Composites Case Proof Attempt

Joseph M. Shunia

January 2024

Theorem 1 (Composites case)**.** *Let $n = pq$ be an odd composite integer greater than 3, with p a prime divisor. Let $d > 2$ be the least prime integer such that $n \not\equiv 1 \pmod{d}$. Suppose that 2 is not a d-th power residue modulo p and that n is not divisible by any prime $\leq d$. Then $(1+x)^n \not\equiv 1 + x^n \pmod{n, x^d - 2}$.*

Proof. **Preliminaries:**

- Definition of p: Under the given conditions, there must exist at least one prime divisor p of n such that 2 is not a d-th power residue modulo p. For the steps included in this proof, p always refers to this specific prime divisor of n.
- Definition of $f(x)$: We define the polynomial $f(x) := (1+x)^n - (1+x^n)$.
- Definition of $g(x)$: We define the polynomial $g(x) := f(x) \pmod{x^d - 2}$.

Introduction: If the polynomial congruence $(1+x)^n \equiv 1 + x^n \pmod{n, x^d - 2}$ holds, it implies $f(x) \equiv 0 \pmod{n, x^d - 2}$. For this to be true, $f(x)$ must also be zero modulo all of the individual prime factors of n up to at least the prime power that appears in the prime factorization of n. This is because if any of the polynomial's coefficients are indivisible by any prime power p^k dividing n (and thus any p^j in $\{p^j \mid 1 < j \leq k\}$), then those coefficients cannot be divisible by n (since n is the unique product of its prime factorization).

Hence, to prove the theorem, it suffices to show that under the given conditions, there must exist a prime divisor p of n such that $f(x) \not\equiv 0 \pmod{p, x^d - 2}$. Or equivalently, that $f(x)$ is not the zero polynomial in the ring $\mathbb{Z}_p[x]$ when reduced modulo $x^d - 2$. This forms the basis for our hypothesis.

Hypothesis: Under the given conditions, there must exist at least one prime divisor p of n such that $(1+x)^n \not\equiv 1 + x^n \pmod{p, x^d - 2}$.

Implications: If our hypothesis is true, it implies $(1+x)^n \not\equiv 1 + x^n \pmod{n, x^d - 2}$. Which is the result we intend to prove.

Step 1. Establishing irreducibility and field structure:

Since p is prime, $\mathbb{Z}_p$ is a finite field and $\mathbb{Z}_p[x]$ is a polynomial ring over this field. We aim to establish that $\mathbb{Z}_p[x]/(x^d - 2)$ forms a field. To do so, we must show that $x^d - 2$ is irreducible in $\mathbb{Z}_p[x]$.

We reference a classical theorem from field theory (Irreducibility Theorem) [1]:

Suppose $c \in F$ where F is a field, and $0 < d \in \mathbb{Z}$. The polynomial $x^k - c$ is irreducible over F if and only if c is not a qth power in F for any prime q dividing k, and c is not in $-4F^4$ when 4 divides k.

In our case, $F = \mathbb{Z}_p$, $c = 2$, and $k = d$, where d is prime.

Regarding the first criterion, given d is prime, d does not have any divisors q, and hence it suffices to check only d itself. We have chosen p such that 2 is not a d-th power residue modulo p, which informs that there is no element $b \in F$ such that $b^d \equiv 2 \pmod{p}$. The first criterion is satisfied. Since d is prime, it is not divisible by 4, and thus second criterion is also satisfied.

By the Irreducibility Theorem, $x^d - 2$ is irreducible in $\mathbb{Z}_p[x]$ and hence, the quotient ring $\mathbb{Z}_p[x]/(x^d - 2)$ forms a finite field.

Step 2. Analyzing the reduction of $f(x)$ modulo $x^d - 2$:

We examine the reduction of $g(x) = f(x) \pmod{x^d - 2} \in \mathbb{Z}[x]$. After reduction modulo $x^d - 2$, the polynomial $g(x)$ has $\deg(g(x)) = d - 1$, and can be written as:

$$g(x) = \sum_{i=0}^{d-1} c_i x^i \tag{1}$$

To justify this: We first look to the expansion of $f(x) = (1 + x)^n - (1 + x^n) \in \mathbb{Z}[x]$:

$$f(x) = \sum_{k=1}^{n-1} \binom{n}{k} x^k \tag{2}$$

Notice that subtracting $1 + x^n$ from $(1 + x)^n$ cancels out the terms $\binom{n}{0}x^0 = 1$ and $\binom{n}{n}x^n = x^n$ that would typically be present in the binomial expansion of $(1 + x)^n$. Thus, we have $\deg(f(x)) = n - 1$.

Reducing $f(x)$ modulo $x^d - 2$ means replacing every term of the form $\binom{n}{k}x^k$ for $k \geq d$ with a lower-degree term, using the relation $x^d = 2$. During this reduction, terms in $f(x)$ with degree $1 \leq k < d$ will retain their degrees, as they are unaffected by the modulo operation. Since $d < n$, these terms are always present in the binomial expansion. Further, since the highest possible degree of any reduced terms is also $d - 1$, the degree of $g(x)$ remains $d - 1$ after the reduction of any additional terms.

To ensure $g(x)$ is nonzero, we must also consider the coefficients of the remainder terms. Since the coefficients of the terms in $f(x)$ are the binomial coefficients in the n-th row of Pascal's Triangle from $\binom{n}{1}$ to $\binom{n}{n-1}$, it is not possible for all coefficients to be zero after the reduction modulo $x^d - 2$. Instead, the coefficients of these terms will be "wrapped" around $x^d - 2$ and added to the fixed term which corresponds to the value of their degree k, which is the term with the variable $x^{k \pmod d}$. Therefore, after the reduction of $f(x)$ modulo $x^d - 2$, the resultant polynomial $g(x)$ will have d polynomial terms with nonzero coefficients and is not the zero polynomial.

In summary, $x^d - 2$ does not divide $f(x)$ in $\mathbb{Z}[x]$ and thus, $g(x)$ is nonzero and has a degree of $d - 1$.

Step 3. Confirming nonzero polynomial in quotient ring:

We look to the quotient ring $\mathbb{Z}_p[x]/(x^d - 2)$, which forms a finite field (See Step 1).

In Step 2, we showed that $g(x) = f(x) \pmod{x^d - 2}$ is nonzero in $\mathbb{Z}[x]$ with $\deg(g(x)) = d - 1$.

To prove our hypothesis, we must also show that $g(x)$ is nonzero in $\mathbb{Z}_p[x]/(x^d - 2)$, as this is equivalent to the statement in our hypothesis, which says: $(1 + x)^n \not\equiv 1 + x^n \pmod{p, x^d - 2}$ for at least one prime p dividing n.

Now, assume for contradiction that $g(x)$ is the zero polynomial in $\mathbb{Z}_p[x]/(x^d - 2)$. This would necessarily imply that all coefficients c_i of $g(x) = \sum_{i=0}^{d-1} c_i x^i$ are zero when taken modulo p, where the c_i are aerated sums of binomial coefficients.

In a finite field, a polynomial of degree r can have at most r roots [2]. This is because a polynomial of degree r in a finite field can be factored into at most r linear factors (each corresponding to a root), within an algebraic closure of that field. However, within the field itself, the number of roots can be fewer than r, but never more.

In our case, if $\mathbb{Z}_p[x]/(x^d - 2)$ is a finite field and $\deg(g(x)) = d - 1$, then $g(x)$ can have at most $d - 1$ roots in this field. The assumption that $g(x)$ is the zero polynomial is a direct contradiction unless $p \leq d - 1$, as it would necessarily imply that $g(x)$ has infinitely many roots (or more precisely, that every element of $\mathbb{Z}_p$ is a root) [3]. However, this is clearly not the case, as we are given n which does not have a prime divisor $\leq d$.

Therefore, $f(x)$ cannot be identically zero in $\mathbb{Z}_p[x]/(x^d - 2)$.

Conclusion:

We have proven our hypothesis under the given conditions by demonstrating $(1+x)^n \not\equiv 1+x^n \pmod{p, x^d-2}$ for at least one prime divisor p of n. Hence, we deduce $(1+x)^n \not\equiv 1+x^n \pmod{n, x^d-2}$. This completes the proof. □

References

[1] Gregory Karpilovsky. *Topics in Field Theory*. North-Holland Mathematics Studies. North-Holland, 1989. ISBN 9780444705207.

[2] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, 3 edition, 2004. ISBN 978-0-471-43334-7.

[3] Swastik Kopparty and Qiang Wang. Roots and coefficients of polynomials over finite fields. *Finite Fields and Their Applications*, 29:198–201, 2014. ISSN 1071-5797. doi: https://doi.org/10.1016/j.ffa.2014.04.002. URL `https://www.sciencedirect.com/science/article/pii/S1071579714000574`.