SOLUTION TO PUTNAM 2012 B6 USING ALGEBRAIC NUMBER THEORY

DAVID CORWIN

We present a quick proof of problem B6 from the 2012 Putnam Exam using algebraic number theory. This is the solution I discovered during the exam, and I couldn't find anyone else with the same solution, so I decided to write it up.

Problem (Putnam Exam 2012 B6)**.** *Let p be an odd prime number such that $p \equiv 2 \pmod 3$. Define a permutation π of the residue classes modulo p by $\pi(x) \equiv x^3 \pmod p$. Show that π is an even permutation if and only if $p \equiv 3 \pmod 4$.*

Since taking the third power fixes 0, the sign of π is determined by the sign of its action on the nonzero residues modulo p. As $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, π is the same as multiplication by 3 on $\mathbb{Z}/(p-1)$.

This permutation is the same as the action of Frob_3 on $\mu_3 = \{w_1, \cdots, w_{p-1}\}$, the set roots of $f(x) = x^{p-1} - 1$. Its action on the roots of this polynomial is even iff it acts trivially on the square root of the discriminant of this polynomial, which is

$$d := \prod_{i<j} (w_i - w_j).$$

This, in turn, is true iff 3 splits in the extension $\mathbb{Q}(d)$.

It is not hard to see that

$$(-1)^{\binom{p-1}{2}} d^2 = \prod_{i,j=1}^{p-1} (w_i - w_j) = \prod_{i=1}^{p-1} f'(w_i) = -(p-1)^{p-1},$$

which is a square times -1.

Therefore, if $p \equiv 3 \pmod 4$, then $\binom{p-1}{2}$ is odd, so adjoining the square root of the discriminant gives $\mathbb{Q}$, so 3 splits tautologically, and the permutation is even. If $p \equiv 1 \pmod 4$, then the extension is $\mathbb{Q}(i)$, in which 3 does not split, so the permutation is odd.