189-346B/377B: Number Theory

Midterm Exam

Friday, February 11

1. Show that the gcd of two integers a and b is a linear combination of a and b, i.e., that if $d = \gcd(a, b)$ then there exist integers m and n for which

$$d = ma + nb.$$

2. State two number-theoretic problems that are believed to be computationally intractable, and for each problem, name a cryptosystem that exploits this presumed intractability. (This question is just to test your knowledge of the salient points in the material covered in class. You do not need to provide descriptions of the cryptosystems in question, only their names. If you can't remember the names, then a brief description will do...)

3. Compute

$$7^{403275023750023740523040602} \pmod{101}.$$

You should express your answer as an integer between 0 and 100.

4. A *Sophie Germain prime* is a prime p of the form $1 + 2q$ where q is also a prime. Assume that p is such a prime. Show that $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ is a primitive root modulo p if and only if

$$a \neq \pm 1, \quad a \neq b^2 \pmod{p}, \text{ for any } b \in (\mathbf{Z}/p\mathbf{Z})^\times.$$

Find the smallest primitive root modulo 23.

5. Solve the equation

$$x^2 + 1 = 0 \pmod{101^2}.$$