Number Theory Homework #8

Prof. Zeev Rudnick

To be handed in on Monday, January 2, 2017.

---

1. Decide which of the following congruences are solvable, and if so, find all solutions:

   a) $x^2 = c \bmod 363$, $c=1,5,31$.   b) $x^2 = 54 \bmod 125$.

2. a) Let p be a prime of the form 4q+1 where q is also a prime. Show that 2 is a primitive root modulo p.

   b) Find 5 examples of such primes.

3. A *Carmichael number* is a composite integer N>1 which satisfies $a^{N-1} = 1 \bmod N$ for all a coprime to N. *Korselt's criterion* states that if N is an odd composite integer which is square-free and all prime divisors p of N satisfy p-1 divides N-1, then N is a Carmichael number. Check which of the following integers are Carmichael numbers: 1105, 1235, 2821, 6601, 8910.

4. Show that if p=6k+1, q=12k+1, r=18k+1 are all prime then their product N=pqr is a Carmichael number. Find two values of k which satisfy this assumption.

Mailbox 085, first floor of Schreiber building

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