Assignment 11.

This homework is due *Tuesday* April 29.

There are total 31 points in this assignment. 28 points is considered 100%. If you go over 28 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. Quadratic Congruences

(1) (9.4.2) Solve the following congruences:
   (a) [2pt] $x^2 \equiv 14 \pmod{5^3}$.
   (b) [2pt] $x^2 \equiv 2 \pmod{7^3}$.
   (c) [1pt] $x^2 \equiv 3 \pmod{7^3}$.

(2) Without actually finding them, determine the number of solutions of the congruences
   (a) [1pt] $x^2 \equiv 9 \pmod{5^{2013} \cdot 29^{10}}$.
   (b) [1pt] $x^2 \equiv 9 \pmod{4 \cdot 5^{2013} \cdot 29^{10}}$.
   (c) [1pt] $x^2 \equiv 9 \pmod{2^{2014} \cdot 5^{2013} \cdot 29^{10}}$.

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

(4) 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 information that $x_1^2 \equiv x_0^2 \pmod{77}$ and the Euclidean algorithm.

2. Continued fractions

(5) (15.2.1abc) Express each of the rational numbers as finite simple continued fraction:
   (a) [1pt] $-19/51$,
   (b) [1pt] $187/57$,

(6) [3pt] (15.2.8+) If $C_k = p_k/q_k$ is the kth convergent of the simple (finite or infinite) continued fraction $[a_0; a_1, a_2, \ldots]$, establish that

$$q_k \geq 2^{(k-1)/2} \quad \text{for } k \geq 2.$$

(*Hint:* Observe that $q_k = a_k q_{k-1} + q_{k-2} \geq 2q_{k-2}$.)

(7) (a) [1pt] Find $\alpha = [1; \overline{2}]$.
   (b) [1pt] Compute the 0th, 1st,…, 5th convergents of α.
   (c) [1pt] Give a "quadratic" upper bound for the difference between α and the 5th convergent in (a).

— see next page —

(8) [2pt] (15.3.1d) Evaluate $[0; 1, \overline{3, 1}]$. (*Hint:* Start with finding $[\overline{3, 1}]$.)

(9) [3pt] (Part of 15.3.5) For any positive integer n, show that $\sqrt{n^2+1} = [n; \overline{2n}]$.
(*Hint:* Integer part of $\sqrt{n^2+1}$ is n because $(n+1)^2 > n^2+1$. Then notice that
$$n + \sqrt{n^2+1} = 2n + (\sqrt{n^2+1} - n) = 2n + \frac{1}{n + \sqrt{n^2+1}}.)$$

(10) [3pt] Given the infinite continued fraction $\alpha = [1; 2, 3, 4, 5, \ldots]$, find the best rational approximation a/b of α with denominator
(a) $b \leq 30$,
(b) $b \leq 157$