

Study guide

- (§28) What is the *order* $e_p(a)$ of a number modulo p ?
- (§28) Know the definition of *primitive root* in terms of order, and the equivalent description in terms of distinct powers.
- (§30) What is the *index* $I(a)$ of a number modulo p ?
- (§29) Be able to prove: $a^n \equiv 1 \pmod p$ iff $e_p(a) \mid n$.
- (§29) How are primitive roots related to Costas arrays?

- Suppose that p is a prime number and g is a primitive root modulo p .
 - Suppose that $d \mid (p-1)$. Prove that $g^{(p-1)/d}$ has order d .
 - Suppose that $\gcd(i, p-1) = 1$. Prove that g^i is also a primitive root modulo p .
 - Prove that for any integer i , $e_p(g^i) = \frac{(p-1)}{\gcd(i, p-1)}$ (it is possible to prove this using parts (a) and (b) fairly quickly).
- Suppose that $a \not\equiv 0 \pmod p$. Prove that for any two integers e, f , $a^e \equiv a^f \pmod p$ if and only if $e \equiv f \pmod{e_p(a)}$.
- As noted in class, we can define the order modulo m $e_m(a)$ of a unit modulo m for any modulus m (prime or composite). We can furthermore define g to be a primitive root modulo m if $e_m(g) = \varphi(m)$.
 - Suppose that m, n are coprime integers. Prove that

$$e_{mn}(a) = \text{lcm}(e_m(a), e_n(a)).$$
 - Deduce that if $m = pq$, where p and q are distinct odd primes, then there are no primitive roots modulo m .
- (Textbook 28.17)
Use Welch's construction to find a Costas array of size 16. Be sure to indicate which primitive root you used.
- (Textbook 28.18, on a construction of Lempel and Golomb)
This exercise describes a special case of a construction of Lempel and Golomb for creating Costas arrays of size $p-2$.
 - Let g_1 and g_2 be primitive roots modulo p . (They are allowed to be equal.) Prove that for every $1 \leq i \leq p-2$ there is a unique $1 \leq j \leq p-2$ satisfying

$$g_1^i + g_2^j \equiv 1 \pmod p$$
 - Create a $(p-2)$ -by- $(p-2)$ array by putting a dot in the i^{th} row and the j^{th} column if i and j satisfy $g_1^i + g_2^j \equiv 1 \pmod p$. Prove that the resulting array is a Costas array.
 - Use the Lempel-Golomb construction to write down two Costas arrays of size 15. For the first, use $g_1 = g_2 = 5$, and for the second, use $g_1 = 3$ and $g_2 = 6$.