Assignment 3.

This homework is due *Thursday* Feb 9.

There are total 54 points in this assignment. 49 points is considered 100%. If you go over 49 points, you will get over 100% for this homework 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.

Part I

In this part, you are asked to solve problems using Bezout's theorem and Euclidean algorithm, but not unique prime factorization.

(1) (2.3.14+) For any integer a, show the following:

  (a) [2pt] $\gcd(a, 5a+1) = 1$.
  (b) [2pt] $\gcd(2a+1, 9a+4) = 1$.
  (c) [3pt] $\gcd(5a+2, 7a+3) = 1$.

(2) [4pt] If $\gcd(a,b) = 1$, show that $\gcd(2a+b, a+2b) = 1$ or 3.

(3) [4pt] Show that $\gcd(a,b)$ divides $\gcd(a+b, a-b)$. Is it true that always $\gcd(a,b) = \gcd(a+b, a-b)$? (Prove or provide a counter example.)

(4) [2pt] (2.4.1) Use Euclidean algorithm to find $\gcd(143, 227)$, $\gcd(272, 1479)$.

(5) (2.4.2bc) Use the reverse Euclidean algorithm to obtain integers x, y such that:
  (a) [3pt] $\gcd(24, 138) = 24x + 138y$.
  (b) [3pt] $\gcd(119, 272) = 119x + 272y$.

(6) (a) [2pt] (2.3.20(a)) Deduce directly from Bezout's theorem that if $\gcd(a,b) = 1$ and $\gcd(a,c) = 1$, then $\gcd(a, bc) = 1$. (*Hint:* Write $1 = 1 \cdot 1 = (ax+by)(au+cv)$. Expand brackets, combine terms with a and terms with bc.)
  (b) [2pt] Use item (a) to prove that if $\gcd(a,b) = 1$, then $\gcd(a, b^n) = 1$ for all integer $n \geq 1$.
  (c) [2pt] Use items (a) and (b) to prove that if $\gcd(a,b) = 1$, then $\gcd(a^n, b^m) = 1$ for all integer $m, n \geq 1$.

— see next page —

Part II

In this part, you are asked to solve problems using anything covered in class, including unique prime factorization.

(7) (a) [2pt] (3.1.5a) Given that p is a prime and $p \mid a^n$, prove that $p^n \mid a^n$.
(b) [4pt] Let $k > 1$ be an integer. Prove that $\sqrt[k]{n}$ cannot be rational, unless n is a perfect k-th power (i.e. $n = m^k$ for some $m \in \mathbb{Z}$). (*Hint:* If $\frac{a}{b} = \sqrt[k]{n}$, then $a^k = nb^k$. Use (a).)

(8) [2pt] Use the fundamental theorem of arithmetic to prove statement of the problem 6c.

(9) (3.1.3bcd) Prove the following:
(a) [3pt] Any integer of the form $3n + 2$ has a prime factor of this form.
(b) [3pt] The only prime of the form $n^3 - 1$ is 7. (*Hint:* Write $n^3 - 1 = (n - 1)(n^2 + n + 1)$.)
(c) [3pt] The only prime p for which $3p + 1$ is a perfect square is $p = 5$. (*Hint:* Write $3p + 1 = n^2$.)

(10) [4pt] (3.1.8) If $p \geq q \geq 5$ are both primes, prove that $24 \mid p^2 - q^2$. (*Hint:* Show that one of two numbers $p + q, p - q$ is divisible by 4.)

(11) [4pt] Prove that for integer $n > 4$, n is composite if and only if $n \mid (n - 1)!$.