Math 345 – Wednesday 11/15/17

Exercise 45. Let p be an odd prime.

(a) If $a = b^2$ is a perfect square, explain why it is impossible for a to be a primitive root modulo p.

(b) Let g be a primitive root modulo p. Prove that g^k is a quadratic residue modulo p if and only if k is even.

(c) If k divides $p-1$, show that the congruence $x^k \equiv 1 \pmod{p}$ has exactly k distinct solutions modulo p.

Exercise 46. Use the discrete logarithm table for $p = 37$ to find *all* solutions to the following congruences.

(a) $12x \equiv 23 \pmod{37}$

(b) $5x^{23} \equiv 18 \pmod{37}$

(c) $x^{12} \equiv 11 \pmod{37}$

(d) $7x^{20} \equiv 34 \pmod{37}$

Exercise 47. Create a discrete logarithm table for $p = 17$, and use it to find all solutions to $5x^6 \equiv 7 \pmod{17}$.