Number Theory Homework #5

Prof. Zeev Rudnick

To be handed in on Monday, December 12, 2016.

---

1) A **primitive root** (שרש פרימיטיבי) modulo n is a residue whose order modulo n is φ(n). Find the minimal primitive root modulo p for all odd primes p less than 20 (p=3,5,7,11,13,17,19).

2) Find all the primitive roots modulo 19.

3) Let p be an odd prime, and $g \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ an invertible residue modulo p. Show that g is a primitive root modulo p if and only if for all prime divisors q of p-1, we have $g^{(p-1)/q} \neq 1 \bmod p$.

4) Show that 4 is not a primitive root modulo p for any prime p>2.

5) Show that if n>2 then φ(n) is even.

6) If m > 2, n > 2 are coprime integers, show that there is no primitive root modulo mn.

Mailbox 085, first floor of Schreiber building

Course homepage: http://www.math.tau.ac.il/~rudnick/courses/int_numth.html