Elementary Number Theory

Math 175, Section 30, Autumn 2010
Shmuel Weinberger (shmuel@math.uchicago.edu)
Tom Church (tchurch@math.uchicago.edu)
www.math.uchicago.edu/~tchurch/teaching/175/

Script 5: Primitive Roots

Definition 5.1. Let k be a positive integer, and let R be a field. Given $x \in R$, we say that x is a *k-th root of unity* if $x^k = 1$. We say that x is a ***primitive*** *k-th root of unity* if it is not an ℓ-th root of unity for any smaller ℓ: that is, $x^k = 1$ and $x^\ell \neq 1$ for all $1 \leq \ell < k$.

Theorem 5.2. If $x^a = 1$ and $x^b = 1$, then $x^{\gcd(a,b)} = 1$.

Theorem 5.3. If x is a primitive k-th root of unity, and x is an m-th root of unity, then $k|m$.

Lemma 5.4. If x is a primitive k-th root of unity in R, then the number of k-th roots of unity in R is at least k.

Theorem 5.5. If there exists a primitive k-th root of unity in a field R, the number of k-th roots of unity in R is exactly k.

Exercise 5.6.

a) Find a primitive cube root of unity in $\mathbb{Z}/7\mathbb{Z}$.

b) Find a primitive cube root of unity in $\mathbb{Z}/13\mathbb{Z}$.

c) Find a primitive cube root of unity in $\mathbb{Z}/19\mathbb{Z}$.

Theorem 5.7. Let p be a prime number. There exists a primitive cube root of unity in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \equiv 1 \pmod 3$.

Definition 5.8. Let q be a prime number and

$$S = \left\{ (a_1, \ldots, a_q) \middle| a_i \in R^\times,\ a_1 a_2 \cdots a_q = 1 \right\}$$

be the set of length-q sequences of elements of $R^\times$ whose product is 1. If $(a_1, a_2, \ldots, a_q) \in S$ is such a sequence, we can "rotate" the sequence to obtain a new sequence $(a_2, \ldots, a_q, a_1) \in S$. We say that a sequence is *rotation-invariant* if rotation yields the same sequence:

$$(a_1, a_2, \ldots, a_q) = (a_2, \ldots, a_q, a_1).$$

We always have the trivial example of a rotation-invariant sequence in S, namely $(1, 1, \ldots, 1) \in S$.

Lemma 5.9. Let q be a prime number. If q divides the size of $R^\times$, then S contains some nontrivial rotation-invariant sequence $(a_1, \ldots, a_q)$.

Theorem 5.10. Let q be a prime number. There exists a primitive q-th root of unity in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \equiv 1 \pmod{q}$.

Theorem 5.11. Let k and ℓ be relatively prime: $(k, \ell) = 1$. If x is a primitive k-th root of unity in R, and y is a primitive ℓ-th root of unity in R, then there exists a primitive $k\ell$-th root of unity in R.

Theorem 5.12. Let q be a prime number, and let k be a positive integer. There exists a primitive q^k-th root of unity in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \equiv 1 \pmod{q^k}$.

Hint: prove by induction on k, and consider the set:

$$T = \left\{ (a_1, \ldots, a_q) \middle| a_i \in \mathbb{Z}/p\mathbb{Z}^\times,\ a_1 a_2 \cdots a_q \text{ is a } q^{k-1}\text{-th root of unity} \right\}$$

Theorem 5.13. Let p be a prime number. There exists an element $a \in \mathbb{Z}/p\mathbb{Z}$ so that every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ is a power of a.