Math 250 – Number Theory – Homework 8

Due: Friday April 21st

Please explain your answers carefully using full sentences, not only symbols. You may use the textbook and your notes, and you're welcome to discuss the problems with one another or with me. However, your final answers should be written on your own and in your own words.

At the top of the first page, please list any classmates you collaborated with while working on these exercises (so that we know to expect similar solutions).

- 1. (a) Compute $4^{56} \mod 63$.
 - (b) Compute $6^{83} + 8^{83} \mod 49$.
 - (c) Find the last two decimal digits of $8003^{8002^{8001}}$.
- 2. (a) Find all primitive roots modulo 11.
 - (b) Find a single primitive roots modulo 25.
 - (c) Find a single primitive root modulo 29.
- 3. Find all solutions to the following congruences.
 - (a) $x^4 \equiv 12 \mod 25$.
 - (b) $x^3 \equiv 27 \mod 29$.
 - (c) $3x^5 \equiv 1 \mod 23$.
- 4. Consider the RSA encryption system with public key n = 91, a = 47 (so message encryption is via sending m to $m^{47} \mod 91$).
 - (a) Work out the value of the private key.
 - (b) Suppose a word is encrypted by representing a sequence of letters by numbers $0 \le m \le 25$, with $A = 0, B = 1, \dots, Z = 25$. Decrypt the message 61, 23, 86, 82 (please do use a calculator).