Math 561/661 **Fall 2021**
Exam 3 **Wed Dec 8**

Problem 1. Chinese Remainder Theorem. Let $m, n \geq 1$ and consider the function

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

This is well defined because $a \equiv a' \bmod mn$ implies that $a \equiv a' \bmod m$ and $a \equiv a' \bmod n$.

(a) If $\gcd(m, n) = 1$, prove for all $c \in \mathbb{Z}$ that $m|c$ and $n|c$ imply $(mn)|c$.

If $\gcd(m, n) = 1$ then there exist $x, y \in \mathbb{Z}$ satisfying $mx + ny = 1$. Now suppose that $m|c$ and $n|c$ for some $c \in \mathbb{Z}$. By definition this means that $mk = c$ and $n\ell = c$ for some $k, \ell \in \mathbb{Z}$. It follows that

$$\begin{aligned} mx + ny &= 1 \\ (mx + ny)c &= c \\ mxc + nyc &= c \\ mx(n\ell) + ny(mk) &= c \\ mn(x\ell + yk) &= c, \end{aligned}$$

and hence $(mn)|c$.

(b) If $\gcd(m, n) = 1$, use part (a) to prove that φ is injective.

Suppose that $\gcd(m, n) = 1$. Our goal is to show for all $a, a' \in \mathbb{Z}/mn\mathbb{Z}$ that $\phi(a) = \phi(a')$ in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ implies $a = a'$ in $\mathbb{Z}/mn\mathbb{Z}$. In other words, we must show for all $a, a' \in \mathbb{Z}$ that $a \equiv a' \bmod m$ and $a \equiv a' \bmod n$ imply $a \equiv a' \bmod mn$.

So let us suppose that $a \equiv a' \bmod m$ and $a \equiv a' \bmod n$. By definition this means that $m|(a - a')$ and $n|(a - a')$. Then since $\gcd(m, n) = 1$ it follows from part (a) that $(mn)|(a - a')$ and hence $a \equiv a' \bmod mn$, as desired.

(c) Since the domain and codomain have the same size, it follows from (b) that there exists an inverse function φ^{-1}. If $mx + ny = 1$, prove that

$$\varphi^{-1}(a \bmod m, b \bmod n) = any + bmx \bmod mn.$$

It suffices to show that $\varphi(any + bmx) = (a, b)$, i.e., that $any + bmx \equiv a \bmod m$ and $any + bmx \equiv b \bmod n$. For the first statement, note that $m \equiv 0 \bmod m$ and $ny = 1 - mx \equiv 1 \bmod m$, so that

$$any + bmx \equiv any + 0 \equiv a \cdot 1 \equiv a \bmod m.$$

The second statement follows by symmetry. Or we can give the details: Since $n \equiv 0 \bmod n$ and $m = 1 - ny \equiv 1 \bmod n$ we have

$$any + bmx \equiv 0 + bmx \equiv b \cdot 1 \equiv b \bmod n.$$

(d) Use part (c) to find all $c \in \mathbb{Z}$ such that $c \equiv 3 \bmod 5$ and $c \equiv 4 \bmod 11$.

From the definition of φ we have $c \equiv a \bmod m$ and $c \equiv b \bmod n$ if and only if $\varphi(c) = (a, b)$. If $\gcd(m, n) = 1$ then since φ is invertible we have $\varphi(c) = (a, b)$ if and only if $c = \varphi^{-1}(a, b)$, i.e., if and only if $c \equiv any + bmx \bmod mn$.

In our case we have $(m, n) = (5, 11)$ and $(a, b) = (3, 4)$. Then by inspection we have $5(-2) + 11(1) = 1$, so we may take $(x, y) = (-2, 1)$. Finally, we have

$$\begin{aligned} c &\equiv any + bmx \\ &\equiv 3 \cdot 11(1) + 4 \cdot 5(-2) \\ &\equiv 33 - 40 \\ &\equiv -7 \\ &\equiv 48 \bmod 55. \end{aligned}$$

Problem 2. Fractions. Let R be an integral domain. A "fraction" is an abstract symbol a/b with $a, b \in R$ and $b \neq 0$.

(a) State the definition of $a/b = a'/b'$.

$$\frac{a}{b} = \frac{a'}{b'} \quad \Longleftrightarrow \quad ab' = a'b.$$

(b) State the definition of $a/b + c/d$.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

(c) If $a/b = a'/b'$ and $c/d = c'/d'$, prove that $a/b + c/d = a'/b' + c'/d'$.

By assumption we have $ab' = a'b$ and $cd' = c'd$, which implies that

$$\begin{aligned} (ad + bc)(b'd') &= (ad)(b'd') + (bc)(b'd') \\ &= (ab')(dd') + (cd')(bb') \\ &= (a'b)(dd') + (c'd)(bb') \\ &= (a'd')(bd) + (b'c')(bd) \\ &= (a'd' + b'c')(bd). \end{aligned}$$

Problem 3. FTA Stuff. Let $f(x) = g(x)q(x) + r(x)$ for some polynomials $f, g, q, r \in \mathbb{C}[x]$ with $g(x) \neq 0$, such that $r(x) = 0$ or $\deg(r) < \deg(g)$.

(a) If $f(x)$ and $g(x)$ have real coefficients, prove that $q(x)$ and $r(x)$ have real coefficients. [Hint: Divide $f(x)$ by $g(x)$ in the ring $\mathbb{R}[x]$.]

Since $f(x), g(x) \in \mathbb{R}[x]$ and $g(x) \neq 0$, the Division Theorem says that there exist $q'(x), r'(x) \in \mathbb{R}[x]$ satisfying $f(x) = g(x)q'(x) + r'(x)$ with $r'(x) = 0$ or $\deg(r') < \deg(g)$. Then it follows from the **uniqueness** of quotient and remainder in the ring $\mathbb{C}[x]$ that $q(x) = q'(x) \in \mathbb{R}[x]$ and $r(x) = r'(x) \in \mathbb{R}$.

Optional Details: We have $gq + r = gq' + r'$. If $r = r' = 0$ then $gq = gq'$ implies $g(q - q') = 0$. Then since $g \neq 0$ we have $q - q' = 0$, hence $q = q'$. So let us assume that r, r' are not both zero. Without loss of generality, let's say that $r \neq 0$. Now assume for contradiction that $r - r \neq 0$, which since $g(q - q') = r - r'$ implies $q - q' \neq 0$. But then we have

$$\deg(g) \leq \deg(g) + \deg(q - q') = \deg(g(q - q')) = \deg(r - r') \leq \deg(r),$$

which contradicts the fact that $\deg(r) < \deg(g)$. We have shown that $g(q - q') = r - r' = 0$, which since $g \neq 0$ also implies that $q - q' = 0$. In other words, we have shown that $q = q'$ and $r = r'$.

(b) If $f(x) \in \mathbb{R}[x]$ and $f(\alpha) = 0$ for some $\alpha \in \mathbb{C} \setminus \mathbb{R}$, use Descartes' Theorem and part (a) to prove that $f(x) = (x^2 - (\alpha + \alpha^*)x + \alpha\alpha^*)q(x)$ for some $q(x) \in \mathbb{R}[x]$.

First we apply Descartes' Theorem in the ring $\mathbb{C}[x]$ to obtain

$$f(x) = (x - \alpha)g(x)$$

for some $g(x) \in \mathbb{C}[x]$. Since $f(x)$ has real coefficients we also have $f(\alpha^*) = 0$, hence

$$0 = f(\alpha^*) = (\alpha^* - \alpha)g(\alpha^*).$$

Since $\alpha^* - \alpha \neq 0$ (because $\alpha \notin \mathbb{R}$) this implies that $g(\alpha^*)$ and then applying Descartes' Theorem again gives

$$g(x) = (x - \alpha^*)h(x)$$

for some $h(x) \in \mathbb{C}[x]$. Putting these together gives

$$\begin{aligned} f(x) &= (x - \alpha)g(x) \\ &= (x - \alpha)(x - \alpha^*)h(x) \\ &= (x^2 - (\alpha + \alpha^*)x + \alpha\alpha^*)h(x). \end{aligned}$$

Finally, since $\alpha + \alpha^* \in \mathbb{R}$ and $\alpha\alpha^* \in \mathbb{R}$, part (a) tells us that $h(x) \in \mathbb{R}[x]$.