Bài toán 1. *Tìm tập hợp S gồm các số nguyên tố sao cho $p \in S$ khi và chỉ khi tồn tại một số nguyên x thỏa mãn:*

$$x^{2010} + x^{2009} + \cdots + 1 \equiv p^{2010} \pmod{p^{2011}}.$$

Độ khó: 5
(ELMO SL 2010/N5)

Lời giải. Đáp số là mọi số nguyên tố có dạng $2011k + 1$, chú ý rằng 2011 cũng là số nguyên tố.

Ta sẽ giải bài toán tổng quát hơn với $x^{q-1} + x^{q-2} + \cdots + 1 \equiv p^{q-1} \pmod{p^q}$. Với p, q là các số nguyên tố lớn hơn 3.

Trước tiên, giả sử $p \in S$, khi đó $\dfrac{x^q - 1}{x - 1} \equiv p^{q-1} \pmod{p^q}$. Suy ra $p \mid \dfrac{x^q - 1}{x - 1}$, nếu $p \mid x - 1$ thì theo định lý LTE ta sẽ thu được $v_p(\dfrac{x^q - 1}{x - 1}) = v_p(x^q - 1) - v_p(x - 1) \leq 1$.

Điều này là mâu thuẫn, vậy nên $x - 1$ không chia hết cho p, suy ra $p \mid x^q - 1$. Vậy $ord_p(x) = q$, hay là $q \mid p - 1$.

Giờ, ta chứng minh với mọi p có dạng $qk+1$ thì đều thuộc S. Thật vậy, ta đã biết trong $\mathbb{F}_p$ có $\phi(q)$ phần tử nhận q làm cấp, vậy nên áp dụng bổ đề Hansel cho đa thức $P(n) = n^q - 1$ thì sẽ tồn tại x đê $p^{q-1} \mid x^q - 1$.

Ta sẽ làm việc trong trường $\mathbb{F}_{p^q}$. Giả sử $x^q - 1 = ap^{q-1}$, lúc này ta có:

$$(x + xp^{q-1})^q - 1 = \sum_{i=0} \binom{q}{i} p^{i(q-1)} x^q - 1 = qp^{q-1}x^q + x^q - 1$$

Hay là

$$(x + xp^{q-1})^q - 1 = p^{q-1}(a + qx^q) = p^{q-1}(a + q(ap^{q-1} + 1)) = p^{q-1}(a + q)$$

Tương tự ta quy nạp được rằng $(x + nxp^{q-1})^q - 1 = p^{q-1}(a + nq)$ với mọi $n \in \mathbb{Z}^+$

Lúc này ta chỉ việc chọn $n = \dfrac{xp^{q-1} - q}{1 - x}$ là xong. Vậy ta kết luận S là tập các số nguyên tố đồng dư 1 mod 2011.

$\square$