Math 561/661 **Fall 2021**
Homework 5 **Drew Armstrong**

---

1. Bézout's Identity for Vectors. Consider a vector of integers $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$. Since every common divisor of $a_1, \ldots, a_n$ is bounded above by the maximum of $|a_i|$, it follows that there exists a unique positive GCD. Let's call it $d = \gcd(a_1, a_2, \ldots, a_n)$.

(a) Prove that there exist integers $x_1, \ldots, x_n \in \mathbb{Z}$ satisfying $a_1x_1 + \cdots + a_nx_n = d$. [Hint: Consider the set $S = \{a_1x_1 + \cdots a_nx_n : x_1, \ldots, x_n \in \mathbb{Z}\}$ and let e be the smallest positive element of this set. Since d divides each a_i we have $d|e$ and hence $d \leq e$. On other hand, show that e is a common divisor of the a_i, so that $e \leq d$. Idea: If the remainder of e mod a_i is nonzero then you can find a smaller positive element of S.]

(b) Use part (a) to prove that

$$\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n).$$

(c) We can turn part (b) into a recursive algorithm. Use this algorithm to find integers $x, y, z \in \mathbb{Z}$ satisfying $35x + 21y + 15z = 1$. [Hint: First find x', y' such that $\gcd(35, 12) = 35x' + 21y'$. Then find x'', y'' such that $\gcd(\gcd(35, 21), 15) = \gcd(35, 21)x'' + 15y''$.]

2. Generalized Chinese Remainder Theorem. Consider some positive integers $n_1, \ldots, n_k$ such that $\gcd(n_i, n_j) = 1$ for all $i \neq j$.[1] If $n = n_1 \cdots n_k$ then our goal is to show that the following ring homomorphism is invertible, and to find its inverse:

$$\begin{array}{rccc} \varphi : & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \\ & a \text{ mod } n & \mapsto & (a \text{ mod } n_1, \ldots, a \text{ mod } n_k). \end{array}$$

(a) For each i, define $\hat{n}_i = n_1 \cdots n_{i-1}n_{i+1} \cdots n_k$. Prove that

$$\gcd(\hat{n}_1, \hat{n}_2, \ldots, \hat{n}_k) = 1.$$

[Hint: Use induction on k. For $1 \leq i < k$ let $\tilde{n}_i = n_1 \cdots n_{i-1}n_{i+1} \cdots n_{k-1}$ so that $\hat{n}_i = \tilde{n}_i n_k$ and assume for induction that $\gcd(\tilde{n}_1, \ldots, \tilde{n}_{k-1}) = 1$. If some prime p divides each $\hat{n}_i$ then it either divides n_k or it divides each $\tilde{n}_i$, which is a contradiction.]

(b) It follows from Problem 1(a) that there exist some integers $x_1, \ldots, x_k \in \mathbb{Z}$ satisfying

$$\hat{n}_1x_1 + \hat{n}_2x_2 + \ldots + \hat{n}_kx_k = 1.$$

In this case prove that $\varphi^{-1}(a_1, \ldots, a_k) = a_1\hat{n}_1x_1 + \cdots + a_k\hat{n}_kx_k$ mod n. [Hint: You only need to show that $a_1\hat{n}_1x_1 + \cdots + a_k\hat{n}_kx_k \equiv a_i$ mod n_i.]

(c) Use your answer from Problem 1(c) to find an expression for the ring homomorphism $\varphi^{-1} : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/105\mathbb{Z}$.

3. Partial Fractions. Let R be a Euclidean domain with size function $N : R \setminus \{0\} \to \mathbb{N}$. You can assume that the result of Problems 1 and 2 still hold in this context.

(a) Suppose that an element $n \in R$ has prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$ and write $n_i = p_i^{e_i}$. Show that there exist elements $x_1, \ldots, x_k \in R$ satisfying

$$\frac{1}{n} = \frac{x_1}{n_1} + \frac{x_2}{n_2} + \cdots + \frac{x_k}{n_k}.$$

[Hint: $\hat{n}_i/n = 1/n_i$.]

---

[1]This is a stronger restriction than $\gcd(n_1, \ldots, n_k) = 1$. For example, $\gcd(2, 3, 4) = 1$ but $\gcd(2, 4) \neq 1$.

(b) Continuing from part (a), prove that there exist elements $m, r_{ij} \in R$ satisfying $r_{ij} = 0$ or $N(r_{ij}) < N(p_i)$, such that

$$\frac{1}{n} = m + \sum_{i=1}^{k} \sum_{j=1}^{e_i} \frac{r_{ij}}{p_i^j}.$$

[Hint: Consider a fraction of the form x/p^e. Divide x by p to obtain $x = pq + r$ where $r = 0$ or $N(r) < N(p)$. Then we have $x/p^e = r/p^e + q/p^{e-1}$.]

4. Conjugation of Complex Polynomials. For any polynomial $f(x) = \sum a_k x^k$ with complex coefficients we define the *conjugate polynomial* by conjugating the coefficients:

$$f^*(x) = \sum a_k^* x^k.$$

(a) For all $f(x) \in \mathbb{C}[x]$ and $\alpha \in \mathbb{C}$ prove that

$$f(\alpha) = 0 \quad \Longleftrightarrow \quad f^*(\alpha^*) = 0.$$

(b) We can think of $\mathbb{R}[x] \subseteq \mathbb{C}[x]$ as a subring. For all $f(x) \in \mathbb{C}[x]$ prove that

$$f(x) = f^*(x) \quad \Longleftrightarrow \quad f(x) \in \mathbb{R}[x].$$

(c) For all $f(x), g(x) \in \mathbb{C}[x]$, prove that

$$(f+g)^*(x) = f^*(x) + g^*(x) \quad \text{and} \quad (fg)^*(x) = f^*(x)g^*(x).$$

(d) For all $f(x) \in \mathbb{C}[x]$, use parts (b) and (c) to show that

$$f(x) + f^*(x) \in \mathbb{R}[x] \quad \text{and } f(x)f^*(x) \in \mathbb{R}[x].$$