Composites Case Proof Attempt

Joseph M. Shunia

January 2024

Theorem 1 (Composites case)**.** Let $n = pq$ be an odd composite integer > 3 with p a prime divisor. Let d be the least positive integer > 2 such that $n \not\equiv 1 \pmod{d}$. Suppose $x^n = 2^{\lfloor \frac{n}{d} \rfloor} \not\equiv 1 \pmod{n}$, and consider the polynomial $f(x) = (1+x)^n - (1+x^n) \in \mathbb{Z}_p[x]$. If n does not have a prime divisor $\leq d$, then $f(x)$ is nonzero when reduced modulo $x^d - 2$.

Proof. Let p be a prime divisor of n. Consider the polynomial ring $\mathbb{Z}_p[x]$. We examine the reduction of $f(x)$ modulo $x^d - 2$, which gives us a polynomial $f(x) \pmod{x^d - 2} \in \mathbb{Z}_p[x]$. After reduction modulo $x^d - 2$, the polynomial $f(x)$ has $\deg(f(x)) = d - 1$, and can be written as $f(x) = \sum_{i=0}^{d-1} c_i x^i$.

The condition $x^n = 2^{\lfloor \frac{n}{d} \rfloor} \not\equiv 1 \pmod{n}$ implies that $x^n = 2^{\lfloor \frac{n}{d} \rfloor} \not\equiv 1 \pmod{p}$ for at least 1 prime divisor p of n. Recall also that we are given d which does not divide n, and hence $p \neq d$. Together, these imply that the powers x^k in $f(x)$ do not behave in a cyclical manner when reduced modulo p, and hence, the polynomial $f(x)$ cannot simplify to the zero polynomial due to any cyclical patterns in the exponents. Furthermore, the fact that $x^d = 2$ in our quotient ring, and not 1, ensures that x is not a dth root of unity in $\mathbb{Z}_p$ for any prime p dividing n. Hence, $f(x)$ does not exhibit any cyclical reduction that would occur if x were a root of unity.

Assume for contradiction that $f(x)$ is the zero polynomial in $\mathbb{Z}_p[x]/(x^d - 2)$. This would imply that all coefficients c_i are zero in $\mathbb{Z}_p$.

Since p is prime, $\mathbb{Z}_p$ is a finite field and $\mathbb{Z}[x]_p$ is a ring over this field. Further, since $2^{\lfloor \frac{n}{d} \rfloor} \not\equiv 1 \pmod{n}$, there must exist at least 1 prime divisor p of n such that $2^{\lfloor \frac{n}{d} \rfloor} \not\equiv 1 \pmod{p}$. This implies that 2 is not a dth power residue modulo p. That is, $a^d \not\equiv 2 \pmod{p} \in \mathbb{Z}_p$ for all integers a. Hence, it follows that $x^d - 2$ is irreducible over $\mathbb{Z}_p[x]$ and therefore, $\mathbb{Z}_p[x]/(x^d - 2)$ forms a field.

By the Fundamental Theorem of Algebra over finite fields, if $\mathbb{Z}_p[x]/(x^d - 2)$ is a field and $\deg(f(x)) = d - 1$, then $f(x)$ can have at most $d - 1$ roots in $\mathbb{Z}_p[x]/(x^d - 2)$. The assumption that $f(x)$ is zero would imply it has p roots, which is a contradiction unless $p \leq d - 1$. However, this is clearly false, since we are given n which does not have a prime divisor $\leq d$.

Therefore, $f(x)$ must be nonzero in $\mathbb{Z}_p[x]/(x^d - 2)$ for at least one prime p that divides n. $\square$