multinomial coefficients satisfy the same recurrence relation and initial condition, the Dyson's conjecture follows. The proof is very simple: consider the polynomial $f(x) = \sum\limits_{j=1}^{n} \prod\limits_{i \neq j} \dfrac{x_i - x}{x_i - x_j}$. Its degree is $n-1$ and $f(x_1) = \dots = f(x_n) = 1$, so $f(x) \equiv 1$. Thus

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

Multiply $\prod\limits_{1 \leqslant i \neq j \leqslant n} \left(1 - \dfrac{x_j}{x_i}\right)^{a_j}$ by this equality to obtain the above recurrence relation.

20. It is a simple exercise on linear algebra. For any subspace let us write out all its (ordered) linear bases. To calculate the number of subspaces, one needs to find out how many bases we have written out and how many bases span the same subspace. The number of (ordered) sets of k linearly independent vectors in n-dimensional space over $\mathbb{F}_q$ can be easily calculated as soon as it is known that this n-dimensional space consists of q^n points (it is obvious: this space is isomorphic to the space of n-tuples $(a_1, \dots, a_n)$ with $a_i \in \mathbb{F}_q$): you have $q^n - 1$ opportunities to choose

[1] You can find the following proof in [GKP] as well!!!

the first vector (any non-zero vector), q^n-q opportunities to choose the second vector (any not from the subspace spanned by the first vector), q^n-q^2 opportunities to choose the third vector (any not from the subspace spanned by the first two vectors) etc. Therefore this number equals $(q^n-1)\cdots(q^n-q^{k-1})=q^{k(k-1)/2}\dfrac{n!_q}{(n-k)!_q}(q-1)^k$. Proceeding like that, we see that the number of bases that span the same subspace is $q^{k(k-1)/2}k!_q(q-1)^k$. Hence the number of subspaces is

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

21. Denote by $y^{(i)}_{2n+1}$ the sum $\sum\limits_{k\equiv i \pmod{p-1}}\binom{2n+1}{k}$, $i=0,1,\ldots,p-2$. Let us prove that these $p-1$ sequences have period modulo p. As we have $y^{(i)}_{2n+1}=y^{(i)}_{2n-1}+2y^{(i-1)}_{2n-1}+y^{(i-2)}_{2n-1}$ (it is obvious), it is enough to prove that $y^{(i)}_0\equiv y^{(i)}_p \pmod p$ for all $0<i<p-1$. And it is obvious:

$$y^{(0)}_0=1\equiv 1+p=\binom{p}{0}+\binom{p}{p-1}=y^{(0)}_p,$$

$$y^{(1)}_0=1\equiv p+1=\binom{p}{1}+\binom{p}{p}=y^{(1)}_p,$$

$$y^{(i)}_0=0\equiv\binom{p}{i}=y^{(i)}_p, \text{for } i=2,3,\ldots,p-2.$$

Let us notice that $y^{(i)}_{2n+1}=\binom{2n+1}{i}$ for $i=0,1,\ldots,p-2$ whenever $2n+1\leqslant p-2$, in particular, $y^{(0)}_{2n+1}=1$ for such n, hence $y^{(0)}_{2n+1}\equiv 1 \pmod p$ for all n. But $y^{(0)}_{2n+1}=1+\sum\limits_{k>0}\binom{2n+1}{k(p-1)}$, which concludes the proof.

(This solution involves power sums.)

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

proceed according to **11** to obtain

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

which is just what we need.

22. Hint: let $B(x)=\dfrac{t}{e^t-1}+\dfrac{t}{2}$. Prove the that $B(x)$ satisfies the following differential equation: $B^2(x)-B(x)+xB'(x)=\dfrac{x^2}{4}$ and deduce the recurrence relation from this equation.

23. All solutions are very straightforward. I prefer the following solution submitted by E. Ferens–Sorotskij, O. Styrt and O. Evtifeeva.

It is clear that $f(m,n)=f(n,m)$ and $f(-m,-n)=f(m,n)$. As $f(m,n)+f(m,-n)=\sum\limits_{0<2j<2k}\dfrac{1}{m^{2j}n^{2k-2j}}$ (the summands, containing n^{2j+1} for some j, cancel, the ones containing n^{2j} for some j, double), we need to prove that

$$\begin{aligned}f(m,n)-f(m,m+n)-f(m+n,n)=f(m,n)+f(m,-n)\Leftrightarrow\\ f(m+n,n)+f(m,m+n)+f(m,-n)=0\Leftrightarrow\\ f(m+n,n)+f(-m,-m-n)+f(-n,m)=0.\end{aligned}$$

Let us prove that for all a,b,c such that $abc\neq 0$ and $a+b+c=0$ holds $f(a,-b)+f(b,-c)+f(c,-a)=0$. (And then substitute a by $m+n$, b by $-n$, c by $-m$.) Let us perform some arithmetic transformations with the formula for $f(m,n)\,(m\neq n)$:

$$\begin{aligned}(n-m)f(m,n)&=\frac{1}{mn^{2k-2}}-\frac{1}{n^{2k-1}}+\\ &\frac{1}{m^{2k-1}}-\frac{1}{m^{2k-2}n}+\frac12\sum_{j=2}^{2k-2}\frac{1}{m^jn^{2k-j-1}}-\frac12\sum_{j=2}^{2k-2}\frac{1}{m^{j-1}n^{2k-j}}=\\ &\frac{1}{2mn^{2k-2}}-\frac{1}{2m^{2k-2}n}+\frac{1}{m^{2k-1}}-\frac{1}{n^{2k-1}},\end{aligned}$$

so

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

One may easily complete the proof:

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

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

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

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

24. Adding up the equalities of the previous problem for all nonnegative integers m,n. Let us notice that

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

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

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

therefore

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

so

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

Use the recurrence relation from **22** to obtain the classical result

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

Remark. One may deduce from this formula the inequality which we used in **18**.

25. Here you see some explanations.

- (This explanation leads to some very strange consequences.)

$$\begin{aligned}&\sum_{k\geqslant 0}\frac{B_k}{k!}t^k=\frac{t}{e^t-1}=-t\cdot\frac{1}{1-e^t}=-t\cdot(1+e^t+e^{2t}+\dots)=\\&-t\cdot\left(1+\sum_{n\geqslant 0}\frac{t^n}{n!}\sum_{k\geqslant 1}k^n\right)=-t-\sum_{n\geqslant 1}\frac{t^n}{n!}\left(n\sum_{k\geqslant 1}k^{n-1}\right).\end{aligned}$$

Let us examine the t^k's coefficients in both sides:

at t^n $(n > 1)$: $-n\sum_{k\geqslant 1} k^{n-1} = B_n$, so $\zeta(1-n) = -\dfrac{B_n}{n}$;
at t^1: $-\sum_{k\geqslant 1} 1 - 1 = -\dfrac{1}{2}$, so $\zeta(0) = -\dfrac{1}{2}$
(at t^0: $1 = 0$, so...).

- (This explanation was suggested by A. Entin and D. Faifman.) Define Bernoulli polynomials $B_n(x)$ as follows: $B_n(x) = nP_{n-1}(x) + B_n$. Then $P_{n-1}(x) = \dfrac{B_n(x) - B_n}{n}$,

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

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

(Defining Bernoulli polynomials with different constant terms, we can obtain any answer we want. I suppose that A. Entin and D. Faifman preferred these polynomials becaused they managed to use their Fourier expansions in **24**...)

- (The corresponding method of summation is attributed to Abel.)
It is easy to check the following equalities (which involve only formal power series):

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

This means that

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

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

so $1 + 2 + \dots = -\dfrac{1}{12}$, $1^2 + 2^2 + \dots = 0$.
Exercise. (Warning: it is not easy.) Proceed this explanation.

26. This text in fact contains solutions for most of the problems on numerators and denominators of Bernoulli numbers. Unfortunately, nobody found it during the conference. Compare this solution with the one in [Ko] (first you need to read the chapter on p-adic analysis there).

Let us denote by σ_{2m} an integer such that all numbers $\dfrac{1}{2m+1}B_k p^{\sigma_{2m}}$ are p-integer $(0 \leqslant k \leqslant 2m-1)$. Then

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

. Let r be large enough, for example, $r > \max(\sigma_{2m} + 2m + N, \sigma_{2n} + 2n + N)$. Consider an integer a, which is not divisible by p. For $i = 1, \dots, p^r - 1$ denote by $b_i(r)$ the remainder of ia modulo p^r: $ia = b_i(r) + p^r q_i(r)$, $0 < b_i(r) < p^r$. Then

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

Adding these congruences for $i = 1, \dots, p^r - 1$ we obtain

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

and rewrite it as follows:

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

It follows from $(*)$ that

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

so

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

We have $p^{2m} > 2m$ (it is clear), so

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

Denote by Σ_{2m} the part of the sum in the right-hand side containing those $b_i(r)$ which are not divisible by p. Let us deal with the remaining summands: $\sum\limits_{i=1}^{p^{r-1}-1} b_{pi}(r)^{2m-1}q_{pi}(r)$. Let $c_i = \dfrac{b_{pi}(r)}{p}$ $(i=1,\dots,p^{r-1}-1)$. It is clear that $c_i = b_i(r-1)$, $q_{pi}(r) = q_i(r-1)$. Rewrite (**) with $r := r-1$:

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

It is obvious that

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

Therefore

$$p^{2m-1}(a^{2m}-1)\frac{B_{2m}}{2m} \equiv \sum_{i=1}^{p^{r-1}-1} b_{pi}(r)^{2m-1}q_{pi}(r) \pmod{p^{r-\sigma_{2m}-2m}}$$

(use that $2m-1 \geqslant 1$). Substitute this into (**) to obtain

$$(a^{2m}-1)\frac{B_{2m}}{2m} \equiv \Sigma_{2m} + \sum_{i=1}^{p^{r-1}-1} b_{pi}(r)^{2m-1}q_{pi}(r) \equiv \Sigma_{2m} + p^{2m-1}(a^{2m}-1)\frac{B_{2m}}{2m} \pmod{p^{r-\sigma_{2m}-2m}},$$

and rewrite this as follows:

$$(a^{2m}-1)(1-p^{2m-1})\frac{B_{2m}}{2m} \equiv \Sigma_{2m} \pmod{p^{r-\sigma_{2m}-2m}},$$

therefore (for r large enough)

$$(a^{2m}-1)(1-p^{2m-1})\frac{B_{2m}}{2m} \equiv \Sigma_{2m} \pmod{p^{N+1}}$$

and

$$(a^{2n}-1)(1-p^{2n-1})\frac{B_{2n}}{2n} \equiv \Sigma_{2n} \pmod{p^{N+1}}.$$

Since $2m-2n$ is divisible $p^{N+1}-p^N = \varphi(p^{N+1})$, and the numbers $b_i(r)$ (which occur in Σ_{2m} and Σ_{2n}) are not divisible by p, it follows that (use Euler's theorem)

$$(a^{2n}-1)(1-p^{2n-1})\frac{B_{2n}}{2n} \equiv \Sigma_{2n} \equiv \Sigma_{2m} \equiv (a^{2m}-1)(1-p^{2m-1})\frac{B_{2m}}{2m} \pmod{p^{N+1}},$$

so (recall that a is not divisible by p as well)

$$(a^{2n}-1)\left((1-p^{2n-1})\frac{B_{2n}}{2n} - (1-p^{2m-1})\frac{B_{2m}}{2m}\right) \equiv 0 \pmod{p^{N+1}}.$$

Choose a such that $a^{2n}-1$ is not divisible by p to complete the proof (it is possible because $2n$ is not divisible by $p-1$).

References

[BSh] Z. I. Borevich, I. R. Shafarevich. Number theory. (In Russian: Moscow, Nauka Publishers, 1985.)

[Ge] A. O. Gel'fond. Calculus of finite differences. (In Russian: Moscow-Leningrad, GITTL, 1952.)

[Go] I. J. Good. Short proof of a conjecture of Dyson. J. Math. Phys., 11, 1970.

[GKP] R. L. Graham, D. E. Knuth, O. Patashnik. Concrete mathematics. Addison–Wesley, 1998. (In Russian: Moscow, Mir Publishers, 1998.)

[Ko] N.Koblitz. P-adic numbers, p-adic analysis and zeta-functions. Springer–Verlag, 1977. (In Russian: Moscow, Mir Publishers, 1982.)

[Mac] I. G. Macdonald. Symmetric functions and Hall polynomials. Clarendon Press, Oxford, 1979. (In Russian: Moscow, Mir Publishers, 1985.)

[MS] J. W. Milnor, J. D. Stasheff. Characteristic classes. (In Russian: Moscow, Mir Publishers, 1979.)

[Pr] V. V. Prasolov. Problems and theorems of linear algebra. (In Russian: Moscow, Nauka Publishers, 1996.)