Problem Of The Month

April 2022

Problem:

For a polynomial $Q$ with integer coefficient and prime $p$, we say that $Q$ excludes $p$ if there is no integer $n$ for which $p \mid Q(n)$. Does there exist a polynomial with integer coefficients having no rational roots which excludes exactly one prime?

Solution: Answer: Yes, for example $Q(x) = (2x^3 + 1)(x^2 - x + 1)$ satisfies all conditions. Clearly $Q(x)$ has no rational roots. We will show that the only prime excluded by $Q(x)$ is $p = 2$.

Observation 1: For any prime $p$ satisfying $p \equiv 1 \pmod{3}$ there exists an integer $n$ such that $n^2 - n + 1 \equiv 0 \pmod{p}$.

Proof. Let $\omega$ be a primitive root modulo $p$ and $n = -\omega^{(p-1)/3}$. Then $n^3 \equiv -1 \pmod{p}$ and $n \not\equiv -1 \pmod{p}$. Now since $n^3 + 1 = (n+1)(n^2 - n + 1)$ we get $n^2 - n + 1 \equiv 0 \pmod{p}$.

Observation 2: For any odd prime $p$ satisfying $p \equiv 2 \pmod{3}$ there exists an integer $n$ such that $2n^3 + 1 \equiv 0 \pmod{p}$.

Proof. Let $a$ be an integer satisfying $2a + 1 \equiv 0 \pmod{p}$. Since $3 \mid p - 2$ we get $3 \mid 2p - 1$. Then for the integer $n = a^{(2p-1)/3}$ by Fermat’s little theorem we have $n^3 \equiv a^{2p-1} \equiv a \pmod{p}$. Therefore, $2n^3 + 1 \equiv 2a + 1 \equiv 0 \pmod{p}$.

$Q(x)$ does not exclude $p = 3$ since $3 \mid Q(2)$. By Observation 1 any prime $p \equiv 1 \pmod{3}$ is not excluded by $Q(x)$. By Observation 2 any odd prime $p \equiv 2 \pmod{3}$ is not excluded by $Q(x)$. Since both $2n^3 + 1$ and $n^2 - n + 1$ are always odd numbers $p = 2$ is excluded by $Q(x)$. We are done.