6.S096: Number Theory Due: January 21, 2024

Problem Set 1— Intro to Arithmetic

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

Instructions: Solve any combination of problems 1-5 that sums to 90 points, then complete the survey problem 0 (worth 10 points), whose results will help shape future problem sets and lectures.

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: GCD and LCM (30 points)

Given two integers a and b, define their least common multiple $\operatorname{lcm}(a, b)$ as the smallest non-negative integer who is a multiple of both a and b.

1. Suppose $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ where p_i is a prime and $\alpha_i, \beta_i \geq 0$ are integers. Show that $\operatorname{lcm}(a, b) = \displaystyle\prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$.
2. Using the similar formula for the greatest common divisor, deduce that:
$$\gcd(a, b) \operatorname{lcm}(a, b) = ab.$$
3. Find the greatest common divisor of $24! + 23$ and $23! + 23$. Can you generalize your result to compute $\gcd((p+1)! + p, p! + p)$ for any prime p ?

Problem 2: Multiplicative Orders (30 points)

1. Let $p \geq 5$ be a prime and let x be an integer. Knowing that $p | x^2 + x + 1$, compute $\operatorname{ord}_p(x)$ the order of x mod p.
Can you find the possible values of $p \mod 6$?
2. Compute $\gcd(3^{k+1}, 2^{3^k} - 1)$.
3. Deduce that $3^{k+1} | 2^{3^k} + 1$.
4. Argue that $3^{k+2} \nmid 2^{3^k} + 1$.

5. Show that $n|\varphi(a^n - 1)$ for positive integers n and a (where $a > 1$)

Problem 3: (Binary) Exponentiation (30 points)

1. Using Euler's Theorem, compute the last two digits of 3^{1363} and 3^{10845}.

2. Implement, on code, a program to compute the last digit of 3^x given an arbitrary positive integer x. Use this to verify your answer for the previous subproblem.

   Update: Nothing is being asked in 3.3.

3. Assume that we have an oracle which allows us to input two elements modulo p and obtain their product, modulo p.

   Henceforth, let us focus on the case of calculating $3^n \bmod p$ for some prime $p \geq 5$. One can can compute this use n multiplications modulo p, by simply storing $3^m \bmod p$ and recurseively multiplying it by 3 using the oracle to get $3^{m+1} \bmod p$.

4. Prove that it is possible to do compute $3^n \bmod p$ using only $O(\log_2 n)$ oracle calls. Exactly how many oracle calls are you using.

   Hint: One can go from $3^{2^i} \bmod p$ to $3^{2^{i+1}} \bmod p$ using one oracle call. How can you combine those?

5. Implement your algorithm from the previous part.

   Using Sage (or other software if you prefer), choose a 256-bit prime number p. Next, let m be a random permutation of the digits of your MIT ID.

   Using this, compute $3^m \bmod p$, and report the running time of your algorithm.

Problem 4: Dirichlet's Theorem (30 points)

1. Imitating Euclid's proof of infinitude of primes, prove that there exists infinitely many primes of the form $4n + 1$. where $n \in \mathbb{N}$.

2. Using a similar idea, show that there are infinitely many primes of the form $4n + 3$, where $n \in \mathbb{N}$.

3. Let p be a prime number. Prove that for all k, there exists a prime divisor q of $p^{p^k} - 1$ which satisfies $q \equiv 1 \bmod p^k$. Conclude that there are infinitely many primes of the form $pn + 1$. [1]

[1] We did not intend a Euclidean-style proof for part (3). However, it is possible to obtain the same conclusion using a Euclidean-style proof. You can also do that instead for this subproblem.

4. Formulate [2] a "conjecture" about the distribution of primes across different residue classes modulo q. That is, conjecture a relationship between $\pi_{a,q}(x) = \#\{p \leq x : p \equiv a \bmod q\}$ and $\pi(x) = \#\{p \leq x\}$.

   Let q be the first four digits of your MIT ID, and choose $a = 1$. Verify the conjecture in thie case up to $n = 10^2, 10^6$, and 10^8, and calculate the error between your prediction for $\pi_{a,q}(x)$ and $\pi(x)$.

It turns out that there are infinitely many primes of the form $an + b$ where $a, b > 0$ are positive integers for which $\gcd(a, b) = 1$. This result is known as Dirichlet's Theorem and, despite being easy to state, is not at all elementary.

Problem 5: Euclidean Algorithm (30 points)

1. Show for positive integers m, n and $x > 1$ that

$$\gcd(x^m - 1, x^n - 1) = x^{\gcd(m,n)} - 1.$$

2. Show that Fibonacci numbers achieve the worst-case of the Euclidean algorithm. That is, if calculating $\gcd(a, b)$ takes at least n steps for some $a > b > 0$, then $a \geq F_{n+2}$ and $b \geq F_{n+1}$. Here, we define the Fibonacci sequence using the recurion $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$, where $F_0 = 0$ and F_1. [3]

3. Let a, b be nonnegative integers. Show that the Euclidean algorithm can compute $\gcd(a, b)$ in $O(\log b)$ steps. [4]

4. Implement the Euclidean algorithm, and use it to report the greatest common divisor of two randomly chosen integers in the interval $[2^{128}, 2^{129})$. Report the running time of your method, averaged over 10 trials.

   Bonus (10 points): Show that the "probability" that two integers, chosen at random, are coprime is exactly $\frac{6}{\pi^2} = \left(\sum_{n\geq 1} n^{-2}\right)^{-1}$.

[2] you may use Sage

[3] Hint: Use induction

[4] This can be proven directly, but it can also follow from the previous step.

Problem 0. Survey (10 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			

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
01/16	Intro to Arithmetic				
01/17	Euler and Fermat's Theorem				
01/18	More Elementary Number Theory				

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.