AM 106: Applied Algebra **Prof. Salil Vadhan**

Problem Set 1

Assigned: Fri. Sept. 14, 2018 Due: Fri. Sept. 21, 2018 (5:00 sharp)

- You must submit your problem sets electronically on the course Canvas site. If you use LaTeX, please submit both the source (`.tex`) and the compiled file (`.pdf`).
- For SAGE problems, also submit a pdf version of your SAGE notebook.
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Please reread the parts of the syllabus about Problem Sets and the Collaboration Policy.

Problem 1. (GCD, 10+1pts)

1. Consider the sequence of fractions $(4n+1)/(6n+1)$ for $n = 1, 2, \ldots$. That is, the sequence $5/7, 9/13, 13/19, \ldots$. Prove that all of these fractions are written in lowest terms. (Hint: GCD is a linear combination.)
2. (Extra Credit) Prove the same for the sequence $(3n+1)/(6n+5)$.

Problem 2. (Equivalence of Induction Axioms, 10pts) Prove that Strong Induction implies the Well-ordering Principle.

Problem 3. (Equivalence Relations, 10pts) Which of the following are equivalence relations? If it is an equivalence relation, describe the equivalence classes. If it is not, which properties fail?

- Domain: Finite subsets of $\mathbb{N}$. Relation: $A \sim B$ if $|A| = |B|$.
- Domain: Functions $h : \mathbb{N} \longrightarrow \mathbb{N}$. Relation: $f \sim g$ if $f(n) = O(g(n))$.
- Domain: The set of positive integers. Relation: $a \sim b$ if ab is a perfect square.
- Domain: $\mathbb{N} = \{0, 1, 2, \ldots\}$. Relation: $a \sim b$ if ab is a perfect square. (We consider 0 to be a perfect square.)

Problem 4. (Modular Exponentiation, 15pts) Follow the instructions at `http://seas.harvard.edu/~salil/am106/fall18/SAGE.html` to create an account for yourself on SAGE and get comfortable using it. Use SAGE to solve this problem and submit a copy of your notebook showing all your work. You should submit an annotated pdf version on Canvas.

- What is the largest value of $n \in \mathbb{N}$ for which you can get SAGE to calculate 3^n?
- Calculate $3^n \bmod 10^6$ for each $n \in \{2^{10} = 1024, 2^{20} = 1048576, 2^{30} = 1073741824, 2^{100}, 2^{100} + 2^{30} + 2^{20} + 2^{10}\}$.
- Calculate $5^n \bmod 11$ for each $n \in \{0, 1, \cdots, 25\}$ (look for a pattern!) and $n = 8^{2^{100}}$.

Problem 5. (Asymptotic Notation, 10pts) True or False? Briefly justify your answers (e.g. in one sentence per part).

- $6n + 1 = O(n)$.
- $n^4 = O(3^n)$.
- $e^n = O\left(n^{\ln n}\right)$.
- $\log_2\left(n^5 + n^2\right) = \Theta\left(\log_2\left(5n^3\right)\right)$.
- $2^{n^5+n^2} = \Omega\left(2^{5n^3}\right)$.