MA 335, Spring 2014

Assignment 6.

This homework is due *Friday* March 7.

There are total 34 points in this assignment. 30 points is considered 100%. If you go over 30 points, you will get over 100% for this homework (but not over 115%) and it will count towards your course grade.

Collaboration is welcome. If you do collaborate, make sure to write/type your own paper *and give credit to your collaborators in your pledge.* Your solutions should contain full proofs. Bare answers will not earn you much.

(1) (part of 4.4.1) Solve the following linear congruences:
   (a) [2pt] $25x \equiv 15 (\text{mod } 29)$.
   (b) [2pt] $6x \equiv 15 (\text{mod } 21)$.
   (c) [2pt] $34x \equiv 60 (\text{mod } 98)$.

(2) (part of 4.4.4) Solve the following sets of simultaneous linear congruences:
   (a) [3pt] $x \equiv 1 (\text{mod } 3)$, $x \equiv 2 (\text{mod } 5)$, $x \equiv 3 (\text{mod } 7)$.
   (b) [4pt] $2x \equiv 1 (\text{mod } 5)$, $3x \equiv 9 (\text{mod } 6)$, $4x \equiv 1 (\text{mod } 7)$, $5x \equiv 9 (\text{mod } 11)$.

(3) [3pt] (4.4.10) (Ancient Chinese Problem) A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

(4) [2pt] (5.2.1) Use Fermat's theorem to verify that 17 divides $11^{104} + 1$.

(5) (5.2.2ac)
   (a) [2pt] If $\gcd(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$. (*Hint:* Use Fermat's theorem mod 7 and mod 5. Then apply the uniqueness part of Chinese Remainder Theorem.)
   (b) [2pt] If $\gcd(a, 133) = \gcd(b, 133) = 1$, show that $133 \mid a^{18} - b^{18}$.

(6) [2pt] (5.2.3) From Fermat's theorem deduce that, for any integer $n \geq 0$,
$$13 \mid 11^{12n+6} + 1.$$

(7) [2pt] (5.2.7+) If $p = 2m + 1$ is an odd prime and $p \nmid a$, prove that $a^m - 1$ or $a^m + 1$ is divisible by p. (*Hint:* Consider the product of these numbers.)

(8) (5.2.10) Assuming a and b are integers not divisible by the prime p, establish the following:
   (a) [2pt] If $a^p \equiv b^p \pmod{p}$, then $a \equiv b \pmod{p}$.
   (b) [3pt] If $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.
   (*Hint:* By (a), $a = b + pk$ for some k, so that $a^p - b^p = (b + kp)^p - b^p$; now show that p^2 divides the later expression.)

(9) [3pt] (5.2.14) If p and q are distinct primes, prove that
$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$