Math 5248: Homework 3

Matthew Pipes

February 5, 2026

Goal Utilization

In this assignment, I completed the following goals:

- **Problem 1:** I used Bezout's Identity clearly and correctly in a proof.
- **Problem 2:** I used Euclid's Lemma clearly and correctly in a proof.
- **Problem 2:** I clearly computed computational solutions so that another student from the class could follow my work.

Problem 1: Bezout's Identity

Proof. Given a and c are coprime, and b and c are coprime, and all are non-zero, we know by Bezout's identity that there exist integers x, x', y, y' such that

$$ax + cy = 1 \quad \text{and} \quad bx' + cy' = 1.$$

Multiplying these equations yields:

$$\begin{gathered}(ax + cy)(bx' + cy') = 1 \cdot 1 \\ abxx' + acxy' + bcyx' + c^2yy' = 1 \\ (ab)\underbrace{xx'}_{X} + c(\underbrace{axy' + byx' + cyy'}_{Y}) = 1 \\ (ab)X + cY = 1\end{gathered}$$

Where X, Y are integers. Then, by Bezout's identity, $\gcd(ab, c) = 1$ and thus ab and c are coprime, as desired. $\square$

Problem 2(a): Peer Review Problem and Euclid's Lemma

Proof: Suppose that p is a prime number and b is an integer. Let a_1 and a_2 be two integers that are solutions to the congruence $x^2 \equiv b \pmod{p}$. By the definition of these solutions, we have:

$$a_1^2 \equiv b \pmod{p} \quad \text{and} \quad a_2^2 \equiv b \pmod{p}$$

Since both a_1^2 and a_2^2 are congruent to b modulo p, they must be congruent to each other:

$$a_1^2 \equiv a_2^2 \pmod{p}$$

Putting the congruence into standard division form yields:

$$p \mid (a_1^2 - a_2^2)$$

which can be factored as:

$$p \mid (a_1 - a_2)(a_1 + a_2)$$

Since p is prime, we apply Euclid's Lemma:

$$p \mid (a_1 - a_2) \quad \text{or} \quad p \mid (a_1 + a_2)$$

Transforming these divisibility statements back into congruence form yields:

$$a_1 - a_2 \equiv 0 \pmod{p} \quad \text{or} \quad a_1 + a_2 \equiv 0 \pmod{p}$$

By adding the appropriate terms to both sides of the congruences, we arrive at the desired conclusion:

$$a_1 \equiv a_2 \pmod{p} \quad \text{or} \quad a_1 \equiv -a_2 \pmod{p}$$

This completes the proof. $\square$

Problem 2(b): Peer Review Problem, Counterexample

Working toward a counterexample for m, b, a_1, a_2, let's first focus on the use of Euclid's Lemma in our prior proof. We had:

$$p \mid (a_1 - a_2)(a_1 + a_2) \implies p \mid (a_1 - a_2) \text{ or } p \mid (a_1 + a_2)$$

Note now that our modulus m is not prime and $m > 0$. Thus, Euclid's Lemma no longer holds. We have:

$$m \mid (a_1 - a_2)(a_1 + a_2)$$

Consider quickly the definition of divisibility that yields:

$$(a_1 + a_2)(a_1 - a_2) = mk \text{ for some } k \in \mathbb{Z}$$

Let $k = 1$, then the prime factorization of m can then be written as $m = (a_1 + a_2)(a_1 - a_2)$.

Now, looking to find these factors, without loss of generality, consider the result if $a_1 + a_2 = m$, and $a_1 - a_2 = 1$ We know:

$$\begin{aligned} m &\equiv 0 \pmod{m} \\ a_1 + a_2 &\equiv 0 \pmod{m} \\ a_1 &\equiv -a_2 \pmod{m} \end{aligned}$$

This simplifies to a result we are trying to avoid. Thus, we must have $m \nmid (a_1 + a_2)$ and $m \nmid (a_1 - a_2)$, **but** we must have that $m \mid (a_1 + a_2)(a_1 - a_2)$.

Consider $m = 12$, $a_1 = 4$, and $a_2 = 2$. We then check:

- $m \nmid (a_1 + a_2) \implies 12 \nmid 6$
- $m \nmid (a_1 - a_2) \implies 12 \nmid 2$
- $m \mid (a_1 + a_2)(a_1 - a_2) \implies 12 \mid (6)(2) \implies 12 \mid 12$

We have found values for m, a_1, and a_2. To find b, we consider the division algorithm for a_1 and a_2:

$$\begin{gathered} a_1^2 = 4^2 = 16 = 12(1) + 4 \\ a_2^2 = 2^2 = 4 = 12(0) + 4 \end{gathered}$$

In both cases, we have that the remainder is 4. Thus, we let $b = 4$, completing our counterexample.

Problem 3: IndCo

Lets first derive the formula for $IndCo$:

$$IndCo = \sum_{i=1}^{4} \frac{k_i(k_i - 1)}{n(n-1)}$$

Where:

$i = \{1 : \text{Spade}, 2 : \text{Heart}, 3 : \text{Diamond}, 4 : \text{Club}\}$

k_i: The number of cards in that suit.

$n = \sum_{i=1}^{4} k_i = \text{total number of cards.}$

To find the probability of picking 2 cards of the same suit consecutively from the deck, we:

Find the total ways to pick 2 cards from the same suit i: $\binom{k_i}{2}$

Divide by ways to pick 2 cards from the deck: $\binom{n}{2}$

Thus, the probability of choosing 2 of the same suit i is:

$$\frac{\binom{k_i}{2}}{\binom{n}{2}} = \frac{\frac{k_i!}{2!(k_i-2)!}}{\frac{n!}{2!(n-2)!}} = \frac{k_i(k_i-1)}{n(n-1)}$$

Then the total probability of drawing 2 cards from all of the suits is the summation:

$$IndCo = \sum_{i=1}^{4} \frac{k_i(k_i - 1)}{n(n-1)}$$