Math 55: Discrete Mathematics
Williams, Spring 2018
GSI: Ai

Week 5: More Number Theory, RSA, Induction

Remarks:

- Note much of this worksheet comes from Week 4 (right before the midterm).
- 6887 is the product of two primes. My coprime "public key" is 11. Use message blocks of 4 digits and the usual conversion, $A = 00, B = 01, \ldots$. Using these parameters, encrypt the message READ. Next pretend you are an attacker. How would you decrypt the code? (You can use a computer for this entire exercise, but exactly one step is supposed to be challenging even for the computer. Which step?)

1. (Ribet Spr13) Numbers a_n are defined as follows: $a_0 = 0, a_1 = 1, a_{n+2} = 5a_{n+1} - 6a_n$ for $n \geq 0$. Prove that $a_n = 3^n - 2^n$ for $n \geq 0$.

2. (Sturmfels Spr09) Solve the recurrence relation $a_n = 6a_{n-1} - 9a_{n-2}$ with the initial conditions $a_0 = 1$ and $a_1 = 9$.

3. (Ribet Spr15) Using the identity $1 = 54 \cdot 129 - 35 \cdot 199$, write down an integer that is congruent to 35 (mod 129) and to 54 (mod 199). You can leave your answer as an arithmetic expression (i.e. one involving products, sums, differences).

4. (Sturmfels Spr12) What amount of postage can be formed using only 5-cent and 6-cent stamps? Formulate a conjecture and prove it. (GSI commentary: Professor did something like this in lecture. Try it.)

5. (Sturmfels Spr12) Determine an integer n such that
$$n \equiv 1 \pmod 7, \quad n \equiv 3 \pmod 8, \quad n \equiv 2 \pmod 9.$$

6. (Sturmfels Spr09) Find an inverse of 81 modulo 250.