Proof of conjectures by Detlefs and Ibrishimova

Robert Israel

April 24, 2019

Take any $r \geq 1$. Note that $\varphi(p^r) = (p-1)p^{r-1}$, where φ is A000010 and p is prime.

Theorem 1 *If p is a member of A003629, i.e. an odd prime for which 2 is not a square, then*

$$2^{\varphi(p^r)/2} \equiv -1 (\bmod p^r)$$

Proof Let t be a primitive root mod p^r. Then $2 \equiv t^k \bmod p^r$ for some k with $1 \leq k < \varphi(p^r)$, and 2 is a square mod p iff 2 is a square mod p^r iff k is even. Since this is not the case, $k\varphi(p^r)/2$ is not divisible by $\varphi(p^r)$, so $2^{\varphi(p^r)/2} \equiv t^{k\phi(p^r)/2} \not\equiv 1 (\bmod p^r)$. On the other hand, letting $x = 2^{\varphi(p^r)/2}$ we have $x^2 \equiv 1 (\bmod p^r)$, and since $x^2 - 1 = (x-1)(x+1)$ and only one of these can be divisible by p, that implies $x \equiv -1 (\bmod p^r)$.