Number Theory: Group Work

COSC 290: Discrete Structures
Spring 2026
Prof. Forrest Davis

February 19, 2026

Working with a small group, complete the following proofs on a (part of a) whiteboard. Before attempting a proof work through one example with actual values so you can see if the claim holds in one case and what exactly the claim is. Start with the first one, then you can do the rest in any order. Note, there are 6 problems total (flip the page around).

1. Prove the following claim directly from the definition of divides (i.e., do not use facts about divides proved in the book). Use a direct proof.

   Claim: For any integers p, q, and r, where p is non-zero, if $p|3q$ and $3q|r$, then $p|3q+r$.

2. Prove the following claim:

   Claim: $\gcd(a,b) = \gcd(b,r)$ where r is the remainder of a mod b (i.e., $a = qb + r$)

   You may find it helpful to first prove the following claims, and then use them to prove the main claim above.

   Claim 2a: If $x|y$ and $x|z$, then $x|\gcd(y,z)$

   Claim 2b: Let n and m be positive integers, then $n|m$ and $m|n$ if and only if $n = m$

   Claim 2c: If $d|x$ and $d|y$ then $d|x - ky$ for any integer k

   Claim 2d: If $d|x$ and $d|y$ then $d|kx + y$ for any integer k

We are in effect trying to prove part of the correctness of Euclid's Algorithm. For this formulation, we are assuming a slightly different version of the algorithm, copied below.

Euclidean Algorithm
Input: Two positive integers, a and b.
Output: $\gcd(a,b)$

(a) if $a < b$, then swap swap a and b

(b) if $b|a$, return b

(c) else return $\gcd(b, a \bmod b)$

3. Consider the following definition for congruence mod m. For any integers x and y and any positive integer m, $x \equiv y \pmod{m}$ if there is an integer k such that $x = y + km$. Using this definition, prove the following claim:

   Claim: For all integers a, b, c, p, q where p and q are positive, if $a \equiv b \pmod{p}$ and $c \equiv b \pmod{q}$ and $q|p$, then $a - 2c \equiv (-b) \pmod{q}$.

4. Prove or disprove:

   Claim: For all positive integers, a, b, c if $a|bc$, then $a|b$ or $a|c$.

5. Use proof by contrapositive to prove the following claim:

   Claim: For all integers a and b, if $3a - 5b = 27$, then $\gcd(a,b) \neq 13$

Work directly from definitions. Don't use facts we have proved about divisibility.

6. Flour and Salt offered free bagels for people in COSC 290. The shop claimed that they gave out a total of $n^2 + 9n - 2$ bagels (weird math flex by Flour and Salt . . .). 11 men and n women get bagels and each person was given the same number of bagels.

   (a) Is there a solution to this problem for which $n \leq 11$?

   (b) Is there a solution when $n > 11$?

   For each part, prove or disprove the claim. You can use simple facts about divisibility (e.g., if $a|b$ and $a|c$ then $a|(b + c)$ which you should have seen in the book).