Binomial Coefficients Modulo Primes and Lucas' Theorem

Mar Detic

Abstract

This paper explores the properties of binomial coefficients modulo a prime number, with a particular focus on the case when the prime is p. We first prove a result that shows that for any prime p, for integers k such that $1 < k < \sqrt{p}$, the binomial coefficient $\binom{p}{k} \equiv 0 \pmod{p}$. Additionally, we discuss Lucas' Theorem, which provides a method for computing binomial coefficients modulo a prime in a more general context.

1 Theorem on Binomial Coefficients Modulo a Prime

Let p be a prime number. Then, for any integer k such that $1 < k < \sqrt{p}$, the binomial coefficient $\binom{p}{k}$ satisfies the congruence

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Consequently, there is no integer k such that $1 < k < \sqrt{p}$ for which

$$\binom{p}{k} \equiv -1 \pmod{p}.$$

2 Proof

We begin by recalling the definition of the binomial coefficient:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

Here, $p!$ is the factorial of p, and $k!$ and $(p-k)!$ are the factorials of k and $p-k$, respectively.

Since p is a prime number, the factorial $p!$ can be written as

$$p! = p \cdot (p-1)!.$$

Therefore, the binomial coefficient becomes

$$\binom{p}{k} = \frac{p \cdot (p-1)!}{k!(p-k)!}.$$

Note that p divides $p!$ but does not divide $k!$ or $(p-k)!$ for any integer k in the range $1 < k < \sqrt{p}$, as k and $p-k$ are both less than p, and neither $k!$ nor $(p-k)!$ contains the factor p.

Thus, the prime factor p in the numerator cannot be canceled by any factors in the denominator. Therefore, the binomial coefficient is divisible by p, and we have the congruence

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Since $0 \not\equiv -1 \pmod{p}$ for any prime p, it follows that there is no integer k such that $1 < k < \sqrt{p}$ for which

$$\binom{p}{k} \equiv -1 \pmod{p}.$$

3 Lucas' Theorem

Lucas' Theorem gives a method for calculating binomial coefficients modulo a prime number p for arbitrary non-negative integers n and k. It states that if n and k are written in base p as

$$n = n_m p^m + n_{m-1} p^{m-1} + \cdots + n_1 p + n_0,$$
$$k = k_m p^m + k_{m-1} p^{m-1} + \cdots + k_1 p + k_0,$$

then the binomial coefficient $\binom{n}{k}$ modulo p is given by

$$\binom{n}{k} \equiv \prod_{i=0}^{m} \binom{n_i}{k_i} \pmod{p},$$

where n_i and k_i are the digits of n and k in base p, respectively.

This theorem allows us to compute binomial coefficients modulo p by breaking the problem into smaller, more manageable parts. For example, instead of computing $\binom{n}{k}$ directly for large n and k, we can compute the binomial coefficients for each corresponding digit n_i and k_i in the base-p expansion of n and k.

4 Differences Between the Theorem and Lucas' Theorem

Although both the result presented in the theorem and Lucas' Theorem deal with binomial coefficients modulo a prime, they differ significantly in their scope and application:

- **Specificity of the Case:** - The theorem presented here specifically addresses binomial coefficients of the form $\binom{p}{k}$ where p is a prime number, and k lies in the range $1 < k < \sqrt{p}$. It proves that these binomial coefficients are congruent to zero modulo p. - Lucas' Theorem is more general and applies to any non-negative integers n and k. It provides a method for calculating $\binom{n}{k} \mod p$ by reducing the problem to smaller binomial coefficients based on the base-p digits of n and k.

- **Scope:** - The result in the theorem only applies to binomial coefficients where the upper index is a prime number. It does not generalize to arbitrary integers n. - Lucas' Theorem applies to all integers n and k, allowing for the calculation of binomial coefficients modulo p for a much broader range of values.

- **Congruence Behavior:** - The theorem specifically proves that $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 < k < \sqrt{p}$, focusing on a special case of binomial coefficients. - Lucas' Theorem does not focus on this specific congruence. Instead, it provides a way to compute binomial coefficients modulo p in a recursive manner based on the digits of n and k in base p.

Thus, while your theorem provides a specific result for binomial coefficients involving a prime p, Lucas' Theorem is a broader result applicable to all integers and provides a method for evaluating binomial coefficients modulo primes in a more general setting.

5 Conclusion

We have proved that for any prime p and integer k such that $1 < k < \sqrt{p}$, the binomial coefficient $\binom{p}{k} \equiv 0 \pmod{p}$, and thus cannot be congruent to $-1 \pmod{p}$. We also provided an overview of Lucas' Theorem, which offers a method for calculating binomial coefficients modulo a prime number for arbitrary values of n and k, extending the result to a broader context.