6.S096: Number Theory	Due: January 29, 2024

Problem Set 2— Arithmetic and Group Theory

A. Anas Chentouf, M. Wacyl Meddour, Mohammed Ali Othman *Scribe:*

Instructions: Solve any combination of problems 1-6 that sums to 93 points, then complete the survey problem 0 (worth 7 points), whose results will help shape future problem sets and lectures.

For full score, you will have to solve problem 1, two of problems 2-4, and one of problem 5-6, and finally, the survey problem.

Collaboration is allowed (in fact, encouraged), but please list your sources and collaborators. If there are none write "**Sources consulted: none**" at the top of your solutions. Note that each student is expected to write their own solutions; it is fine to discuss the problems with others, but your writing must be your own.

The first person to report each non-trivial typo/error in any of the problem sets or lecture notes will receive 1-5 points of extra credit (depending on the severity).

Problem 1. Properties in Group Theory (10 points)

Let G_1, G_2 be groups and $\phi : G_1 \to G_2$ be a group homomoprhism. Let m be your MIT ID. Prove parts

$$\{2^{m+i} \bmod 13 : 0 \leq i \leq 5\}$$

of this problem.

1. The identity element of G_1 is unique.
2. If $xy = xz$ for elements $x, y, z \in G_1$, then $y = z$.
3. The relation $(xy)^{-1} = y^{-1}x^{-1}$ holds for all $x, y \in G_1$.
4. G_1 has at least two subgroups, $\{e_{G_1}\}$ and G_1 itself. itself. [1]
5. If $H \leq G_1$ and $x \in H$, then $\langle x \rangle \leq H$.
6. The product (G_1, G_2) under the operation $(*, *')$ is also a group.
7. The intersection of two subgroups of G is also a subgroup of G. Is the same true for the union?

[1] Groups with only these two subgroups are called *simple*, and can be thought of as building blocks of groups. Does this remind you of anything?

8. Let x be an element of a group G. The maps $\phi_g : G \to G$ sending $x \mapsto gx$ and $\phi^g : G \to G$ sending $x \mapsto xg$ are bijections.

9. If $x_1, \cdots x_n$ are elements of G_1 then $\phi(x_1 \cdots x_n) = \phi(x_1) \cdots \phi(x_n)$.[2]

10. The homomorphism sends the identity element to the identity element $\phi(e_{G_1}) = e_{G_2}$.

11. The homomorphism respects inversion:

$$\phi(x^{-1}) = \phi(x)^{-1}.$$

12. The kernel and the image are subgroups of G_1 and G_2, respectively.

[2] Here, $x_1 \cdots x_n$ is the product under the G_1 group operation and $\phi(x_1) \cdots \phi(x_n)$ is the product under the G_2 group operation.

Problem 2. Results about Groups (24 points)

This is a collection of results in elementary group theory.

1. Let x, y be elements of a group G. Show that xy and yx have the same order in G.

2. Let H be a subgroup of G, and let $g \in G$. If $|g| = n$ and $g^m \in H$ where n and m are co-prime integers, then show that $g \in H$.

3. Let a and b be elements of a group G. Assume that a has order 7 and that $a^3 b = ba^3$. Prove that $ab = ba$.

4. An nth root of unity is a complex number z such that $z^n = 1$. Prove that the n th roots of unity form a cyclic subgroup of the multiplicative complex numbers of order n.

5. Determine the product of all the nth roots of unity. ‘

6. Let G be an abelian group written multiplicatively. Show that in any finite group
$$\prod_{g \in G} g^2 = 1.$$
   We have just generalized Wilson's theorem.

Problem 3. Quadratic Residues (24 points)

Let p be an odd prime.

1. Prove that there exists a prime less than p which is a quadratic nonresidue modulo p. That is, there exists q such that $\left(\frac{q}{p}\right) = -1$.

2. Show that the smallest quadratic nonresidue modulo p (when considered in the set $\{1, \cdots, p-1\}$) must be a prime.

In fact, we will now prove that this q can be chosen to be less than $\sqrt{p} + 1$.

3. Consider the smallest quadratic nonresidue r and suppose for the sake of contradiction that $r \geq \sqrt{p}+1$. Notice this means that $r \cdot (r-1) > (r-1)^2 \geq p$. Now consider the following numbers $\{r, 2r, \cdots, (r-1)r\}$

   We know that the first number r is less than p and that the last number in the set $(r-1)r$ is greater than p. Let a be the smallest positive integer such that $ra > p$, which is the same as saying $r(a-1) < p < ra$.

   Think of two different ways of finding the Legendre symbol $\left(\frac{ra}{p}\right)$ and arrive at a contradiction.

Problem 4. Modular Arithmetic (24 points)

Let p be a prime and let q be a prime that divides $p-1$.

1. Let $a \in \mathbb{F}_p^*$ and let $b = a^{(p-1)/q}$. Prove that either $b = 1$ or else b has order q.

2. Suppose that we want to find an element of $\mathbb{F}_p^*$ of order q. Using part (a), we can randomly choose a value of $a \in \mathbb{F}_p^*$ and check whether $b = a^{(p-1)/q}$ satisfies $b \neq 1$. How likely are we to succeed? In other words, compute the value of the ratio

$$\frac{\#\{a \in \mathbb{F}_p : a^{(p-1)/q} \neq 1\}}{\#\mathbb{F}_p^\times}.$$

3. Let p be a prime such that $q = \frac{1}{2}(p-1)$ is also prime. Suppose that g is an integer satisfying $g \not\equiv \pm 1 \pmod{p}$ and $g^q \not\equiv 1 \pmod{p}$. Prove that g is a primitive root modulo p.

Problem 5. Some Cryptography (35 points)

Alice and Bob create a symmetric cipher as follows. Their private key k is a large integer and their messages (plaintexts) are d-digit integers $M = \{m \in \mathbb{Z} : 0 \leq m < 10^d\}$. To encrypt a message, Alice computes α as the square root of k to d decimal places, throws away the part to the left of the decimal point, and keeps the remaining d digits. Let α be this d-digit number. (For example, if $k = 87$ and $d = 6$, then $\alpha = 327379$.)

Alice encrypts a message m as

$$c \equiv m + \alpha \pmod{10^d}.$$

Since Bob knows k, he can also find α, and then he decrypts c by computing $m \equiv c - \alpha \pmod{10^d}$.

1. Alice and Bob choose the secret key $k = 11$ and use it to encrypt 6-digit integers (i.e., $d = 6$). Bob wants to send Alice the message $m = 328973$. What is the ciphertext that he sends?

2. Alice and Bob use the secret key $k = 23$ and use it to encrypt 8-digit integers. Alice receives the ciphertext $c = 78183903$. What is the plaintext m?

3. Show that the number α used for encryption and decryption is given by the formula
$$\alpha = \lfloor 10^d(\sqrt{k} - \lfloor \sqrt{k} \rfloor) \rfloor,$$
where $\lfloor t \rfloor$ denotes the greatest integer that is less than or equal to t.

4. (**Bonus Problem**: 10 points) If Eve steals a plaintext/ciphertext pair (m, c), then it is clear that she can recover the number α, since $\alpha \equiv c - m \pmod{10^d}$. If 10^d is large compared to k, can she also recover the number k? This might be useful, for example, if Alice and Bob use some of the other digits of subsequent messages.

5. Alejandro and Bilal use a different cryptosystem - one in which their private key is a (large) prime k and their plaintexts and ciphertexts are integers. Bilal encrypts a message m by computing the product c = km. Eve intercepts the following two ciphertexts: $c_1 = 12849217045006222$ and $c_2 = 6485880443666222$. Find Bilal and Alejandro's private key.

Problem 6. Birthday Attacks against Discrete Logarithms (35 points)

1. Assuming no leap years and uniform distribution of birthdays, as well as independence. Prove that in a room of 23 people, there exists at least 2 with the same birthday with a probabibility greater than 50%.

2. Generalize this by computing $P(N, k)$ that exact probability that at least one collision occurs when N elements are uniformly and independently distributed across k bins. [3] You may assume that $N \leq k$.

   In the following parts, you may find it useful to use the fact that

   $$(1 - e^{-1})x \leq 1 - e^{-}x \leq x$$

   when $x \in [0, 1]$.

3. Show that this probability can can bounded as

   $$1 - \exp\left(\frac{-N(N-1)}{2k}\right) \leq P(N, k) \leq \frac{N(N-1)}{2k}.$$

4. By slightly adjusting your estimate, show that when $N \leq \sqrt{2k}$, we have that

   $$P(N, k) \geq (1 - e^{-1})\frac{N(N-1)}{2k}.$$

5. Implement this birthday attack against the discrete logarithm. That is, write a program which, given a prime p, some primitive root g modulo p and a value y, finds the discrete logarithm x such that $g^x \equiv y \pmod{p}$, assuming that x is small (at most 45 bits). [4]

   Use $g = 3, p = 1223439062505387810550553$, and $y = 928594445087275299406553$.

[3] So the previous problem would be with $N = 23$ people distributed across $k - 365$ bins.

[4] This assumption is important and crucial.

Problem 0. Survey (7 points)

Complete the following survey by rating each of the problems you solved on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind numbing," 10 = "mind blowing"), and how difficult you found the problem (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour. [5]

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			
Problem 4			
Problem 5			
Problem 6			

Please rate each of the following lectures/sessions that you attended on a scale of 1 to 10, according to the quality of the material (1="pointless", 10="priceless"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="watching paint dry", 10="head still spinning"), and the novelty of the material (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
01/23	Quadratic Residues and Primitive Roots				
01/24	Group Theory				
01/25	More Group Theory/Cryptography				

Feel free to record any additional comments you have on the problem sets or lectures; in particular, how you think they could be improved (which they surely can!).

[5] This survey, as well the template of the Pset, is copied from Andrew Sutherland's 18.783 problem sets.