AM 106: Applied Algebra	**Prof. Madhu Sudan**
Problem Set 2	
Assigned: Wed. Sept. 13, 2017	Due: Tue. Sept. 19, 2017 (11:59 PM)

- You may submit your solutions via assignment page on the canvas website of the course.
- For collaboration and late days policy, see course website at `http://madhu.seas.harvard.edu/courses/Fall2017`
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.

Problem 1. (Solving Equations via Euclid)

1. Use the Extended Euclidean Algorithm to compute $\gcd(18900, 17017)$ and express it as an integer linear combination of 18900 and 17017. Show your work.
2. Find an integer solution to the equation $18900x + 17017y = 14$.
3. Provide a general characterization, in terms of the integers a,b, and c, for when there is an integer solution to the equation $ax + by = c$. Prove that your characterization is necessary and sufficient. Explain how it yields a polynomial-time algorithm for determining whether such an equation is solvable and, if so, finding a solution.
4. Prove by induction that if the Euclidean Algorithm makes k divisions when computing $\gcd(x, y)$, where $x > y \geq 1$ and $k \geq 1$, then $x \geq F_{k+2}$, where F_n is the n'th Fibonnaci number as defined on Problem 3 on PS0. Using Problem 3 of PS0, deduce that the number of divisions used when computing the gcd of two n-bit numbers is at most $(\log_\varphi 2) \cdot n \approx 1.44n$. (Note that this improves the bound of $2n$ given in lecture.)

Problem 2. (Groups) Which of the following are groups? For those that are finite groups write a Cayley table. Briefly justify your answers.

1. $\{0, 3, 6, 9\}$ with addition mod 12.
2. $\{1, 3, 5, 7, 9\}$ with multiplication mod 11.
3. The set of polynomials with rational coefficients (e.g. $(8/3)x^3 - 2x + 1/2$), except for the zero polynomial, under polynomial multiplication.
4. The set of maps $T : \mathbb{R}^3 \to \mathbb{R}^3$ such that $\|T(x) - T(y)\| = \|x - y\|$ for all $x, y \in \mathbb{R}^3$, under composition. (For a vector $v = (v_1, v_2, v_3) \in \mathbb{R}^3$, such as $x - y$ or $T(x) - T(y)$, $\|v\|$ denotes its Euclidean length, namely $\|v\| = \sqrt{v_1^2 + v_2^2 + v_3^2}$.) Distance-preserving maps such as these are called *isometries*. You may use, without proof, the fact that isometries of $\mathbb{R}^n$ are always onto (aka surjective).

Problem 3. (Abelian Groups)

1. **Gallian 2.14:** Let G be a group with the following property: Whenever a, b and c belong to G and $ab = ca$, then $b = c$. Prove that G is Abelian.

2. If for all sufficiently large n it is the case that $\forall a, b \in G, (ab)^n = a^n b^n$ then G is abelian. (**Hint:** In particular it suffices for this to hold for any three successive n.)