Addendum A: Aritmética modular

1. El anillo $\mathbb{Z}_m$

Comenzaremos convirtiendo la relación módulo m en un conjunto a través de sus clases de equivalencia por lo que antes de continuar es recomendable detenerse si los conceptos asociados a una relación de equivalencia parecen ajeno, es muy importante que éste quede lo más claro posible.

Teorema A.1. *Para un entero $m > 1$, la relación $\cdot \equiv \cdot \mod m$ es de equivalencia.*

Debido a este teorema propondremos una notación que haga referencia precisamente a las relaciones de equivalencia. Usaremos de nueva cuenta la convención acerca de los números m y n tomándolos siempre como > 1 cuando sean mencionados.

Definición A.1. Para un entero cualquiera a, definimos la *clase de equivalencia módulo m* como el conjunto

$$[a]_m = \{x \in \mathbb{Z} \mid x \equiv a \mod m\}.$$

Definimos también el conjunto de *los enteros módulo m*, como

$$\mathbb{Z}_m = \{[a]_m \mid a \in \mathbb{Z}\}.$$

A continuación se menciona una importante propiedad acerca de las clases de equivalencia módulo m, sin embargo, ésta se presenta sin prueba asumiendo que se está lo suficientemente familiarizado con el tema de relaciones de equivalencia[1].

Proposición A.2. *Para cualesquiera enteros a y b los siguientes enunciados son equivalentes:*

1. $a \equiv b \mod m$.
2. $[a]_m = [b]_m$.
3. $[a]_m \cap [b]_m \neq \varnothing$.

La proposición anterior deriva sin mucho problema en el hecho que las clases equivalencia forman una partición del conjunto $\mathbb{Z}$. Poco usaremos este hecho, aunque en nuestra discusión de divisibilidad el resultado ya fue probado. El efecto en particular que tendrá este hecho, y que nos interesa mucho más, es determinar cuántas clases de equivalencia resultan en la relación módulo m. De acuerdo al teorema de la división, para cada entero a, existen un par único de enteros q y r de forma que $0 \leq r < m$ y

$$a = qm + r.$$

[1] ¿No has ido a leer tus notas de relaciones de equivalencia? Ahora es un buen momento. Corre.

Esto implica en particular que $a \equiv r \mod m$ por lo que

$$[a]_m = [r]_m;$$

además, si existiera otro número $0 \leq s < m$ de forma que $[a]_m = [s]_m$, eso implicaría que $a \equiv s$ mód m y en consecuencia, existiría un entero p de forma que $a = pm + s$, lo cual por supuesto deriva en tener $p = q$ y $s = r$. Podemos en ese caso concluir que a pertenece a una y sólo una de las siguientes clases de equivalencia:

$$[0]_m, [1]_m, \ldots, [m-1]_m.$$

La discusión anterior no es más que una mera repetición de la presentada en la prueba de la proposición 3.11 de la lectura anterior, la cual enunciamos ahora en términos de clases de equivalencia.

Teorema A.3.

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

Este teorema es muchas veces usado para llamar a $\mathbb{Z}_m$ *el conjunto de las clases residuo de* m, precisamente porque cada entero pertenecerá a la clase de equivalencia del residuo que tenga. Otra conclusión que puede pasar desapercibida con facilidad por la notación y que resulta del teorema anterior es que el conjunto $\mathbb{Z}_m$ es finito al existir sólo un número finito de residuos posibles en la división.

Ahora que tenemos un conjunto base podemos preguntarnos que significará sumar dos elementos en él. Exploremos primero esta idea desde el punto de vista de congruencias, considerando de momento a la congruencia como si de una igualdad se tratara. Pongamos primero un ejemplo, sabemos que $6 \equiv 1 \mod 5$, también $7 \equiv 2 \mod 5$ y por último $13 \equiv 3 \mod 5$. Esta última expresión se puede escribir también como

$$7 + 6 \equiv 2 + 1 \mod 5.$$

Por primitivo que parezca el ejemplo, nos sugiere como lidiar con el caso general. Recordemos que el teorema 3.13 garantiza que $[a_1]_m = [a_2]_m$ y $[b_1]_m = [b_2]_m$, se deben tener dos cosas:

$$[a_1 + b_1]_m = [a_2 + b_2]_m$$

y

$$[a_1 \cdot b_1]_m = [a_2 \cdot b_2]_m.$$

Estas expresiones nos permiten definir una suma y un producto en las clases de equivalencia, pues uno de los temores al operar las clases usando representares es que el cambio de representante no defina de manera única la clase resultado de la operación. En esos casos se dice que *la operación está bien definida*, el teorema 3.13 prueba que las operaciones están bien definidas.

Definición A.2. En $\mathbb{Z}_m$, se definen la operaciones

$$[a]_m +_m [b]_m = [a + b]_m$$

y

$$[a]_m \cdot_m [b]_m = [a \cdot b]_m$$

La operaciones están asociadas a los elementos de $\mathbb{Z}_m$ pero como se puede apreciar, la notación comienza a ser algo voluminosa, volviendo deseable, cuando el contexto lo permita, eliminar los subíndices en la suma y el producto, por lo que muchas veces y cuando no exista ambigüedad y cuando sea prudente se escribirá:

$$[a]_m + [b]_m = [a + b]_m$$

y

$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

sin confundir las operaciones que aparecen a la izquierda de las igualdades (suma y producto para $\mathbb{Z}_m$) con las que aparecen a la derecha (suma y producto para $\mathbb{Z}$).

Estamos en un punto interesante pues hemos encontrado un conjunto y le hemos asociado dos operaciones, el conjunto en cuestión es significativamente distinto a $\mathbb{Z}$, aunque derivado de él, y sus operaciones esconden la teoría de congruencias. Aunque parezca sorprendente, ésta es al menos la segunda ocasión en que nos encontramos con un fenómeno de este tipo.

Teorema A.4. *El conjunto $\mathbb{Z}_m$ con las operaciones $+_m$ y $\cdot_m$ es un anillo conmutativo.*

La prueba es un ejercicio excelente para recordar el significado de anillo y conectar las ideas que se han estado discutiendo. Para ilustrar uno de los enunciados de la definición de anillo mostramos la propiedad distributiva: Para enteros a, b y c, tenemos

$$\begin{aligned}
[a]_m \cdot ([b]_m + [c]_m) &= [a]_m \cdot [b + c]_m \\
&= [a \cdot (b + c)]_m \\
&= [a \cdot b + a \cdot c]_m \\
&= [a \cdot b] + [a \cdot c]_m \\
&= [a]_m \cdot [b]_m + [a]_m \cdot [c]_m.
\end{aligned}$$

Lo que garantiza la validez de la propiedad distributiva.

Ahora que $\mathbb{Z}_m$ ha resultado un anillo, podemos realizar preguntas relevantes acerca de su naturaleza operativa, para así revelar sus propiedades algebraicas. Por ejemplo, una muy natural resulta al preguntar si las leyes de cancelación son válidas. Sin dificultad alguna, podemos notar que la prueba de la ley de cancelación de la suma en $\mathbb{Z}$ funciona para los enteros módulo pero la prueba de la ley de cancelación del producto, dependía de una propiedad adicional impuesta a $\mathbb{Z}$. Vamos a explorar la respuesta a esta pregunta intentando imponer algunas condiciones sobre los enteros para tener

$$[a]_m \cdot [b]_m = [0]_m$$

y

$$[a]_m \cdot [b]_m = [1]_m.$$

Estas ecuaciones modulares, corresponden a propiedades asociadas de manera abstracta al concepto de dominio entero y de unidad respectivamente. Estos serán nuestros siguientes puntos de partida para descubrir algunas otras propiedades de $\mathbb{Z}_m$.

2. El dominio entero $\mathbb{Z}_p$

Una afirmación que se realizó en la primer lectura, cuando se presentó por primera vez el concepto de anillo, consistió en dar por hecho que existían otros ejemplos. En la sección anterior se mostró que ejemplos existen en abundancia (tantos como enteros existan), pero poco o nada se habló de estos como dominios enteros. En esta sección mostraremos, continuando la discusión de los enteros módulo m, que existen otro dominios enteros diferentes de $\mathbb{Z}$ y también que no todos los anillos forman un dominio entero.

Vamos a mostrar primero que no todos los enteros módulo m son en efecto un dominio entero y para esto basta mostrar un caso en particular. Habrá que identificar primero que $[0]_m$ es el neutro aditivo, esto quiere decir que si $\mathbb{Z}_m$ no es un dominio entero, entonces existen enteros $a \neq 0$ y $b \neq 0$ que no sean múltiplos de m de forma que

$$[a]_m \cdot [b]_m = [0]_m.$$

Esto se puede alcanzar con $m = 6$ pues

$$[3]_6 \cdot [4]_6 = [12]_6 = [0]_6.$$

Por lo que nos vemos obligados a concluir que $\mathbb{Z}_6$ no resulta en dominio entero, mostrando que no todos los anillos son dominios enteros y que en efecto, esa propiedad es una adición importante para el anillo $\mathbb{Z}$.

Esto nos abre la puerta para preguntar bajo qué condiciones $\mathbb{Z}_m$ resulta en un dominio entero. En otras palabras, para que enteros $m > 1$, se tiene que

$$[a]_m \cdot [b]_m = [0]_m$$

implica que $[a]_m = [0]_m$ o $[b]_m = [0]_m$. Si observamos detenidamente el ejemplo para $m = 6$, veremos que el problema se presenta al tener 6 un divisor entre sus residuos distinto de 1 y de sí mismo, lo que nos debe llevar a considerar que quizá la situación se resuelva si pedimos que el módulo no tenga más divisores que uno y sí mismo. En efecto, los números primos no sólo serán suficientes sino necesarios para obtener dominios enteros y el resultado no es en absoluto nuevo, se trata en realidad del lema de Euclides y su corolario descritos en la lectura 3.

Teorema A.5. *El entero $m > 1$ es primo si y sólo si $\mathbb{Z}_m$ es un dominio entero.*

Demostración. Mostremos primero que la condición impuesta es suficiente, para esto debemos suponer a m primo. Notamos primero que

$$[a]_m \cdot [b]_m = [0]_m,$$

implica que $ab \equiv 0 \mod m$ o lo que es lo mismo $m \mid ab$; por el lema de Euclides, $m \mid a$ o $m \mid b$, o de manera equivalente $[a]_m = [0]_m$ o $[b]_m = [0]_m$. En resumen, si $[a]_m \cdot [b]_m = [0]_m$, entonces $[a]_m = [0]_m$ o $[b]_m = [0]_m$, lo que indica que $\mathbb{Z}_m$ es un dominio entero.

Supongamos ahora que $\mathbb{Z}_m$ es un dominio entero. Mostraremos que $m \mid ab$ siempre implica que $m \mid a$ o $m \mid b$; en efecto, si $m \mid ab$, entonces

$$[a]_m \cdot [b]_m = [0]_m,$$

lo que implica que $[a]_m = [0]_m$ o $[b]_m = [0]_m$, o lo que es lo mismo $m \mid a$ o $m \mid b$. Por el corolario al lema de Euclides, debemos concluir que m es primo. ∎

Como el teorema anterior afirma, los enteros módulo algún primo son especiales por resultar ser dominios enteros. Esta caracterización nos lleva a considerar una convención: Cuando escribamos $\mathbb{Z}_m$ se considerará m como un número compuesto, mientras al escribir $\mathbb{Z}_p$ se tomará p como un número primo. Esta convención nos permite, usando el teorema anterior, afirmar que $\mathbb{Z}_p$ es un dominio entero, mientras $\mathbb{Z}_m$ no lo es.

3. Unidades en $\mathbb{Z}_m$

Para explorar el segundo punto, debemos definir a nos referimos con unidad en $\mathbb{Z}_m$, notando que nos interesa explorar con ésta los elementos que poseen inverso, presentamos una definición de unidad para $\mathbb{Z}_m$.

Definición A.3. Un elemento $[a]_m$ de $\mathbb{Z}_m$ se dice *una unidad de* $\mathbb{Z}_m$ si existe un entero b de forma que

$$[a]_m \cdot [b]_m = [1]_m$$

La definición sólo hace lo obvio al definir una unidad de la misma manera que en los enteros, pero es de nuestro interés traducir el enunciado a nuestra instancia particular para preguntar bajo qué condiciones podemos encontrar enteros a y b de forma que

$$ab \equiv 1 \mod m.$$

¡Pero ya hemos hecho esa pregunta antes! El corolario 3.19 responde que eso sólo pasa si y sólo si $(a, m) = 1$. Así, la ecuación

$$[3]_9 \cdot [x]_9 = [1]_9$$

no tiene solución, pero la ecuación

$$[4]_9 \cdot [x]_9 = [1]_9$$

esta obligada a tener una. No es difícil concluir de estas afirmaciones que en $\mathbb{Z}_9$ la ley de cancelación del producto no es válida, pues por ejemplo es cierto que

$$[3]_9 \cdot [6]_9 = [18]_9 = [9]_9 = [3]_9 \cdot [3]_9$$

pero

$$[3]_9 \neq [6]_9.$$

El párrafo anterior nos ruega a preguntar si en alguno de los conjuntos $\mathbb{Z}_m$, todos los elementos de distintos de $[0]_m$ son unidades. No debe ser sorprendente a esta altura afirmar que existe un conjunto de este tipo: $\mathbb{Z}_p$. Vamos agregar cierta terminología para presentar este resultado de una manera adecuada.

Definición A.4. Denotamos el *el conjunto de unidades en* $\mathbb{Z}_m$ como $\mathbb{Z}_m^*$.

En el ejemplo para módulo 9, podemos simplemente afirmar que $[3]_9 \notin \mathbb{Z}_9^*$, así como $[4]_9 \in \mathbb{Z}_9^*$. Además tenemos que

$$\mathbb{Z}_7^* = \{[1]_7, \ldots, [6]_7\}.$$

Aunque la notación parezca algo convulsionada, este par de ejemplos encierran cuan simple un enunciado puede ser redactado en la terminología adecuada. Es importante aprender a desenredar la notación pues ésta encierra el completo significado de los objetos de interés.

Para continuar con la discusión necesitamos comentar el resultado expuesto por el ejercicio 3.1[2] en el que se da una condición suficiente y necesaria para que un número sea primo relativo con un primo. En particular debemos notar que si $a < p$, entonces $p \nmid a$ y consecuencia $(a, p) = 1$. De acuerdo al corolario 3.19 esto es condición suficiente y necesaria para obtener la solución de la congruencia

$$ax \equiv 1 \mod p.$$

Traduzcamos esto a la notación de los enteros módulo p.

Teorema A.6. *Para un un primo p, si $[a]_p \neq [0]_p$, entonces $[a]_p$ es una unidad.*

Demostración. Comencemos aplicando el teorema de la división sobre a y p, encontrado enteros q y $0 \leq r < p$ de forma que $a = qp + r$. Ahora, si $r = 0$, entonces $a \equiv 0 \mod p$ obteniendo que $[a]_p = [0]_p$, lo que debido a la hipótesis, es imposible y concluimos que $r \neq 0$. En ese caso como $r < p$, tenemos que $p \nmid r$ y en consecuencia $(p, r) = 1$. De acuerdo al corolario 3.19, existe un entero s tal que

$$rs \equiv 1 \mod p.$$

Pero $[a]_p = [r]_p$, que junto a la anterior igualdad implica que

$$[a]_p \cdot [s]_p = [1]_p$$

indicando que $[a]_p$ es una unidad, probando el resultado. ∎

Este resultado muestra que el conjunto de los enteros $\mathbb{Z}_p$ pose más estructura que la de un simple anillo pues todos sus elementos tienen la posibilidad de definir un inverso. Esta es en realidad una nueva estructura algebraica.

Definición A.5. Un anillo conmutativo R en el que todos sus elementos distintos de 0_R tienen inverso multiplicativo, se dice *un campo* o *cuerpo*.

Corolario A.7. *Para un primo p cualquiera, $\mathbb{Z}_p$ es un campo.*

4. El pequeño teorema de Fermat

Concluiremos presentando un interesante resultado conocido como *el pequeño teorema de Fermat*, haciendo referencia a Pierre de Fermat, quien lo enunció en una carta. La prueba, aunque no es difícil, requiere de algunos resultados muy específicos de divisibilidad y congruencias, por lo que habrá que regresar un poco sobre nuestro pasos para presentar una series de resultados.

Proposición A.8. *Si p es un número primo, entonces para todo $0 < j < p$, se tiene*

$$p \left| \binom{p}{j} \right.$$

[2]Si no lo has hecho, corre, hazlo, aquí esperamos. Prometemos no avanzar sin ti.

Demostración. Debemos primero recordar la definición de combinación, en este caso

$$\binom{p}{j} = \frac{p!}{j!(p-j)!}$$

o lo que es lo mismo

$$j!\binom{p}{j} = \frac{p!}{(p-j)!} = p(p-1)\dots(p-j+1)$$

de lo que podemos concluir que

$$p \left| j!\binom{p}{j} \right.$$

Por otro lado, si $p \mid j!$, entonces p divide a alguno de los factores $1, \dots, j-1$ o j. Pero $j < p$ por lo que p no puede dividir a ninguno de éstos por lo que debemos entonces concluir que $p \nmid j!$.

Usando el lema de Euclides en enunciado final del primer párrafo, debemos tener que $p \mid j!$ o $p \left| \binom{p}{j} \right.$. Pero la conclusión del segundo párrafo nos lleva concluir que la primera posibilidad es imposible, lo que garantiza el enunciado que buscamos. ■

Proposición A.9. *Para cualquier primo p y enteros a y b, se tiene*

$$(a+b)^p \equiv a^p + b^p \mod p.$$

Demostración. Es necesario aplicar el teorema del binomio:

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

éste nos permite concluir que

$$(a+b)^p - (a^p + b^p) = \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k.$$

Pero

$$\binom{p}{k} \equiv 0 \mod p$$

para todo $0 < k < p$, por lo que el lado derecho de la igualdad resulta un múltiplo de p lo que permite concluir que

$$(a+b)^p \equiv a^p + b^p \mod p.$$

■

La proposición anterior nos informa que el teorema del binomio módulo un primo presenta una forma extremadamente simple y conveniente, de hecho, de esta verdad se desprende el llamado pequeño teorema de Fermat.

Teorema A.10 (Fermat)**.** *Si p es un primo entonces para cualquier entero a,*

$$a^p \equiv a \mod p$$

Demostración. Probaremos primero el resultado para $a \geq 0$ usando inducción. El caso base $a = 0$ es elemental, supongamos entonces que

$$a^p \equiv a \mod p.$$

Por la proposición anterior

$$(a+1)^p \equiv a^p + 1 \mod p$$

lo que combinado con la hipótesis de inducción resulta precisamente en

$$(a+1)^p \equiv a + 1 \mod p.$$

Por inducción el resultado sigue para todo entero $a \geq 0$. Para probar el resultado para un entero $a < 0$, usaremos el párrafo sobre $-a$, i.e., tenemos que

$$(-a)^p \equiv -a \mod p.$$

Partiremos el análisis en dos casos: para $p = 2$ y $p \neq 2$.

Si por un lado $p = 2$, como $-a \equiv a \mod p$, entonces $(-a)^2 \equiv a \mod p$ y como $a^2 = (-a)^2$, podemos concluir $a^2 \equiv a \mod p$ como afirma el resultado.

Supongamos ahora que $p \neq 2$. Como p es primo, este debe ser impar. Esto implica que

$$(-a)^p = (-1)^p a^p = -a^p$$

y en ese caso

$$\begin{aligned} a^p &\equiv -a^p \\ &\equiv (-a)^p \\ &\equiv -a \\ &\equiv a \mod p. \end{aligned}$$

De lo anterior sigue el resultado para $p \neq 2$ y con esto concluye la prueba. ∎

Por la forma en que se presenta el teorema anterior, es tentador enunciarlo usando clases de equivalencia, el siguiente corolario resalta este hecho, la prueba se deja como ejercicio y consiste simplemente en verificar las definiciones de los enteros modulo p.

Corolario A.11.

$$([a]_p)^{p-1} = \begin{cases} [0]_p & si\ p \mid a \\ [1]_p & si\ p \nmid a \end{cases}$$

Como comentario final, es de notar que muchos de los resultados expuestos son en realidad consecuencia de un estudio más abstracto contenido en la teoría de anillos. De hecho, casi todas las construcciones que se han hecho sobre $\mathbb{Z}$, se pueden realizan sobre un anillo cualquier, incluida la descomposición prima. Tendremos oportunidad después de ver en la teoría de polinomios este mismo resultado lo que abrirá paso a una teoría mucho más general.

Ejercicios

Ejercicio A.1. Encuentra el entero $0 \leq r < m$ que es capaz de representar a las siguientes clases de equivalencia.

1. $-[3]_6$
2. $-[7]_9$
3. $-[9]_{10}$
4. $([5]_7)^{-1}$
5. $([10]_{11})^{-1}$
6. $([4]_9)^{-1}$

Ejercicio A.2. Prueba que el conjunto de los enteros módulo m es un anillo conmutativo.

Ejercicio A.3. Demuestra que la ley de cancelación de la suma es válida en $\mathbb{Z}_m$. ¿Es válida en cualquier anillo conmutativo? Sugerencia: No te dejes engañar, la prueba de esta ley en $\mathbb{Z}$ no tiene nada de especial.

Ejercicio A.4. En un anillo conmutativo R decimos que a es un divisor de cero si existe un elemento b del anillo de forma que $ab = 0_R$. Muestra que si m es compuesto, entonces $\mathbb{Z}_m$ tiene al menos un divisor de cero.

Ejercicio A.5. Define el concepto de unidad para un anillo conmutativo R cualquiera.

Ejercicio A.6. Muestra que el producto entre unidades es cerrado, i.e., si a y b son unidades de un anillo conmutativo, entonces $a \cdot b$ es también una unidad.

Ejercicio A.7. Usando un anillo $\mathbb{Z}_m$ muestra que la suma de unidades no es necesariamente una unidad. Sugerencia: Para conseguir esto, debes dar un contraejemplo.

Ejercicio A.8. Prueba que un número primo distinto de 2, es impar.

Ejercicio A.9. Prueba el corolario A.11.

Referencias

[CLRT90] Cárdenas, Humberto, Luis, Emilio, Raggi, Francisco y Tomás, Francisco: *Álgebra Superior*. Editorial Trillas, 1990.

[Rot05] Rotman, Joseph J.: *A first course in abstract algebra*. Pearson, 3ª edición, 2005.

Considerar notas el texto precedente es producto de la imaginación febril de autor. El único propósito al que sirven es dar una interpretación personal de algunos textos que han sido usados para preparar el curso de «Matemáticas discretas» impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Es muy probable que el presente texto esté lleno de errores gramaticales, imprecisiones técnicas y sea sujeto a cambios constantes.