Orders, generators

Andres Buritica Monroy

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. (In other words, $a \in \mathbb{Z}_n^*$ iff $a \in \mathbb{Z}_n$ and $\gcd(a, n) = 1$.)

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

If $\mathrm{ord}_n(a) = |\mathbb{Z}_n^*| = \varphi(n)$, 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.

2 Exercises

- $a^k \equiv 1 \pmod{n} \iff \mathrm{ord}_n(a) \mid k$.
- $\mathrm{ord}_n(a) \mid \varphi(n)$.
- If $q \mid 2^p - 1$, where p and q are prime, 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 the least residues of $\{g^1, g^2, \ldots, g^{\varphi(n)}\}$ are $\mathbb{Z}_n^*$.
- 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.
- If $a \mid \varphi(n)$ and there exists a generator mod n, then there are $\varphi(a)$ residues x mod n such that $\mathrm{ord}_n(x) = a$.
- 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 $n < p - 1$,

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

- 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 $\operatorname{ord}_p(x) \gcd(\varphi(n), k) \mid \varphi(n)$.

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 $k \le 2$.
- 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. Let $p > 10$ be a prime. Prove that there are positive integers m, n with $m + n < p$ such that p divides $5^m 7^n - 1$.
2. Find all positive integers n such that $n \mid 2^n - 1$.
3. Prove that if $\sigma(n) = 2n + 1$, then n is a perfect square.
4. Let p be a prime. Find all nonempty sets S of residues mod p such that if the least residues of a and b are not in S, then
$$\prod_{i \in S}(a - i) \equiv \prod_{i \in S}(b - i) \pmod p.$$
5. Let p be an odd prime and r an odd natural number. Show that $pr + 1$ does not divide $p^p - 1$.
6. Let p be an odd prime and let m and n be natural numbers not divisible by p. Prove that if there is some integer s such that $p \mid m^{2^s} + n^{2^s}$, then $p \equiv 1 \pmod{2^{s+1}}$.
7. Find all positive integers n such that $n \mid 2^{n-1} + 1$.
8. Find all positive integers n that satisfy the following property: for all positive integers m, relatively prime to n, we have $2n^2$ divides $m^n - 1$.
9. Find all primes p, q, r such that $p \mid q^r + 1,\ q \mid r^p + 1,\ r \mid p^q - 1$.

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 $q \equiv 1 \pmod p$.