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

Problem Set 2

Assigned: Fri. Sept. 21, 2018 Due: Fri. Sept. 28, 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. (Solving Linear Diophantine Equations, 30pts) It was shown in section that for integers a, b, c, with at least one of a, b nonzero, there is an integer solution (x, y) to the equation $ax + by = c$ if and only if $\gcd(a, b)$ divides c. Moreover a solution can be found in polynomial time using the Extended Euclidean Algorithm. Solve Parts 1 and 4 below in SAGE, using only basic arithmetic (including `a//b` and `a%b` which give the quotient and remainder when dividing integer `a` by integer `b`), control flow (loops, if-then), and variables or arrays, and submit a pdf of your notebook. See the "PS2 Tips" section at `http://seas.harvard.edu/~salil/am106/fall18/SAGE.html` for some more pointers to SAGE features that may be helpful on this problem set.

1. In the year 2020, Mick Fanning made a \$326,712,409 bet against fellow retired surfer Kelly Slater that the young phenom Caroline Marks would beat Slater's record of 11 world championship titles by the year 2040. Marks succeeded in the year 2039, but Fanning and Slater are having a difficulty reconciling their bet because they have put all of their assets into cryptocurrencies, some in Bitcoin and some in Ether. In the year 2039, each Bitcoin is worth \$15,567,679, and each Ether is worth \$8,926,249. Use the Extended Euclidean Algorithm to come up with a way for Fanning and Slater to exactly reconcile their bet by trading integer quantities of their cryptocurrencies. (Your method can involve Fanning giving change back to Slater. You may assume that both Fanning and Slater hold vast amounts of each cryptocurrency.)

2. Prove that, for integers a, b not both 0, the set of all integer solutions (x, y) to the equation $ax + by = 0$ is
$$\{(z \cdot b/\gcd(a, b), -z \cdot a/\gcd(a, b)) : z \in \mathbb{Z}\}.$$
(Hint: as shown in section, an integer is a multiple of both a and b if and only if it is a multiple of $\mathrm{lcm}(a, b) = ab/\gcd(a, b)$.)

3. Let (x_0, y_0) be any solution to the equation $ax + by = c$. Show that the set of all solutions to the equation $ax + by = c$ is

$$\{(x_0 + z \cdot b/\gcd(a,b), y_0 - z \cdot a/\gcd(a,b)) : z \in \mathbb{Z}\}.$$

4. Using Parts 1 and 3, find the exchange of cryptocurrencies between Fanning and Slater that involves Fanning giving the least possible change (in dollar value) back to Slater (even no change, if that's possible).

Problem 2. (Groups, 20pts) Which of the following are groups? For those that are finite groups write a Cayley table. Briefly justify your answers.

1. $\{1, 4, 13, 16\}$ with multiplication modulo 17.
2. $\{0, 3, 6, 9, 12\}$ with addition modulo 13.
3. The set of polynomials $a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ of degree at most 5 with integer coefficients (e.g. $8x^4 - 3x^3 + 1$), under polynomial addition.
4. Powers of 2 $\{1, 2, 4, 8, \ldots\}$ under multiplication.
5. The set of *derangements* on 5 elements, namely $\{\pi \in S_5 : \forall i \in [5]\pi(i) \neq i\}$. Operation: composition.
6. Set of affine-linear functions $f(x) = ax + b$ with $a \in \mathbb{Q} - \{0\}$ and $b \in \mathbb{Q}$. Operation: composition.

Problem 3. (Removing uninvertible elements suffices, 10pts) Suppose a set H has a binary operation that satisfies closure and associativity and has an identity e. Let G be the subset of H consisting of all elements that have an inverse, i.e. $G = \{a \in H : \exists b \in H \; ab = ba = e\}$. Prove that G is a group (under the same binary operation).