Math 7770 Spring 2011
Homework 5
Due: February 21, 2011

You are welcome to work together but everyone needs to write up **distinct** solutions. If you use any books outside of our textbook or other people, please make sure to give them credit. Make sure your solutions are complete. If your handwriting is atrocious, I am happy to give you a basic introduction to LaTeX.

Warmup

- §2.7 # 1. Reduce the following congruences to equivalent congruences of degree ≤ 6.
  (a) $x^{11} + x^8 + 5 \equiv 0 \bmod 7$
  (b) $x^{20} + x^{13} + x^7 + x \equiv 2 \bmod 7$
  (c) $x^{15} - x^{10} + 4x - 3 \equiv 0 \bmod 7$.
- §2.8 # 4. To what exponents do each of 1, 2, 3, 4, 5, 6 belong modulo 7? To what exponents do they belong modulo 11? (We did 7 in class so feel free to pick another number to try.)
- §2.8 # 8. Use Theorem 2.37 to determine how many solutions each of the following congruences has:
  (a) $x^{12} \equiv 16 \bmod 17$
  (b) $x^{48} \equiv 9 \bmod 17$
  (c) $x^{20} \equiv 13 \bmod 17$
  (d) $x^{11} \equiv 9 \bmod 17$
- §3.1 # 3. Prove that 3 is a quadratic residue of 13 but a quadratic non-residue of 7.

Problems

1. §2.8 # 5. Let p be an odd prime. Prove that a belongs to the exponent 2 modulo p if and only if $a \equiv -1 \bmod p$.
2. §2.8 # 9. Show that $3^8 \equiv -1 \bmod 17$. Explain why this implies that 3 is a primitive root of 17.
3. §2.8 # 12. Prove that if p is a prime, $(a, p) = 1$ and $(n, p-1) = 1$ then $x^n \equiv a \bmod p$ has exactly one solution.
4. §2.8 # 21. Let g be a primitive root of the odd prime p. Show that $-g$ is a primitive root, or not, according as $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$.

Challenge

I. §2.8 # 23. Prove that if a belongs to the exponent 3 modulo a prime p, then $1+a+a^2 \equiv 0 \bmod p$, and $1 + a$ belongs to the exponent 6.