Math 581: Homework 3
Due: Friday, May 7th

1 (10 pts)) We will prove that when working with integers, the Euclidean Algorithm will always produce the GCD of two numbers.

(a) Prove that the remainders found in the Euclidean Algorithm form a decreasing sequence.

(b) Prove that this sequence must terminate with a final remainder of zero.

(c) Proceed by induction on the number of steps in the Euclidean Algorithm. If there are two steps:

$$\begin{aligned} a &= b \cdot q_1 + g \\ b &= g \cdot q_2 + 0 \end{aligned}$$

Prove that any divisor of both a and b is necessarily a divisor of g. Explain why this proves that $g = (a, b)$.

(d) Now suppose that any time we have $n + 1$ equations:

$$\begin{aligned} a &= b \cdot q_1 + r_1 \\ b &= r_1 \cdot q_2 + r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} \cdot q_n + r_n \\ r_{n-1} &= r_n \cdot q_{n+1} + 0 \end{aligned}$$

that $r_n = (a, b)$. Prove that when we have $n + 2$ equations, $r_{n+1} = (a, b)$.

(e) Explain how we have proved that when working with integers, the Euclidean Algorithm will always produce the GCD of two numbers.

2) The Lennox Theater charges \$12.00 for 3D tickets and \$7.00 for regular tickets. If one evening's revenue is \$16395, how many people saw 3D movies?

3 (10 pts)) In this problem, we will show that in $R = \mathbb{Z}[\sqrt{-5}]$, some numbers can factor into irreducible elements in two different ways.

(a) Define a function

$$\begin{aligned} N : R - \{0\} &\to \mathbb{N} \\ a + b\sqrt{-5} &\mapsto a^2 + 5b^2 \end{aligned}$$

Prove that $N(\alpha) \cdot N(\beta) = N(\alpha\beta)$.

(b) Prove that μ is a unit in R if and only if $N(\mu) = 1$.

(c) Prove that 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible in R.

(d) Find two distinct factorizations of 6 into irreducible elements in R.

Theorem 1 (Polynomial Division Theorem)**.** *Let F be a field and consider any polynomial $n(x) \in F[x]$ and a nonzero polynomial $d(x)$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that*

$$n(x) = d(x)q(x) + r(x) \qquad \textit{with } r(x) = 0 \textit{ or } \deg(r) < \deg(d).$$

4) Prove that the quotient and remainder in the theorem are unique.

(a) Suppose that (q_1, r_1) and (q_2, r_2) both satisfied the conditions of the theorem for a divisor $n(x)$ and dividend $d(x)$. Use these two equations to produce a third equation relating d, q_1, q_2, r_1, and r_2.

(b) If $q_1 \neq q_2$ explain why $\deg(r_1 - r_2) \geqslant \deg(d)$.

(c) Prove uniqueness of the quotient and remainder in the Polynomial Division Theorem.

5) We will prove that the quotient and remainder in the Polynomial Division Theorem exist.

(a) Prove the existence of $q(x)$ and $r(x)$ if $n = 0$.

(b) Prove the existence of $q(x)$ and $r(x)$ if $d(x)|n(x)$.

(c) Suppose that $n \neq 0$ and $d(x) \nmid n(x)$. Consider the set:

$$S = \{\deg(n(x) - d(x)k(x)) : k(x) \in F[x]\}$$

Explain why S is not empty.

(d) Explain why S has a least element.

(e) Use the least element found above to obtain an element $r(x)$ and explain why $\deg(r) < \deg(d)$. Hint, suppose that $\deg(r) \geqslant \deg(d)$ and consider the polynomial

$$s(x) = r(x) - cx^{\deg(r) - \deg(d)} \cdot d(x)$$

for some suitable value of c.

(f) Explain how to choose $q(x)$ satisfying the conditions of the Polynomial Division Theorem.