(L9) (May 1, 2020), Let us continue with the proof of claim 2, it is May 11 but nevermind. Recall that $S_k(n) = 1^k + 2^k + \cdots + (n-1)^k$ where $k, n \in \mathbb{N}$. We prove that if p is a prime, $k \in \mathbb{N}$ and $p-1$ does not divide k, then

$$S_k(p) = \sum_{j=1}^{p-1} j^k \equiv 0 \pmod{p} \quad (1).$$

Recall the following algebraic result.

Proposition If $F = (F, 0_F, 1_F, +, \cdot)$ is a field, $F^\times = (F^\times, 1_F, \cdot)$ is the multiplicative group of $\neq 0_F$ elements in F ($F^\times = F \setminus \{0_F\}$), and $C \subset F^\times$ is a finite subgroup, then C is cyclic, i.e. $C = \{q^n \mid n = 1, 2, \ldots, |C|\}$ is generated by a single element q.

We leave ~~the~~ proof to algebraists and prove (1). Let $q \in \mathbb{Z}_p^\times$ be a generator of the group $\mathbb{Z}_p^\times = (\mathbb{Z}_p^\times, 1_{\mathbb{Z}_p}, \cdot)$. ~~Since $q^{p-1} = q^{|\mathbb{Z}_p^\times|} \equiv 1 \pmod{p}$~~. We have

$$q^k S_k(p) = \sum_{j=1}^{p-1} (qj)^k \underset{\bmod p}{\equiv} \sum_{j=1}^{p-1} j^k = S_k(p)$$

because if j runs in $\mathbb{Z}_p^\times$ then so does qj. Also $q^k \not\equiv 1 \pmod{p}$, because $q^{p-1} \equiv 1$ and $\{q^j \mid j = 1, 2, \ldots, p-1\} = \mathbb{Z}_p^\times$. Thus

$(q^2-1)S_q(p) \equiv 0 \pmod p \rightsquigarrow S_q(p) \equiv 0 \pmod p$. (2)
$\underbrace{(q^2-1)}_{\not\equiv 0}$

Claim 3 If $q \in \mathbb{N}$ is a prime p and q is even then

$$|B_q - p^{-1} S_q(p)|_p \leq 1.$$

Proof. If $m \in \mathbb{N}$ and $0 \leq j \leq p^{m+1}$ then j has a unique expression in the form $j = up^m + v$, $0 \leq u < p$ and $0 \leq v < p^m$.

Then $S_q(p^{m+1}) = \sum_{j=1,0}^{p^{m+1}} j^q = \sum_{u=0}^{p-1} \sum_{v=0}^{p^m-1} (up^m+v)^q \equiv$

$\equiv p \sum_{v=0}^{p^m-1} v^q + qp^m \sum_{u=0}^{p-1} u \sum_{v=0}^{p^m-1} v^{q-1} \pmod{p^{2m}}$, by the binomial expansion $(v+up^m)^q \equiv v^q + \binom{q}{1} v^{q-1} up^m + \underbrace{\ldots}_{\equiv 0} \pmod{p^{2m}}$.

Here $\cdot = S_q(p^m)$. Also, $2\sum_{u=0}^{p-1} u = p(p-1) \equiv 0 \pmod p$.

Thus $\boxed{S_q(p^{m+1}) \equiv p S_q(p^m) \pmod{p^{m+1}}}$ (for $p>2$ we have $\sum_{u=0}^{p-1} u = p \cdot \frac{p-1}{2} \equiv 0 \pmod p$, for $p=2$ we use that in q is even). On dividing by p^{m+1} we can write this congruence as

$$\boxed{|p^{-m-1} S_q(p^{m+1}) - p^{-m} S_q(p^m)|_p \leq 1.}$$

Since $|\cdots|_p$ satisfies the ultrametric inequality, we have that

$\forall$ integers $l, m > 0$: $|p^{-l} S_k(p^l) - p^{-m} S_k(p^m)|_p \leq 1$. We set $m = 1$ and send $l \to \infty$. Then $p^{-l} \to 0$ in the p-adic sense and by Claim 1, $|B_k - p^{-1} S_k(p)|_p \leq 1$. $\boxtimes$

Proof. (of the C.-von S. thm.) By Claim 2 and Claim 3:

$$|B_k + p^{-1}|_p \leq 1 \;\dots\; (p-1) \mid k$$

$$|B_k|_p \leq 1 \;\dots\; (p-1) \nmid k.$$

Let, for even $k \in \mathbb{N}$,

$$W_k := B_k + \sum_{\substack{q \text{ prime} \\ q-1 \mid k}} \frac{1}{q}.$$

If p is any prime then

$$\underset{\in \mathbb{Q}}{W_k} = \begin{cases} B_k + p^{-1} + \sum_{\substack{q, \text{-"-} \\ q \neq p}} q^{-1} & \dots\; p \text{ belongs to the } q\text{'s} \\ B_k + \sum_{q, \text{-"-}} q^{-1} & \dots \text{ else.} \end{cases}$$

Since for both sums $\sum_{\dots} q^{-1}$ we have $|\sum_{\dots} q^{-1}|_p \leq 1$, together with we get that $|W_k|_p \leq 1$ for every prime number p, (recall that $|a|_p \leq 1$, $|b|_p \leq 1 \Rightarrow |a+b|_p \leq 1$). But this means that $W_k \in \mathbb{Z}$ (writing $W_k = \frac{a}{b}$ with coprime $a, b \in \mathbb{Z}$ we see that no p divides b). (*) $\boxtimes$

Finally, we state and then prove — by means of the theorem on residues — the generalization of the formula

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

(*) The proof of the von S.-C. thm. is due to Witt, it is taken from Cassels' book Local Fields

Theorem Let $k \in \mathbb{N}$. Then

$$\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{(-1)^{k+1}\, 2^{2k-1}}{(2k)!} B_{2k} \pi^{2k}$$

where B_{2k} are, of course, the Bernoulli numbers.

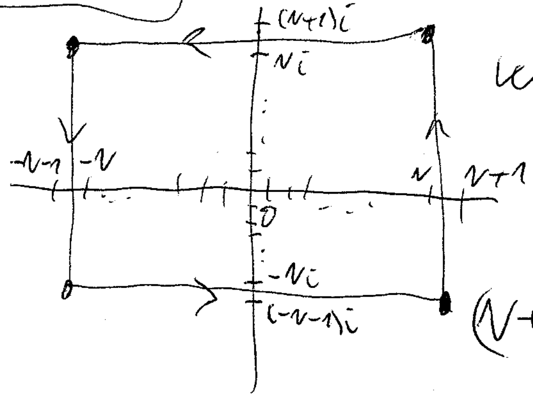
Proof. We take the function $H(z) = \dfrac{2\pi i}{e^{2\pi i z} - 1}$. We claim that $H : \mathbb{C} \setminus \mathbb{Z} \to \mathbb{C}$ is a meromorphic function with $\operatorname{Res}(H, n) = 1$ for every $n \in \mathbb{Z}$. Indeed, by the properties of the exponential function we have that $e^{2\pi i z} - 1 = 0 \iff z \in \mathbb{Z}$ and, for any $n \in \mathbb{Z}$,

$$\lim_{z \to n} (z-n) H(z) = \lim_{z \to n} \frac{2\pi i (z-n)}{e^{2\pi i z} - 1} =$$

$$= 2\pi i \lim_{z \to n} \frac{z-n}{e^{2\pi i z} - 1} = 2\pi i \lim_{z \to n} \frac{(z-n)'}{(e^{2\pi i z} - 1)'} = \cancel{2\pi i} \lim_{z \to n} \frac{1}{\cancel{2\pi i}\, e^{2\pi i z}}$$

$$= 1.$$

Let $N \in \mathbb{N}$ and Γ_N be the ↺-oriented square where the corners • are $(N + \frac{1}{2})(\pm 1 \pm i)$



$(N + \frac{1}{2})(1 - i)$

For $k \in \mathbb{N}$ let $I_N := \dfrac{1}{2\pi i} \displaystyle\int_{\Gamma_N} H(z) \frac{1}{z^{2k}}\, dz$. By the residue theorem or rather theorem on residues we have:

$$\boxed{I_N = \sum_{n=-N}^{N} \operatorname{Res}\left(H(z)\frac{1}{z^{2k}}, n\right)} = \operatorname{Res}\left(H(z)\frac{1}{z^{2k}}, 0\right) + \boxed{+\, 2\sum_{n=1}^{N} \frac{1}{n^{2k}}},$$

because for $n \in \mathbb{Z}, n \neq 0$, we have that

$$\operatorname{Res}\left(H(z)\frac{1}{z^{2k}}, n\right) = \frac{1}{n^{2k}} \underbrace{\operatorname{Res}(H(z), n)}_{=1} = \frac{1}{n^{2k}}.$$

We claim that if we look at I_N as an $\int$ (actually, $\frac{1}{2\pi i}\int$) then $\boxed{\lim_{N\to\infty} I_N = 0.}$

Exercise: $\exists$ constant $C>0$ s.t. $z \in \Gamma_N \Rightarrow$ $\Rightarrow |H(z)| < C$, independently of N.

Thus, since the perimeter of Γ_N is $8N+4$, we have that

$$|I_N| = \frac{1}{2\pi}\left|\int_{\Gamma_N} H(z)\frac{1}{z^{2k}}\,dz\right| \leq \frac{1}{2\pi}\cdot \underset{8N+4}{\underset{\shortparallel}{|\Gamma_N|}} \cdot \max_{z\in\Gamma_N}\left|\frac{H(z)}{z^{2k}}\right| =$$

$$= O\left(\frac{1}{N^{2k-1}}\right) \to 0 \text{ for } N\to\infty.$$

Thus we have derived the identity

$$\boxed{\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = -\frac{1}{2}\operatorname{Res}\left(H(z)\frac{1}{z^{2k}}, 0\right).}$$

Now

$$H(z) = \frac{2\pi i}{e^{2\pi i z}-1} \underset{\uparrow}{=} \sum_{\ell=0}^{\infty} \frac{B_\ell (2\pi i)^\ell z^{\ell-1}}{\ell!}$$

the definition of the B-#s

and the coeff. of $\frac{1}{z}$ in the (Laurent) expansion of $H(z)\frac{1}{z^{2k}}$ around 0 is ($\ell = 2k$)

$$\operatorname{Res}\left(H(z)\frac{1}{z^{2k}}, 0\right) = \frac{1}{(2k)!} B_{2k} (2\pi)^{2k} (-1)^k.$$

Therefore

$$\sum_{n=1}^{\infty} \frac{1}{n^{2q}} = -\frac{1}{2} \mathrm{Res}\left(H(z)\frac{1}{z^{2q}} \Big| 0\right)$$

$$= -\frac{1}{2} \frac{(-1)^{q} (2\pi)^{2q} B_{2q}}{(2q)!}$$

$$= \boxed{\frac{(-1)^{q+1} 2^{2q-1}}{(2q)!} \pi^{2q} B_{2q}}$$

$\square$

For example, $(q=5)$ $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^{10}} = \frac{(-1)^{6}\, 2^{\cancel{8}9}}{10!} \pi^{10} \underbrace{B_{10}}_{=5/66} =$

$$= \boxed{\frac{5 \cdot 512}{66 \cdot 10!} \pi^{10}}$$