Number Theory Homework #6

Prof. Zeev Rudnick

To be handed in by Monday, December 12, 2011.

---

1. Find the last two digits in the decimal expansion of 7^{2011} (for example, the last two digits of 1729 are 29). Do the same for 3^{2011} and 7^{2012}.
2. Let p be an odd prime. Show that for any invertible $\boldsymbol{a}$ mod p, $\boldsymbol{a}^{\frac{p-1}{2}} \equiv \pm 1 \mod \boldsymbol{p}$.
   Hint: what is the **square** of this element ?

3. 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 primes p less than 50.

4. Show that 4 is not a primitive root modulo p for any prime p>3.

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