MA 335, Spring 2012

Assignment 11.

This homework is due *Thursday* April 12.

This homework is somewhat short, but it's still worth the same as the other ones in terms of the course grade. Consider it an opportunity to catch up if you are behind.

There are total 28 points in this assignment. 24 points is considered 100%. If you go over 24 points, you will get over 100% for this homework (up to 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) (9.4.7ab+) Determine the values of *odd* a for which the congruences below are solvable and solve these congruences.
   (a) [1pt] $x^2 \equiv a \pmod{2^2}$,
   (b) [2pt] $x^2 \equiv a \pmod{2^4}$,
   (c) [2pt] $x^2 \equiv a \pmod{2^5}$.

(2) Without actually finding them, determine number of solutions of the congruences
   (a) [2pt] $x^2 \equiv 45 \pmod{76}$,
   (b) [2pt] $x^2 \equiv 45 \pmod{152}$,
   (c) [2pt] $x^2 \equiv 17 \pmod{152}$,
   (d) [2pt] $x^2 \equiv 41 \pmod{152}$,
   (e) [2pt] $x^2 \equiv 9 \pmod{2^{2012}5^{2011}29^{10}}$.

(3) [3pt] (∼9.4.8) Prove in-class theorem about number of solutions of the congruence $x^2 \equiv a \pmod{n}$ for $n > 1$ and $\gcd(a, n) = 1$. (Hint/idea given in class.)

(4) [3pt] Solve the congruence $x^2 \equiv 9 \pmod{2^3 \cdot 5^2 \cdot 7^2}$.

(5) Alice and Bob engage in Blum's remote coin flipping protocol with $n = 7{\cdot}11$.
   (a) [2pt] (16.3.2a) Bob picks a number $x_0 = 13$, computes $13^2 \equiv 15 \pmod{77}$ and sends Alice $a = 15$. Help Alice do her part: find all solutions of the congruence $x^2 \equiv 15 \pmod{77}$.
   (b) [2pt] Assume Alice sends Bob $x_1 = 57$, thus losing the coin toss. Pretending that you don't know primes p, q s.t. $77 = pq$, find p, q using the Euclidean algorithm.

(6) [3pt] What is Alice's chance to win in a variation of Blum's remote coin flipping protocol where $n = pqr$ is used (where p, q, r are distinct odd primes) instead of $n = pq$?