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: $a^n \equiv 1 \bmod p$ iff $e_p(a) \mid n$.
- (§29) How are primitive roots related to Costas arrays?

1. Suppose that p is a prime number and g is a primitive root modulo p.
   (a) Suppose that $d \mid (p-1)$. Prove that $g^{(p-1)/d}$ has order d.
   (b) Suppose that $\gcd(i, p-1) = 1$. Prove that g^i is also a primitive root modulo p.
   (c) 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).
2. Suppose that $a \not\equiv 0 \bmod p$. Prove that for any two integers e, f, $a^e \equiv a^f \bmod p$ *if and only if* $e \equiv f \bmod e_p(a)$.
3. 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 $e_m(g) = \varphi(m)$.
   (a) Suppose that m, n are coprime integers. Prove that
   $$e_{mn}(a) = \operatorname{lcm}(e_m(a), e_n(a)).$$
   (b) Deduce that if $m = pq$, where p and q are distinct odd primes, then there are no primitve roots modulo m.
4. (Textbook 28.17, on a Costas array of size 16)
5. (Textbook 28.18, on a construction onf Lempel and Golumb)