ELMO 2019 P5

March 28, 2025

Problem. *Let $\mathbb{S}$ be a nonempty set of positive integers such that, for any (not necessarily distinct) integers a and b in $\mathbb{S}$, the number ab + 1 is also in $\mathbb{S}$. Show that the set of primes that do not divide any element of $\mathbb{S}$ is finite.*

Solution. *Let p be a prime which doesnt divide any element in $\mathbb{S}$ but has at least 2 different residues in $\mathbb{S}$. Let Q be the set of all residues of numbers in S modulo p. Then we have $1 < |Q| < p$. Note that if $p < 7$ this can never hold. We will consider all primes ≥ 7. Note that if $1 \in Q$ then for all $a \in Q$, we have $a + 1 \in Q$. This is a contradiction as we will have every number modulo p by repeating this process. Hence $1 \notin Q$.*

Now note that if $a \in Q$ then $a \cdot Q + 1 = Q$ as $a \cdot Q + 1$ has same cardinality as of Q and every element of $a \cdot Q + 1$ is an element of Q. Hence for all $a, b \in Q$, we have $a \cdot Q = Q - 1 = b \cdot Q$.

Now note that $(ab)Q = a(bQ) = a(Q - 1) = aQ - a = Q - a - 1$, similarly $(ab)Q = b(aQ) = b(Q - 1) = bQ - b = Q - b - 1$ hence $Q - a = Q - b$, therefore $\forall c \in Q, c + a - b \in Q$. If we choose distinct a and b we get $c + t(a - b) \in Q$ for all t, note that this implies all residues are in Q which is a contradition. Hence if a prime has at least 2 residues in $\mathbb{S}$, then it has all the residues. Hence all primes which are greater than second smallest element has an element in $\mathbb{S}$ that it divides. QED

Exploration. *let g be a primitive root of prime p, index set Q by powers of g. We are only talking in field $\mathbb{F}_p$ from now on.So $Q = \{g^{a_i} : 0 \leq i < k\}$. Let $d = min(\{a_i - a_{i-1}\} : 0 < i < k)$. Then note that if $x \in Q$ then so is $x \cdot g^d$. Now note that for all $0 \leq i < k$ we have $g^{a_i+d} \in Q$, this implies $a_{i+1} - a_i = d$ for all possible i and $a_{k-1} + d = a_0 + (p - 1)$ so $k \cdot d = p - 1$. Hence set Q is $g^{a_0} \cdot \{1, g^d, g^{2d}, \dots g^{(k-1)d}\}$. Now as $g^{2a_0} + 1 \in \mathbb{Q}$, we get $g^{2a_0} + 1 \equiv g^{a_0+cd} \mod p$ for some $0 \leq c < k$. Post that it's somehow easy to solve you show that -1 is a power of g , so we have $(1 + 1/b) \in S$, so $b + 2 \in S$, this solves the problem Basically the solution , but I used the $a^2 + 1$ and then $ab + 1$ identity repeatedly to rederive many of these identities. The relation is too strong tbh and a few different integers should explore the whole modulo (0 ,1 implies whole modulo is reachable). Now it is not always reachable because the most basic case where $a^2 + 1 \equiv a \mod p$ then we can choose all numbers $a \mod p$ and be done. But 2 seemed sufficient to get all modulos (verified lazily with computer till like* *primes<1000). One can write this solution w/o primitive roots but they help guide the solution and show dark in light if you dont see the trick.*

Tags. *NT , Algebra , ab+1*