NT Berman Unity

February 24, 2025

Problem. *Let p be an odd prime and x be an integer such that $p \mid x^3 - 1)$ but $p \nmid x - 1$. Prove that*

$$p \mid (p-1)!\left(x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots - \frac{x^{p-1}}{p-1}\right)$$

John Berman

Solution. *First of all we note that since $\mathbb{Z}/p\mathbb{Z}$ is a field therefore we can deal with rational numbers just fine. Hence our initial condition is equivalent to*

$$\left(x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots - \frac{x^{p-1}}{p-1}\right) \equiv 0 \mod p$$

which is equivalent to

$$\sum_{i=1}^{p-1} \frac{(-1)^i x^i}{i} \equiv 0 \mod p$$

Let $P(x)$ be the polynomial $\sum_{i=1}^{p-1} \dfrac{(-1)^i x^i}{i}$. Since $p|(x^3-1)$ but $p \nmid x-1$ this implies $p|(x^2+x+1)$. Now note that $x^{3n+c} \equiv x^c \mod p$. Note that order of x with respect to p is 3, hence $3|p-1$. As p is an odd prime,we get $6|p-1$. Hence $p = 6m+1$ for some natural m. Hence

$$P(x) \equiv \left(\left(\sum_{i=0}^{i=2m-1} \frac{(-1)^{3i+3}}{3i+3}\right) + \left(\sum_{i=0}^{i=2m-1} \frac{(-1)^{3i+1}}{3i+1}\right) x + \left(\sum_{i=0}^{i=2m-1} \frac{(-1)^{3i-2}}{3i+2}\right) x^2\right) \mod p$$

Let $A = \left(\sum_{i=0}^{i=2m-1} \dfrac{(-1)^{3i+3}}{3i+3}\right), B = \left(\sum_{i=0}^{i=2m-1} \dfrac{(-1)^{3i+1}}{3i+1}\right), C = \left(\sum_{i=0}^{i=2m-1} \dfrac{(-1)^{3i-2}}{3i+2}\right)$
.

We will prove that $A \equiv B \equiv C \mod p$. which will prove $P(x) \equiv 0 \mod p$ which will prove our original proposition . We will divide our proof into 2 parts , first we prove $A \equiv B \mod p$, in second part we will prove $A \equiv C \mod p$.

Proof that $A \equiv B \mod p \rightarrow$

Note that as $1/a \equiv -1/(p-a) \mod p$, we get

$$\left(\sum_{i=0}^{i=2m-1} \frac{(-1)^{3i+3}}{(3i+3)}\right) \equiv \left(\sum_{i=0}^{i=2m-1} \frac{(-1)^{3i+2}}{6m+1-(3i+3)}\right) \mod p$$

which implies

$$A \equiv \left(\sum_{i=0}^{i=2m-1} \frac{(-1)^{6m-2-3i}}{6m-2-3i} \right) \mod p$$

as we know $\sum_{i=a}^{i=b} f(i) = \sum_{i=a}^{i=b} f(a+b-i)$*, we get*

$$A \equiv \left(\sum_{i=0}^{i=2m-1} \frac{(-1)^{3i+1}}{3i+1} \right) \equiv B \mod p$$

Proof that $A \equiv C \mod p \rightarrow$

We will prove that $3A \equiv A + B + C \mod p$*, which will automatically prove* $A \equiv C \mod p$*. First of all note that* $A + B + C \equiv \sum_{i=1}^{6m} (\frac{(-1)^i}{i}) \mod p$*. As* $\sum_{i=1}^{6m} (\frac{1}{i}) \equiv 0 \mod p$ *(as each inverse is mapped bijectively to a non - zero element, therefore it is just sum of all non zero elements, sum of whose is 0). We get* $\sum_{i=1}^{6m} (\frac{(-1)^i}{i}) \equiv 2 \sum_{i=1}^{3m} (\frac{1}{2i}) \mod p$ *which implies*

$$A + B + C \equiv \sum_{i=1}^{3m} \frac{1}{i} \mod p$$

Let $D = \sum_{i=1}^{m} \left(\frac{1}{2i-1} + \frac{1}{4m+2i} \right)$*. We claim that* $D \equiv 0 \mod p$*. To prove that , first notice (using* $1/a \equiv -1/(p-a) \mod p$ *and* $\sum_{i=a}^{i=b} f(i) = \sum_{i=a}^{i=b} f(a+b-i)$ *respectively),*

$\sum_{i=1}^{m} \left(\frac{1}{4m+2i} \right) \equiv \sum_{i=1}^{m} \left(\frac{-1}{6m+1-(4m+2i)} \right) \equiv \sum_{i=1}^{m} \left(\frac{-1}{6m+1-(4m+2(m+1-i))} \right) \mod p$*, this implies* $\sum_{i=1}^{m} \left(\frac{1}{4m+2i} \right) \equiv \sum_{i=1}^{m} \left(\frac{-1}{2i-1} \right) \mod p$*. Hence* $D \equiv 0 \mod p$.

Now note that $3A \equiv \left(\sum_{i=0}^{i=2m-1} \dfrac{3 * (-1)^{3i+3}}{3i+3} \right) \equiv \sum_{i=1}^{i=2m} \dfrac{(-1)^i}{i} \mod p$ *. Now* $\sum_{i=1}^{i=2m} \dfrac{(-1)^i}{i} \equiv 2D + \sum_{i=1}^{i=2m} \dfrac{(-1)^i}{i} \mod p$*. This implies*

$\sum_{i=1}^{i=2m} \dfrac{(-1)^i}{i} \equiv \sum_{i=1}^{m} \left(\frac{2}{2i-1} + \frac{1}{2m+i} \right) + \sum_{i=1}^{i=2m} \dfrac{(-1)^i}{i} \equiv \sum_{i=1}^{3m} \frac{1}{i} \mod p$*,*

Hence $3A \equiv A + B + C \mod p$ *, as* $A \equiv B \mod p$*, we get* $A \equiv C \mod p$*. Since* $A \equiv B \equiv C \mod p$*, we have* $P(x) \equiv A(1+x+x^2) \mod p$ *,hence* $P(x) \equiv 0 \mod p$ *which proves our original proposition*

Exploration. *Complex numbers!, altho not strictly needed gives a direction to the proof, since each cube root of unity is independent i knew we had to prove* $A \equiv B \equiv C \mod p$*. First part was trivial, tried and experimented many algebraic manipulation, looking into values of sum of inverses of 2 residue 3 using computer and many more things. Finally tried the value of the their sum since the sum looks somehwat pretty, it's clear you've to choose 0 residue to make this even somewhat solvable. Post that it was trivial . Main idea was to prove* $A \equiv C \mod p$ *indirectly using* $3A \equiv A + B + C \mod p$ *.Overall a medium-hard problem (for me) since main idea was clear*

Tags. *Number Theory , roots of unity , John Berman (for searching using authors) , harmonic sums*