COL202: Discrete Mathematical Structures. II semester, 2024-25.
Amitabha Bagchi
Tutorial Sheet 11: Introductory Number Theory.
17 April 2025

Important: The question marked with a ♠ is this week's quiz. The start time for the quiz is 1PM and the end time for the quiz is 1:12PM. Questions marked with a * may be a little harder and can be considered optional.

Problem 1
Given integers a, b with $b > 0$ prove (by Well Ordering or otherwise) that there exist q, r such that $a = bq + r$ and $0 \leq r < b$. Further, argue that q and r are unique.

Problem 2 [Shoup08, Prob. 1.2]
Suppose that n is a composite number (i.e. not a prime). Show that there is a prime $p \leq \sqrt{n}$ such that $p \mid n$.

Problem 3 [LLM18, Prob. 9.2]
Show that $2^{k-1}(2^k - 1)$ is a perfect number (i.e. it is the sum of its factors) if $2^k - 1$ is a prime. Discuss what the issues might be in $2^k - 1$ is not a prime.

Problem 4 [LLM18, Prob. 9.5]
Show that for any two integers a, b, $\gcd(a^5, b^5) = (\gcd(a, b))^5$.

Problem 5 [LLM18, Prob. 9.6]
Prove that $\gcd(a, b)$ is the minimum positive value of any integer linear combination of integers a, b.

Problem 6 [Shoup08, Prob. 1.17]
Let a, b, c be positive integers with $\gcd(a, b) = 1$ and $c \geq (a - 1)(b - 1)$. Show that there exist non-negative integers s, t such that $c = as + bt$.

Problem 7 ♠ [Shoup08, Prob. 1.19]
Suppose $\{a_1, \ldots, a_k\}$ is a relatively prime family of integers (i.e., $\gcd(a_i, a_j) = 1$ for all $i \neq j$) and there is an n such that $\forall i : a_i \mid n$, show that $\prod_{i=1}^{k} a_i \mid n$.

Problem 8 [Shoup08, Prob. 1.28]
Show that for every positive integer k there exist k consecutive composite numbers, i.e., there are arbitrarily large gaps between primes.

Problem 9 [LLM18, Prob. 9.14]
In Euclid's GCD algorithm there is a "Euclidean state machine" that undertakes transitions of the form

$$(x, y) \to (y, \mathrm{rem}(x, y))$$

for $y > 0$. Prove that the smallest positive integers $a \geq b$ for which this machine will have exactly n transitions till it reaches the end are $F(n + 1)$ and $F(n)$ where $F(k)$ is the kth Fibonacci number.

References

[LLM18] E. Lehman, F. T. Leighton, and A. R. Meyer. Mathematics for Computer Science, June 2018, MIT Open Courseware.

[Shoup08] Victor Shoup, A Computational Introduction to Number Theory and Algebra Version 2.1 2008.