Polynomials mod p, orders, generators

Andres Buritica

1 Introduction

Let p be a prime and n be a positive integer throughout.

Recall that $\mathbb{Z}_n$ denotes the integers mod n, and $\mathbb{Z}_n^*$ denotes the subset of $\mathbb{Z}_n$ containing the invertible elements. A *polynomial in* $\mathbb{Z}_n$ is a polynomial with coefficients in $\mathbb{Z}_n$.

The *order* of an invertible element a of $\mathbb{Z}_n$, denoted $\text{ord}_n(a)$, is the smallest positive integer n such that $a^n \equiv 1 \pmod{n}$.

If $\text{ord}_n(a) = |Z_n^*|$, then a is said to be a *generator* mod n.

There is always a generator mod p; we prove this in section 3, but assume it for now.

If a polynomial of degree d in $\mathbb{Z}_p$ has more than d roots mod p, then it is the zero polynomial. (The proof is the same as the proof for polynomials with real coefficients.)

2 Exercises

- $a^k \equiv 1 \pmod{n} \iff \text{ord}_n(a) \mid n$.
- $\text{ord}_n(a) \mid \varphi(n)$.
- If $q \mid 2^p - 1$, then $q > p$.
- Every prime factor of $2^{2^n} + 1$ is congruent to 1 mod 2^{n+1}.
- If g is a generator mod n, then $\{g^1, g^2, \ldots, g^{\varphi(n)}\}$ contains all nonzero residues mod n exactly once.
- If g is a generator mod n, and $\varphi(n) = 2k$, then

$$g^k \equiv -1 \pmod{n}.$$

- There are either 0 or $\varphi(\varphi(n))$ generators mod n.
- There are $\varphi(a)$ residues x mod p such that $x^a \equiv 1 \pmod{p}$ but $x^k \not\equiv 1 \pmod{p}$ for any $k < a$.
- If there exists a generator mod n, then the product of the elements of $\mathbb{Z}_n^*$ is -1 mod n.

- For any positive integer $n < p-1$,

$$\sum_{i=1}^{p-1} i^n \equiv 0 \pmod{p}.$$

- For every function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ there is a unique polynomial P in $\mathbb{Z}_p$ of degree less than $p-1$ such that $f(x) = P(x)$ for each $x \in \mathbb{Z}_p$.

- Let g be a generator mod p, and let $ab = p-1$. Then,

$$\prod_{i=1}^{a} (x - g^{bi}) \equiv x^a - 1 \pmod{p}.$$

  What does this tell us about the roots of the cyclotomic polynomials in mod p?

- Consider all $\binom{p-1}{k}$ products of k elements of $\mathbb{Z}_p$. Their sum is divisible by p.

- For any positive integer $n < p-1$,

$$\sum_{i=1}^{p-1} i^n \equiv 0 \pmod{p}.$$

  (Give a proof involving polynomials.)

- Assume there exists a generator mod n. An element $x \in \mathbb{Z}_n^*$ can be written as y^k for $y \in \mathbb{Z}_n^*$ iff $\mathrm{ord}_p(x) \gcd(\varphi(n), k) \mid \varphi(n)$.

3 Existence of generators

Let p be an odd prime.

- There exists a generator mod p.
- There exists a generator mod p^k for any positive integer k.
- There exists a generator mod $2p^k$ for any positive integer k.
- There exists a generator mod 2^k iff $k \leq 2$.
- If $n = xy$, where x and y are coprime and larger than 2, then there does not exist a generator mod n.

4 Problems

1. Find all positive integers n such that $n \mid 2^n - 1$.
2. Prove that if $\sigma(n) = 2n + 1$, then n is a perfect square.
3. Find all positive integers n such that $n \mid 2^{n-1} + 1$.
4. Find all primes p, q, r such that $p \mid q^r + 1,\ q \mid r^p + 1,\ r \mid p^q - 1$.
5. Find the sum of all generators mod p.
6. Let n and m be nonnegative integers, and let p be prime. Prove that

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

   where $n = \sum n_i p^i$ and $m = \sum m_i p^i$.
7. Find all positive integers n for which there exists a function $g : \mathbb{Z}_n \to \mathbb{Z}_n$ such that all the functions

   $$g(x), g(x) + x, \ldots, g(x) + 100x$$

   are bijections $\mathbb{Z}_n \to \mathbb{Z}_n$.

5 Homework

1. Prove that for all positive integers $a > 1$ and n we have $n \mid \varphi(a^n - 1)$.
2. Assume that g is a generator mod p such that $p \mid g^2 - g - 1$.
   (a) Prove that $g - 1$ is a generator mod p.
   (b) Prove that if $p \equiv 3 \pmod 4$, then $g - 2$ is also a generator mod p.
3. Let p and q be primes. Prove that there is an integer x such that $(x+1)^p \equiv x^p \pmod q$ if and only if $q \equiv 1 \pmod p$.