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 $\gcd(\gcd(35, 21), 15) = \gcd(35, 21)x'' + 15y''$.]

(a): Let $d = \gcd(a_1, \ldots, a_n)$. Since d is a common divisor of $a_1, \ldots, a_n$ we can write $dk_i = a_i$ for some integers $k_1, \ldots, k_n \in \mathbb{Z}$. Now 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 S. By definition we have $e = a_1x_1 + \cdots + a_nx_n$ for some $x_1, \ldots, x_n \in \mathbb{Z}$. But then we have

$$e = dk_1x_1 + \cdots + dk_nx_k = d(k_1x_1 + \cdots + k_nx_n)$$

which implies that $d|e$ and hence $d \leq e$. On the other hand, we will show that $e \leq d$. To do this, let us divide each a_i by e to obtain some integers $q_i, r_i \in \mathbb{Z}$ satisfying

$$\begin{cases} a_i = eq_i + r_i, \\ 0 \leq r_i < e. \end{cases}$$

I claim that $r_i = 0$ for all i. Indeed, if $r_i > 0$ then since $r_i < e$ and since

$$r_i = e - a_iq_i = a_1(-x_1) + \cdots + a_i(q_i - x_i) + \cdots + a_n(-x_n) \in S,$$

we obtain a positive element of S that is strictly smaller than e. Contradiction. We have shown that $r_i = 0$ for all i and hence e is a common divisor of $a_1, \ldots, a_n$. Since d is the **greatest** common divisor, this implies that $e \leq d$ as desired.

In summary, we have shown that

$$d = e = a_1x_1 + \cdots + a_nx_n$$

for some integers $x_1, \ldots, x_n \in \mathbb{Z}$.

(b): For this part we write $e = \gcd(a_1, \ldots, a_{n-1})$. Then we consider the sets

$$\begin{aligned} \text{Div}(a_1, \ldots, a_n) &= \{d \in \mathbb{Z} : d|a_i \text{ for all } i\}, \\ \text{Div}(e, a_n) &= \{d \in \mathbb{Z} : d|e \text{ and } d|a_n\}. \end{aligned}$$

If we can show that these two sets are equal then the desired GCDs will also be equal. First suppose that $d \in \text{Div}(e, a_n)$ so that $d\ell = e$ and $dm = a_n$ for some $\ell, m \in \mathbb{Z}$. Since e is a common divisor of $a_1, \ldots, a_{n-1}$ we also have $ek_i = a_i$ for some $k_1, \ldots, k_{n-1} \in \mathbb{Z}$. But this implies that $a_i = ek_i = d\ell k_i$ so that $d|a_i$ for all $1 \leq i \leq n-1$ and it follows that d is in the set $\text{Div}(a_1, \ldots, a_n)$. On the other hand, suppose that $d \in \text{Div}(a_1, \ldots, a_n)$ so that $dk_i = a_i$ for some integers $k_1, \ldots, k_n \in \mathbb{Z}$. From part (a) we can also write $e = a_1x_1 + \cdots + a_{n-1}x_{n-1}$ for some integers $x_1, \ldots, x_{n-1} \in \mathbb{Z}$. It follows that

$$e = a_1x_1 + \cdots + a_{n-1}x_{n-1} = dk_1x_1 + \cdots + dk_{n-1}x_{n-1} = d(k_1x_1 + \cdots k_{n-1}x_{n-1}),$$

and hence d is an element of $\text{Div}(e, a_n)$ as desired.

(c): Our goal is to find $x, y, z \in \mathbb{Z}$ such that $35x + 21y + 15z = 1$. For this we will use the Euclidean Algorithm and the fact that

$$\gcd(35, 21, 15) = \gcd(\gcd(35, 21), 15) = \gcd(7, 15) = 1.$$

First we apply the EA to find x', y' such that $7x' + 15y' = 1$:

$$\begin{array}{r|c|c} 0 & 1 & 15 \\ 1 & 0 & 7 \\ -2 & 1 & 1 \end{array}$$

We see that $7(-2)+15(1) = 1$. Then we apply the EA to find x'', y'' such that $35x''+21y'' = 7$:

$$\begin{array}{r|c|c} 1 & 0 & 35 \\ 0 & 1 & 21 \\ 1 & -1 & 14 \\ -1 & 2 & 7 \end{array}$$

We see that $35(-1) + 21(2) = 7$. Then putting the two equations together gives

$$1 = 7(-2) + 15(1) = [35(-1) + 21(2)]\,(-2) + 15(1) = 35(2) + 21(-4) + 15(1).$$

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 by explicitly finding its inverse:

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

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

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

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

(a): The result is true when $k=2$ because in that case we have $\hat{n}_1 = n_2$ and $\hat{n}_2 = n_1$, so that

$$\gcd(\hat{n}_1, \hat{n}_2) = \gcd(n_2, n_1) = 1.$$

Now let $k \geq 3$ and assume for induction that the statement is true for $k-1$. Given integers $n_1, \ldots, n_k \in \mathbb{Z}$ with $\gcd(n_i, n_j) = 1$ for all $i \neq j$, our goal is to show that

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

And by induction we may assume that

$$\gcd(\tilde{n}_1, \ldots, \tilde{n}_{k-1}) = 1,$$

where $\tilde{n}_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_{k-1}$. So let us suppose for contradiction that there exists a common prime divisor $p|\hat{n}_1, \ldots, p|\hat{n}_k$. There are two cases:

- Suppose that $p|n_k$. Since $p|\hat{n}_k$ and since p is prime we must also have $p|n_i$ for some $1 \leq i \leq k-1$. Then $p|n_k$ and $p|n_i$ contradict the fact that $\gcd(n_i, n_k) = 1$.
- Suppose that $p \nmid n_k$. Then since $\hat{n}_i = \tilde{n}_i n_k$ for all $1 \leq i \leq k-1$ and since $p|\hat{n}_i$, we must have $p|\tilde{n}_i$ for all $1 \leq i \leq k-1$, which contradicts the induction hypothesis.

We have shown that the numbers $\hat{n}_1, \ldots, \hat{n}_k$ have no common prime factor, as desired.

(b): Let integers $n_1, \ldots, n_k \in \mathbb{Z}$ satisfy $\gcd(n_i, n_j) = 1$ for all $i \neq j$. If $\hat{n}_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$ then it follows from Problem 1(a) that there exist $x_1, \ldots, x_k \in \mathbb{Z}$ satisfying

$$\hat{n}_1 x_1 + \cdots + \hat{n}_k x_k = 1.$$

Let $n = n_1 \cdots n_k$ and recall the definition of the ring homomorphism φ:

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

I claim that the inverse of the ring homomorphism φ is given by

$$\varphi^{-1}(a_1, \ldots, a_k) = b \bmod n,$$

where $b = a_1 \hat{n}_1 x_1 + \cdots a_k \hat{n}_k x_k$. To prove this we need to show that $b \equiv a_i \bmod n_i$ for all i. First we observe for all $i \neq j$ that $n_i | \hat{n}_j$ and hence $\hat{n}_j \equiv 0 \bmod n_i$, so that

$$b \equiv 0 + \cdots + 0 + a_i \hat{n}_i x_i + 0 + \cdots + 0 \bmod n_i.$$

Then we observe that $\hat{n}_i x_i = 1 - \sum_{j \neq i} \hat{n}_j x_j$, so that

$$\hat{n}_i x_i \equiv 1 - \sum_{j \neq i} 0 \equiv 1 \bmod n_i,$$

and hence

$$b \equiv a_i \hat{n}_i x_i \equiv a_i(1) \equiv a_i \bmod n_i.$$

(c): Let $(n_1, n_2, n_3) = (3, 5, 7)$ so that $(\hat{n}_1, \hat{n}_2, \hat{n}_3) = (35, 21, 15)$. In Problem 1(c) we showed that the integers $(x_1, x_2, x_3) = (2, -4, 1)$ satisfy $\hat{n}_1 x_1 + \hat{n}_2 x_2 + \hat{n}_3 x_3 = 1$. Therefore the inverse ring homomorphism $\varphi^{-1} : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/105\mathbb{Z}$ is given by

$$\varphi^{-1}(a_1, a_2, a_3) = 70a_1 - 84a_2 + 15a_3 \bmod 105.$$

For example, φ^{-1} preserves the multiplicative identity, as it should:

$$\varphi^{-1}(1, 1, 1) = 70 - 84 + 15 = 1 \bmod 105.$$

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

(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 $x/p^e = r/p^e + q/p^{e-1}$.]

(a): Let $n = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes $p_i \neq p_j$ and let $n_i = p_i^{e_i}$, so that $n = n_1 \cdots n_k$. Let $\hat{n}_i = n/n_i$ as in Problem 2. Then from Problem 2(a) there exist elements $x_1, \ldots, x_k \in R$ satisfying[2]

$$1 = \hat{n}_1 x_1 + \cdots + \hat{n}_k x_k,$$

and dividing both sides by n gives[3]

$$\frac{1}{n} = \frac{\hat{n}_1 x_1}{n} + \cdots + \frac{\hat{n}_k x_k}{n} = \frac{x_1}{n_1} + \cdots + \frac{x_k}{n_k} = \frac{x_1}{p_1^{e_1}} + \cdots + \frac{x_k}{p_k^{e_k}}.$$

(b): Now consider any fraction x/p^e where p is prime and $e \geq 0$. Our goal is to show that

$$\frac{x}{p^e} = \frac{r_1}{p^e} + \frac{r_2}{p^{e-1}} + \cdots + \frac{r_e}{p} + m$$

for some elements $m, r_1, \ldots, r_e \in R$ satisfying $r_i = 0$ or $N(r_i) < N(p)$ for all i. The idea is to repeatedly divide the numerator by p. First we have $x = r_1 + pq_1$ so that

$$\frac{x}{p^e} = \frac{r_1 + pq_1}{p^e} = \frac{r_1}{p^e} + \frac{q_1}{p^{e-1}}.$$

Then we divide q_1 by p to obtain $q_1 = r_2 + pq_2$, and repeat to obtain

$$\frac{x}{p^e} = \frac{r_1}{p^e} + \frac{r_2}{p^{e-1}} + \cdots + \frac{r_e}{p} + q_e.$$

By construction each remainder r_i satisfies $r_i = 0$ or $N(r_i) < N(p)$.

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

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

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

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

(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

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

---

[2]In the familiar Euclidean domains $\mathbb{Z}$ and $\mathbb{F}[x]$ we may take $m = 0$ but not in general. See *Partial Fractions in Euclidean Domains* (1989) by Packard and Wilson.

[3]Here we are working in the field of fractions of the domain R. See HW6.

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

(a): Since $* : \mathbb{C} \to \mathbb{C}$ preserves all ring operations, we have
$$f(\beta)^* = \left(\sum_k \alpha_k \beta^k\right)^* = \sum_k \alpha_k^* (\beta^*)^k = f^*(\beta^*).$$
It follows from this that $f(\beta) = 0$ implies $f^*(\beta^*) = f(\beta)^* = 0^* = 0$ and $f^*(\beta^*) = 0$ implies $f(\beta) = (f^*(\beta^*))^* = 0^* = 0$.

(b): Two formal polynomials are equal if and only if their coefficients are equal. The coefficient of x^k in $f(x)$ is α_k and the coefficient of x^k in $f^*(x)$ is α_k^*. If $f^*(x) = f(x)$ then we must have $\alpha_k^* = \alpha_k$, which implies that $\alpha_k \in \mathbb{R}$ for all k. In other words, we must have $f(x) \in \mathbb{R}[x]$.

(c): Let $f(x) = \sum_k \alpha_k x^k$ and $g(x) = \sum_k \beta_k x^k$. The coefficients of $f+g$ are $\alpha_k + \beta_k$, hence the coefficients of $(f+g)^*$ are $(\alpha_k + \beta_k)^* = \alpha_k^* + \beta_k^*$. But these are also the coefficients of $f^* + g^*$, hence $(f+g)(x) = f^*(x) + g^*(x)$. For the second statement, recall that
$$f(x)g(x) = \sum_k \left(\sum_{i+j=k} \alpha_i \beta_j\right) x^k.$$
So the coefficients of $(fg)^*(x)$ are
$$\left(\sum_{i+j=k} \alpha_i \beta_j\right)^* = \left(\sum_{i+j=k} \alpha_i^* \beta_j^*\right).$$
But these are also the coefficients of $f^*(x)g^*(x)$, hence $(fg)^*(x) = f^*(x)g^*(x)$.

(d): As we sometimes do, we will write f instead of $f(x)$ to save space. Let $f(x) \in \mathbb{C}[x]$. Then from part (c) we have
$$(f+f^*)^* = f^* + f^{**} = f^* + f = f + f^*$$
and
$$(ff^*)^* = f^* f^{**} = f^* f = ff^*,$$
hence it follows from part (b) that $f + f^* \in \mathbb{R}[x]$ and $ff^* \in \mathbb{R}[x]$.