American Mathematical Monthly
Problem 11407 by Erwin Just

Let p be a prime such that $p > 3$. Let R be a ring (not necessarily commutative and not necessarily having a multiplicative identity) such that

$$\sum_{i=1}^{p} x^{2i-1} = 0 \tag{1}$$

holds for every $x \in R$. Prove that $R = 0$, where 0 means the trivial ring (i. e. the ring consisting of one element only).

Solution by Darij Grinberg.
Every $x \in R$ satisfies

$$\begin{aligned} x - x^{2p+1} &= x^{2\cdot 1-1} - x^{2(p+1)-1} = \sum_{i=1}^{p} x^{2i-1} - \sum_{i=2}^{p+1} x^{2i-1} \\ &= \sum_{i=1}^{p} x^{2i-1} - \sum_{i=1}^{p} \underbrace{x^{2(i+1)-1}}_{=x^2 x^{2i-1}} \qquad \text{(here we substituted } i+1 \text{ for } i \text{ in the second sum)} \\ &= \underbrace{\sum_{i=1}^{p} x^{2i-1}}_{=0 \text{ by (1)}} - x^2 \underbrace{\sum_{i=1}^{p} x^{2i-1}}_{=0 \text{ by (1)}} = 0 - 0 = 0. \end{aligned}$$

Thus,

$$x = x^{2p+1} \tag{2}$$

for every $x \in R$.

Now, let $y \in R$. Then, (2) (applied to $x = y$) yields $y = y^{2p+1}$, so that

$$\left(y^{2p}\right)^2 = y^{4p} = y^{(2p-1)+(2p+1)} = y^{2p-1} y^{2p+1} = y^{2p-1} y = y^{2p}.$$

Thus, y^{2p} is idempotent; hence,

$$\left(y^{2p}\right)^k = y^{2p} \tag{3}$$

for every integer $k \geq 1$. Applying (1) to $x = y^{2p}$ yields $\sum_{i=1}^{p} \left(y^{2p}\right)^{2i-1} = 0$; thus,

$$0 = \sum_{i=1}^{p} \underbrace{\left(y^{2p}\right)^{2i-1}}_{=y^{2p} \text{ by (3)}} = \sum_{i=1}^{p} y^{2p} = p y^{2p}. \tag{4}$$

On the other hand, applying (2) to $x = 2y^{2p}$ yields $2y^{2p} = \left(2y^{2p}\right)^{2p+1}$; thus,

$$2y^{2p} = \left(2y^{2p}\right)^{2p+1} = 2^{2p+1} \underbrace{\left(y^{2p}\right)^{2p+1}}_{=y^{2p} \text{ by (3)}} = 2^{2p+1} y^{2p},$$

so that

$$0 = 2^{2p+1} y^{2p} - 2y^{2p} = \left(2^{2p+1} - 2\right) y^{2p}. \tag{5}$$

But $p > 3$ yields $p > 4$ (since p is a prime, and 4 is not a prime), and thus $4^{p-1} \equiv 1 \bmod p$ (by Fermat's Little Theorem). Besides, p is a prime, so that every positive integer less than p is invertible modulo p. Hence, 2 and 3 are invertible modulo p (since $2 < 3 < p$). Now,

$$2^{2p+1}-2 = 2^{3+2(p-1)}-2 = 2^3 \cdot 2^{2(p-1)}-2 = 2^3 \cdot \left(2^2\right)^{p-1}-2 = 2^3 \cdot \underbrace{4^{p-1}}_{\equiv 1 \bmod p} -2 \equiv 2^3 \cdot 1 - 2 = 6 = 2 \cdot 3 \bmod p.$$

Thus, $2^{2p+1} - 2$ is invertible modulo p (since $2 \cdot 3$ is invertible modulo p, since 2 and 3 are invertible modulo p). In other words, $2^{2p+1} - 2$ is coprime to p. Hence, by Bezout's theorem, there exist integers a and b such that $a\left(2^{2p+1} - 2\right) + bp = 1$. Hence,

$$y^{2p} = 1y^{2p} = \left(a\left(2^{2p+1} - 2\right) + bp\right) y^{2p} = a \underbrace{\left(2^{2p+1} - 2\right) y^{2p}}_{=0 \text{ by (5)}} + b \underbrace{py^{2p}}_{=0 \text{ by (4)}} = 0 + 0 = 0.$$

Applying (2) to $x = y$ yields $y = y^{2p+1}$, so that $y = y^{2p}y = 0y = 0$.

Thus, we have proven that $y = 0$ for every $y \in R$. Hence, $R = 0$, qed.