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

Problem Set 5

Assigned: Fri. Oct. 18, 2018 Due: Fri. Oct. 25, 2018 (11:59pm sharp)

Problem 1. (Classification of Abelian Groups, 15 pts) Determine which of the following groups are isomorphic to each other:

1. $\mathbb{Z}_{36}$.
2. $\mathbb{Z}_4 \times \mathbb{Z}_9$.
3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$.
4. $\mathbb{Z}_{74}^*$.
5. $\mathbb{Z}_{76}^*$.

Problem 2. (Normal Subgroups and Factor Groups, 12 pts)

1. Recall from Problem 2 on Problem Set 4 the subgroup $S^1 = \{a + bi | a^2 + b^2 = 1\} \leq \mathbb{C}^*$. Is S^1 normal in $\mathbb{C}^*$? If so, determine the factor group $\mathbb{C}^*/S^1$.
2. Find all normal subgroups H of S_3. For each, determine the factor group S_3/H.

Above "determine the factor group" means identify a familiar group that is isomorphic to G/H (and justify that it is isomorphic).

Problem 3. (Orders in Factor Groups, 12 pts)

1. Find all elements of order 10 in $\mathbb{Q}/\mathbb{Z}$.
2. Show that if H is a finite, normal subgroup of G, and aH has order k in G/H, then a has order kd in G for some divisor d of $|H|$. (Hint: consider $a^{k|H|}$.)

Problem 4. (Decryption in the Rabin cryptosystem, 21 pts) For an abelian group G, let $\mathrm{QR}(G) = \{x^2 : x \in G\}$ denote the subgroup of G consisting of the set of squares in G. The notation $\mathrm{QR}(G)$ comes from the fact that the elements of $\mathrm{QR}(\mathbb{Z}_N^*)$ are also known as "quadratic residues" modulo N.

1. If $N = pq$ with $\gcd(p, q) = 1$, prove that $\mathrm{QR}(\mathbb{Z}_N^*) \cong \mathrm{QR}(\mathbb{Z}_p^*) \times \mathrm{QR}(\mathbb{Z}_q^*)$.
2. Let r be a positive integer such that $r \equiv 2 \pmod 4$. (That is, r is even, but $r/2$ is odd.) Prove that if G is a cyclic group of order r, then for every element $y \in \mathrm{QR}(G)$, it holds that $z = y^{(r+2)/4} \in \mathrm{QR}(G)$ and $z^2 = y$. That is, every square in G has a square root that is also a square, and we can find it by raising to the power $(r + 2)/4$. (The result of Problem 4.1 on Problem Set 3 may be helpful.)

3. After Eve successfully followed Alice and Bob to their secret surfing spot (Problem 4 on Problem Set 3) and proved that she was not a kook by shredding double-overhead waves, Alice and Bob invited her to join them on their regular sessions. Because of their failure to use El Gamal encryption correctly, they decide to switch to the Rabin cryptosystem (invented by Michael Rabin, now emeritus professor at Harvard). Eve's private key in the Rabin cryptosystem (Blum–Williams variant) is a pair of large primes p and q such that $p \equiv q \equiv 3 \pmod 4$, and her public key is $N = pq$. To tell Eve that a surf session is on, Bob constructs a ciphertext c by choosing a random element $x \in \mathrm{QR}(\mathbb{Z}_N^*)$ such that the least-significant bit of x is 1, and setting $c = x^2 \pmod N$. (That is, when viewed as an integer in the set $\{0, 1, \ldots, N-1\}$, x is an odd number.) To tell Eve that a surf session is off, Bob instead chooses a random $x \in \mathrm{QR}(Z_N^*)$ with least-significant bit 0, and sets $c = x^2 \pmod N$.

   Your task is to use Parts 1 and 2 and SAGE to help Eve decrypt Bob's ciphertexts for the first week (nights/mornings 0–7) and figure out which mornings she needs to wake up early to go surfing. By following the PS5 Tips in `http://seas.harvard.edu/~salil/am106/fall18/SAGE.html`, the variables `p` and `q` will be assigned with Eve's private key, and the list `c` will contain the ciphertexts for the first week. In addition to commands you have used on previous problem sets, here you may also use SAGE's command for the Extended Euclidean Algorithm (namely, `xgcd`).

   As you will see, decryption is possible given the factorization of N, which Eve possesses but is conjectured to be infeasible to compute for an adversary who only has access to the public key N. Remarkably, it can be proven that factoring N is the *only* way to break this encryption scheme: any procedure that distinguishes the two types of encryptions (least-significant bit 0 or 1) with nonnegligible probability can be used to factor N in polynomial time!