ABSTRACT ALGEBRA – HOMEWORK ASSIGNMENT FOR WEEK 1

1. Review of Basic Number Theory and such from Discrete

The following should have been covered in Discrete in some shape or form. In a sense the whole point of the course is that the manipulations below (starting with Problem 2) have little to do with integers per se, and that they are abstract algebra features. You'll do these manipulations many times in the class.

(1) (a) Let n and k be two positive integers. Show that

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

(b) **Binomial Theorem.** Let a and b be two numbers[1]. Use induction on n to prove that

$$(a+b)^n = \sum_{k=0}^{k=n} \binom{n}{k} a^k\, b^{n-k}.$$

(2) Let $a_1, \alpha_1, a_2, \alpha_2$ be integers. Let $b \neq 0$ be an integer with $b \big| a_1$ and $b \big| a_2$. Show that $b \big| \alpha_1 a_1 + \alpha_2 a_2$.

(3) Let a, b, c be integers. Assume that $b, c \neq 0$ and that $c \big| b$ and $b \big| a$. Show that $c \big| a$.

(4) (a) Use the Euclidean Algorithm to find $\mathrm{GCD}(1296, 2016)$.

(b) Based on the computations you just did find a pair of integers x and y such that

$$1296 \cdot x + 2016 \cdot y = \mathrm{GCD}(1296, 2016).$$

(5) The following theorem has been addressed in class.

Theorem. *Let p be a prime integer, and let a, b be integers such that $p \big| ab$. Then $p \big| a$ or $p \big| b$.*

Again, let p be a prime integer. Assume $a_1, a_2, ..., a_n$ are integers such that $p \big| a_1 a_2 ... a_n$. Use induction to show that there is an a_i ($1 \leq i \leq n$), such that $p \big| a_i$.

[1] It's irrelevant what kind of numbers a and b are: integers, rationals, reals, complex numbers... The argument you provide should be applicable to, say, two square matrices a and b of the same size so long they commute: $a \cdot b = b \cdot a$. In this sense of the word this homework problem is truly an abstract algebra problem.

2. The Fundamental Theorem of Arithmetic

The goal of the following homework problem is to have the proof of the Fundamental Theorem of Arithmetic go through your hands. The skeleton of the proof is given below. Please follow it: fill in the blanks and re-write the proof neatly. FYI: Alternations of this particular proof will appear over and over again in the course.

Theorem. *Let a be a non-zero, non-unit integer. Then a can be expressed as a product of primes*

$$a = \pm p_1 p_2 ... p_n.$$

This factorization is unique in the following sense: If

$$a = \pm p_1 p_2 ... p_n = \pm q_1 q_2 ... q_m,$$

with p_i and q_i all prime, then $(p_1, p_2, ..., p_n)$ is a permutation of $(q_1, q_2, ..., q_m)$.

Proof. It suffices to consider positive integers $a \geq 2$. We prove the statement using The Principle of Strong Induction. In the base case of $a = 2$ there is nothing to show as 2 is already its unique prime factorization. Now let $b \geq 2$ and assume that the statement is true for all $2 \leq a \leq b$. We need to show that the statement is true for ____________.

If ____________ is prime there is nothing show. So assume ____________ is composite. We then have

$$\underline{\qquad\qquad} = \underline{\qquad\qquad} \cdot \underline{\qquad\qquad}$$

for some integers ____________ and ____________ with

$$2 \leq \underline{\qquad\qquad} \leq b.$$

By the Induction Hypothesis we know that ____________ and ____________ permit factorization into primes. Thus we have

$$\underline{\qquad\qquad} = \underline{\qquad\qquad} \quad \text{and} \quad \underline{\qquad\qquad} = \underline{\qquad\qquad}$$

for some primes ____________. Since $b + 1 =$ ____________ we have

$$b + 1 = \underline{\qquad\qquad}$$

for primes ____________. This completes the proof of existence of prime factorization of ____________. Next assume that

$$\underline{\qquad\qquad} = p_1 p_2 ... p_n = q_1 q_2 ... q_m$$

are two prime factorizations of ____________. We see that $p_1 \mid$ ____________. By Problem 5 from this assignment we know that ____________. Permuting $q_1, ..., q_m$ if necessary we may assume that ____________ $= q_1$. Thus we have

$$p_2 ... p_n = \underline{\qquad\qquad}.$$

Since $a = p_2 ... p_n$ satisfies ____________ the Inductive Hypothesis applies and we have that ____________ is a permutation of ____________. We may now conclude that $(p_1, p_2, ..., p_n)$ is ____________. This completes the proof of uniqueness of prime factorization. $\square$

3. Parallels Between Number Theory and Polynomial Algebra

I made a claim that the content of the first portion of this assignment has little to do with integers per se. In the rest of the assignment you are expected to apply the very same techniques from the first part of the assignment to polynomials in one variable with real[2] coefficients.

(1) What adjustments to your solutions to Problems 2 and 3 need to be made in order to prove the following?
   (a) Let $A_1(X), \alpha_1(X), A_2(X), \alpha_2(X)$ be polynomials with real coefficients. Let $B \neq 0$ be another polynomial with real coefficients and let $B \big| A_1$ and $B \big| A_2$. Show that $B \big| \alpha_1 A_1 + \alpha_2 A_2$.
   (b) Let $A(X), B(X), C(X)$ be polynomials with real coefficients. Assume that $B, C \neq 0$ and that $C \big| B$ and $B \big| A$. Show that $C \big| A$.

   Please do <u>not</u> re-prove these statements. The point is that you understand which aspects of your solutions generalize to *abstract algebra*.

(2) (a) Use the Euclidean Algorithm to find $\mathrm{GCD}(x^9 + 1, x^4 - 1)$. I do wish to see all the details of your long division.
   (b) Based on the computations you just did find a pair of polynomials $P(x)$ and $Q(x)$ such that
$$(x^9 + 1) \cdot P(x) + (x^4 - 1) \cdot Q(x) = \mathrm{GCD}(x^9 + 1, x^4 - 1).$$

(3) (a) Use the Euclidean Algorithm to find $\mathrm{GCD}(2x + 1, 6x^3)$. I do wish to see all the details of your long division.
   (b) Based on the computations you just did find a pair of polynomials $P(x)$ and $Q(x)$ such that
$$(2x + 1) \cdot P(x) + (6x^3) \cdot Q(x) = 1.$$
   (c) Based on the computations you just did find a pair of polynomials $P(x)$ and $Q(x)$ such that
$$(2x + 1) \cdot P(x) + (6x^3) \cdot Q(x) = x + 1.$$

(4) In class we mentioned that there is a GCD Theorem for polynomials in one variable. It goes something like so.

   Theorem. *Let $A(X)$ and $B(X)$ be two non-zero polynomials with coefficients in real numbers, and let $D(X)$ be any its greatest common divisor[3]. Then there exist polynomials $P(X)$ and $Q(X)$ with real coefficients such that*
$$A(X) \cdot P(X) + B(X)Q(X) = D(X).$$

   Fill-in the blanks / re-write in full the proof of this theorem. Use the following skeleton.

[2] FYI: There would be absolutely no difference if I changed my mind and replaced the word "real" with "rational" or "complex".

[3] In this context greatest common divisor is only unique if one requests that it be *monic* i.e that its leading coefficient be 1.

Proof. Consider the set

$$\mathcal{S} = \Big\{ \deg(C) \,\Big|\, C \neq 0 \text{ and } C(X) = A(X)\cdot P(X) + B(X)\cdot Q(X) \text{ with } P(X), Q(X) \in \mathbb{R}[X] \Big\}.$$

Since $\mathcal{S} \subseteq \mathbb{N} \cup \{0\}$ we know that $\mathcal{S}$ contains its minimum element. So let

$$C(X) = \underline{\hspace{3cm}} \neq 0$$

with $\underline{\hspace{3cm}}$ be such that $\underline{\hspace{3cm}}$ is minimum possible. Dividing by the leading coefficient of C if necessary we may assume that $\underline{\hspace{3cm}}$. To prove our theorem it suffices to prove that C is the greatest common divisor of A and B.

Our first goal is to show that C is a common divisor of A and B. Suppose that $\underline{\hspace{3cm}}$. By the polynomial long division we know that there exist polynomials $R(X)$ and $S(X) \neq 0$ such that

$$A(X) = \underline{\hspace{3cm}} \quad \text{and} \quad \underline{\hspace{3cm}}.$$

Since

$$\begin{aligned} 0 \neq S(X) &= \underline{\hspace{3cm}}C(X) + \underline{\hspace{3cm}}A(X) \\ &= \underline{\hspace{3cm}}A(X) + \underline{\hspace{3cm}}B(X) \end{aligned}$$

we see that $\deg(S) \in \underline{\hspace{3cm}}$. However, since $\deg(S) < \underline{\hspace{3cm}}$ the latter contradicts the assumption that $\deg(C)$ is $\underline{\hspace{3cm}}$. It follows that $C \,\big|\, \underline{\hspace{1cm}}$. By the same argument we may conclude that $C \,\big|\, \underline{\hspace{1cm}}$. Overall, we have proven that C is a common divisor of A and B.

To show that C is the greatest common divisor consider a common divisor E of A and B. Since $E \,\big|\, A$ and $E \,\big|\, B$ we must, by Problem $\underline{\hspace{3cm}}$ of this assignment, have

$$E \,\Big|\, \underline{\hspace{3cm}} \quad \text{i.e.} \quad \underline{\hspace{1cm}} \,\Big|\, C.$$

In particular, it follows that $\deg(\underline{\hspace{1cm}}) \leq \deg(\underline{\hspace{1cm}})$. We now see that C is the greatest common divisor of A and B. ◻

(5) State the counterpart to the Fundamental Theorem of Arithmetic for polynomials in one variable. You do <u>not</u> need to prove it.