Primitive Roots

www.artofproblemsolving.com/community/c3589

by Peter, Megus, ZetaX, TomciO

1 Let n be a positive integer. Show that there are infinitely many primes p such that the smallest positive primitive root of p is greater than n.

---

3 Show that for each odd prime p, there is an integer g such that $1 < g < p$ and g is a primitive root modulo p^n for every positive integer n.

---

4 Let g be a Fibonacci primitive root $\pmod{p}$. i.e. g is a primitive root $\pmod{p}$ satisfying $g^2 \equiv g+1 \pmod{p}$. Prove that - $g-1$ is also a primitive root $\pmod{p}$. - if $p = 4k+3$ then $(g-1)^{2k+3} \equiv g-2 \pmod{p}$, and deduce that $g-2$ is also a primitive root $\pmod{p}$.

---

5 Let p be an odd prime. If $g_1, \cdots, g_{\phi(p-1)}$ are the primitive roots $\pmod{p}$ in the range $1 < g \le p-1$, prove that

$$\sum_{i=1}^{\phi(p-1)} g_i \equiv \mu(p-1) \pmod{p}.$$

---

6 Suppose that m does not have a primitive root. Show that

$$a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{m}$$

for every a relatively prime m.

---

7 Suppose that $p > 3$ is prime. Prove that the products of the primitive roots of p between 1 and $p-1$ is congruent to 1 modulo p.
