Number Theory, Fall 2016. Test #1.
Due on Thursday, September 22nd, in class

Directions: Provide complete arguments (do not skip steps). State clearly and FULLY any result you are referring to. Partial credit for incorrect solutions, containing steps in the right direction, may be given. If you are unable to solve a problem (or a part of a problem), you may still use its result to solve a later part of the same problem or a later problem in the exam.

Rules: You are NOT allowed to discuss midterm problems with anyone else except me. You may ask me any questions about the problems (e.g. if the formulation is unclear), but as a rule I will only provide minor hints. You may freely use your class notes, the class textbook by Jones and Jones, all materials from Math 5653 websites (Spring 2013, Spring 2014, Fall 2016) and all publicly available materials from Math 3354 website from Spring 2016. The use of other books or online sources is generally not allowed; if there is a particular source you would like to consult, you should check with me first if that would be Ok.

1. (10 pts) Let m and n be coprime integers. Determine all possible values of $gcd(3m+n, m+3n)$. For each value you list show (by an explicit example) that it is indeed possible and prove that all other values cannot occur.

Bonus: (value TBD). Solve an analogous question for $gcd(am+bn, cm+dn)$ where a, b, c, d are fixed integers (the answer will depend on a, b, c and d). Correct answer (or even something close to a correct answer) will receive some credit.

2. (10 pts) Let $a, b, c \in \mathbb{Z}$, and consider the system of three congruences

$$x \equiv a \mod 5, \quad 2x \equiv b \mod 7, \quad 2x \equiv c \mod 32.$$

Find all a, b and c for which the system has an (integer) solution, and in the case when there is a solution, find a formula for the general solution. Your answer should be an explicit formula involving a, b and c, but you will probably need to break down the argument into several cases.

3. (10 pts) Let $n \geq 2$ be an integer. Find the number of reduced solutions to the congruence

$$x^3 - 5x^2 + 6x \equiv 0 \mod n.$$

The answer can be expressed in terms of prime factorization of n.

4. (10 pts) Let $f(x) = x^2 + ax + b$ for some $a, b \in \mathbb{Z}$, and let p be an odd prime. Let S_{p^2} denote the set of reduced solutions to the congruence

$$f(x) \equiv 0 \mod p^2.$$

Prove that $|S_{p^2}|$ is equal to 0, 2 or p and show that each of those three possibilities may occur (for some a and b). **Note:** you are not allowed to pick your p in the problem; the proof should work for arbitrary p.