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

Problem Set 3

Assigned: Fri. Oct. 5, 2018 Due: Fri. Oct. 12, 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. (Subgroups) Draw the subgroup lattice for each of the following groups. Identify which subgroups are cyclic and write all of the generators for those subgroups.

1. $\mathbb{Z}_{18}$
2. $\mathbb{Z}_{19}^*$.
3. $\mathbb{Z}_{20}^*$.
4. D_5. (Please use the Rot_k and Ref_k notation for elements of D_n from lecture.)

Problem 2. (Subgroups) Let H and K be subgroups of a group G.

1. Show that $H \cap K$ is also subgroup of G.
2. Show that $H \cup K$ is *not* a subgroup unless $H \subseteq K$ or $K \subseteq H$. (Hint: if $H \nsubseteq K$ and $K \nsubseteq H$, then there is an element $h \in H - K$ and an element $k \in K - H$.)

Problem 3. (Orders of Permutations) What are all the possible orders for elements of S_8 and of A_8? Justify your answers.

Problem 4. (Breaking El Gamal when the Group Size has Small Factors) Let $G = \langle g \rangle$ be a cyclic group of order q, let d be a divisor of q, and let $H = \langle g^d \rangle$ be the cyclic subgroup of G of order q/d.

1. For an element a of G, prove that $a \in H$ if and only if $a^{q/d} = e$. Thus, one can efficiently test whether a is in H by exponentiation.
2. Let $a = g^x$ be a public key for the El Gamal encryption scheme, and let $(b, c) = (g^y, a^y \cdot m)$ be an encryption of message $m \in G$. Show that if either $a \in H$ or $b \in H$, then $m \in H \Leftrightarrow c \in H$.

3. Eve really wants to find out the secret surfing spot frequented by her neighbor Alice and Alice's surfing partner Bob. She would follow them to the spot, but surf days are unpredictable in New England and when they go, they always leave home ridiculously early in the morning (4am for "dawn patrol"). Alice pulling her car out of the driveway always wakes Eve up, but not soon enough for Eve to catch up. Then Eve realizes that Bob, who is a skilled surf forecaster, must be telling Alice every night whether or not they are going to go surfing the next morning. So she starts monitoring their internet communications, which unfortunately are encrypted using the El Gamal encryption scheme.

   Eve looks up their El Gamal group $G = \langle g \rangle$ which is a subgroup of $\mathbb{Z}_p^*$ of order $q = (p-1)/2$ generated by $g \in \mathbb{Z}_p^*$, and Alice's public key $a \in G$. Every night Eve collects the ciphertext (b_i, c_i) sent from Bob to Alice $(i = 0, 1, 2, \ldots)$. For the first 10 nights, Eve is just in observation mode, collecting the ciphertexts and seeing which mornings she is awakened by Alice pulling out of her driveway for surfing. She is awakened on the mornings after nights 3, 7, and 8. Then, using her knowledge of the theory of cyclic groups from AM106, Eve feels equipped to break their encryption and determine one of the surfing mornings in advance.

   Your task is to come up with and carry out this attack for Eve in SAGE. By following the PS3 Tips instructions in `http://seas.harvard.edu/~salil/am106/fall18/SAGE.html`, variables will be assigned with all of the data you need. The variables `p`, `g`, and `a` contain the prime p, the generator g, and Alice's public key a. The lists `b` and `c` contain the elements of the ciphertexts for the first 30 nights. Using Parts 1 and 2 and the fact that Alice and Bob go surfing only after nights 3, 7, and 8 out of nights 0—9, find at least one other night that Alice and Bob will go surfing the next morning. You may assume that Bob always sends the same message m_0 when they are going to go surfing and the same message m_1 when they are not going to go.

4. Why would the above kind of attack be unlikely to succeed if q had only large factors (e.g. d had more than 100 digits)? (There are at least two different reasons.)