El estudio de $\mathbb{Z}_n$ en secundaria

Félix Núñez y Geovany Sanabria

Resumen

Se aborda el estudio del conjunto $\mathbb{Z}_n$ en secundaria, tratando de aportarle a los docentes en matemáticas, una manera de trabajar en el aula con este conjunto. Dicha propuesta es presentada desde una perspectiva constructivista y en el contexto de la Teoría de Situaciones de Brousseau.

Palabras claves: Didáctica, divisiblidad, situaciones didácticas, algebra modular.

1 Introducción y Justificación

Los programas de estudios de la Enseñanza General Básica de Costa Rica, específicamente en el nivel de sétimo año, están los contenidos que tiene que ver con el estudio de los conjuntos de $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$. Al abordarlos, se suelen solapar sus propiedades algebraicas en lo que concierne a las operaciones de suma y multiplicación.

Al mismo tiempo, tópicos como la divisibilidad, módulos y factorización en $\mathbb{N}$ y $\mathbb{Z}$ son mancillados y algunos transformados en recetas que los estudiantes memorizan sin justificación. Muy pocos alumnos saben justificar la regla de divisivibilidad del 3 y algunos se verían en problemas tratando de determinar si un número negativo es o no divisible por 3, por ejemplo: en el caso de -1496, no faltará quien cometa el error de realizar la suma $-1+4+9+6=18$ y concluir que dicho número es divisible entre 3, cuando a todas luces no lo es.
Por otro lado, las propiedades algebraicas de las operaciones usuales, así como también la factorización y divisibilidad en los conjuntos numéricos que correspondan, constituyen temas generalizados en el estudio del álgebra. Por eso, parece natural pensar que dichos tópicos deben ser bien desarrollados y justificados dentro de los conjuntos numéricos, en tanto que permitiría un paso menos brusco al estudio de la misma.

De lo anterior, surge esta propuesta sobre cómo abordar el estudio del conjunto $\mathbb{Z}_n$ en secundaria, tratando de aportarle a los docentes en matemáticas, una manera de trabajar en el aula con este conjunto. Dicha propuesta es presentada desde una perspectiva constructivista y en el contexto de la Teoría de Situaciones de Brousseau. El docente encontrará aspectos

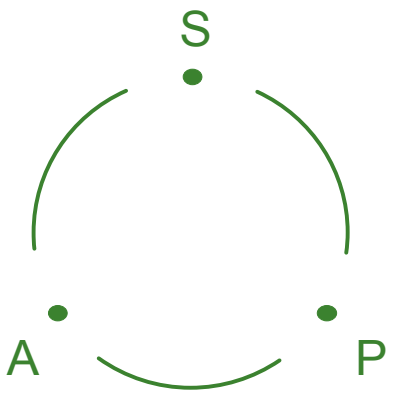

Figure 1:

generales que pueden fungir como base para elaborar situaciones didácticas, así como también justificaciones matemáticas de los procedimientos señalados y de las creaciones didácticas.

En la primera parte se definen los conjuntos $\mathbb{Z}_n$ y sus operaciones de suma y producto. En una segunda parte se estudian las propiedades algabraicas de dichas operaciones. Finalmente, se aborda la divibisibilidad por medio de la estructura de anillo de $\mathbb{Z}_n$.

Teoría de situaciones

En los años ochentas, en Francia, Ives Chevallard (1998) planteó la posibilidad de que la didáctica de la matemática fuera considerada como ciencia. Para ello, era indispensable que tuviera un objeto de estudio, con un determinismo propio el cual fuera necesario investigar. Es así que se adoptó el enfoque sistémico, tomado de las ciencias sociales, en el que se analizan los fenómenos desde una perspectiva global. De esta manera, surge la necesidad de incluir en el viejo modelo enseñanza-aprendizaje, al saber, modelo en el cual se englobaban los fenómenos didácticos . Como el saber forma parte de la globalidad de los fenómenos didácticos a estudiar, y el enfoque sistémico es el adoptado, era necesario incluirlo en la problemática, y es de esta manera que el objeto de estudio de la didáctica de la matemática es el sistema didáctico (o terna didáctica), el cual Chevallard (1998) define como el juego que se da entre un profesor, unos alumnos y un saber.
A partir de allí, la didáctica de la matemática se entiende como el estudio de un sistema didáctico y todas las interrelaciones entre sus componentes.
A manera de esquema, se puede ver así:

Sistema Didáctico, donde S es el saber, A el alumno y P el profesor.

Es por ello que cuando se analiza un fenómeno didáctico se hace desde tres componentes:
- Cognitivo: Desde el polo del alumno
- Epistemológico: Desde el polo del saber
- Pedagógico: Desde el polo del profesor, el cual tiene sus propias concepciones acerca de lo que es la enseñanza

Desde el polo epistemológico, Chevallard (1998) distingue un fenómeno llamado la transposición didáctica, que corresponde a todas las transformaciones que sufre el conocimiento científico escogido para ser apto de enseñar.

La teoría de campos conceptuales, es una teoría cognitiva que pretende brindar un marco teórico coherente y algunos principios de base para entender, desde la perspectiva del autor, Gérard Vergnaud (1990), cómo es que el estudiante aprende, cómo es que se dan las filiaciones y rupturas entre los conocimientos, especialmente en los niños y adolescentes, ya que en los adultos, afirma, el aprendizaje se da más por hábitos.
Vergnaud (1990) no se plantea cómo mejorar el aprendizaje de un determinado concepto, sino que más bien, teoriza sobre cómo es que se da el aprendizaje de la población mencionada, en las ciencias y técnicas principalmente.
Es claro que las estructuras de pensamiento son muy complicadas de entender y explicar, por lo que es menester ubicarse en la perspectiva del autor, sin que esto quiera decir que así es como sucede el aprendizaje del niño y el adolescente.
Por otro lado, Guy Brousseau (1986) aborda el problema de la didáctica de la matemática desde la perspectiva constructivista con una teoría llamada teoría de situaciones, cuyos elementos son las situaciones didácticas y el contrato didáctico. Estos trabajos se ubican en la perspectiva pedagógica, y es en ella donde centraremos la atención.
Situaciones didácticas
Como dijimos anteriormente, Guy Brousseau (1986) estudia el problema de la didáctica de la matemática desde una perspectiva constructivista, con su teoría de situaciones. Un postulado piagetiano establece que el niño aprende por adaptación al medio, que es factor de contradicciones, de dificultades y desequilibrios. Tal aprendizaje se manifiesta por respuestas nuevas que son la prueba del aprendizaje. Brousseau (1986) toma ese postulado piagetiano pero lo modifica puesto que para él esa forma natural de aprender, es insuficiente para transmitir un cúmulo de conocimientos culturales, además, corre el riesgo de liberar al docente de toda responsabilidad. Debe existir una intención de enseñar algo. Es por ello que Brousseau (1986) propone que sea el profesor quien proporcione el medio a través del cual el niño deba lograr el aprendizaje. Por eso, poner en situación al alumno no debe ser tan al natural, sino que debe haber una intencionalidad didáctica (implícita o explícita) . De ahí que él modifica el concepto de situación en la que el niño piagetiano es enfrentado, para dar paso al concepto de situación didáctica, que es "un conjunto de relaciones establecidas explícita y/o

implícitamente entre un alumno o un grupo de alumnos, un cierto medio (que comprende eventualmente instrumentos y objetos) y un sistema educativo (representado por el profesor) con la finalidad de lograr que estos alumnos se apropien de un saber constituido o en vías de constitución" Brousseau (1986).
Es el profesor quien pone al alumno en interacción con el medio y al hacerlo "devuelve" al estudiante en situación a-didáctica, la responsabilidad de su propio aprendizaje. Esta etapa se dice a-didáctica, porque el profesor al poner en juego al estudiante con el medio (el problema propuesto, la situación asignada), se le coloca a distancia con el conocimiento que se le desea enseñar. La solución encontrada al problema propuesto, es el conocimiento que se quiere que el alumno aprenda en situación a-didáctica. En esta etapa, es decir, en esa donde el profesor logre la "devolución", se dan situaciones de formulación y validación, en la que el estudiante ensaya, falla, corrige y se supera. Una vez que logra resolver el problema, si es que lo logra, el profesor en la etapa de institucionalización, enuncia el resultado obtenido por el estudiante. De alguna manera, el profesor va en el sentido inverso del matemático que investiga, puesto que el matemático tiene un resultado, lo publica, borrando las huellas que lo llevaron a descubrirlo, es decir descontextualizando, despersonalizando, destemporalizando, para que el conocimiento nuevo, tengan validez en el tiempo y sea lo más general posible. El profesor al proponer el problema a los estudiantes, debe de alguna manera recontextualizar, repersonalizar, y retemporalizar, para que la clase funcione como una comunidad científica en pequeñito, y recorran de alguna manera el camino que llevó al matemática a descubrir tal resultado que desea enseñar. La elección de un buen problema es pues piedra angular en esta teoría.
¿Cuándo es que hay aprendizaje? Para Brousseau, el aprendizaje se da, cuando en un medio a-didáctico, es decir fuera del contexto escolar, el estudiante es capaz de aplicar lo que aprendió. Esta idea está muy ligada con la dialéctica herramienta-objeto de Régine Douady (). Para ella, un estudiante sabe matemáticas no sólo si sabe definiciones y teoremas de un corpus matemático (objetos) sino que también, que pueda utilizarlos como herramientas en otra situación. Por ejemplo, si es capaz de derivar bien una función, como también de reconocer el concepto de derivada de una función como herramienta para resolver problemas de máximos y mínimos. En nuestro caso, deseamos que el estudiante pueda comprender y aplicar las nociones de las operaciones de $\mathbb{Z}_n$,por ejemplo, en criptografía.
Puede darse el caso que el estudiante no quiera interactuar con el problema, es decir que no se logre la devolución, por eso Brousseau (1986) inserta en su teoría, la noción de contrato didáctico, que es el conjunto de deberes y derechos tanto de unos como de otros, es tácito, establece lo que esperan los estudiantes del profesor y viceversa. Si el estudiante no acepta la devolución, es decir sino se interesa en el problema, el contrato didáctico se rompe, y se busca otra alternativa, con el afán de interesar al estudiante y sacarlo de una situación de bloqueo, y un nuevo contrato didáctico rige la situación didáctica. Brousseau habla de tener cierto cuidado, porque con el afán de interesar al estudiante en situación de bloqueo, el profesor

puede caer en ciertos efectos que de alguna manera, los profesores los hemos vivido: efecto Topaze, efecto Jourdain, deslizamiento metacognitivo, el envejecimiento de las situaciones de enseñanza

Efecto Topaze: Este efecto se da cuando el maestro comienza a dar pistas al alumno para resolver algún problema propuesto, y termina dando casi o inclusive la respuesta al problema, en este caso los conocimientos pretendidos desaparecen completamente.

Ejemplo

Se ve el tema de resolución de ecuaciones cuadráticas, y se presenta al estudiante la siguiente ecuación: y se le plantea resolverla, el alumno no capta como resolverla, y el maestro empieza a dar pistas: Mira que tiene un 2 sobre la x, también tiene la forma ; pero el alumno no atina como resolverla, por último el maestro le dice que utilice la fórmula general. En este momento el maestro ha disimulado su respuesta dando la solución al problema.

Efecto Jourdain: Se da a causa de evitar el debate del conocimiento o un fracaso entre el profesor y el alumno, el primero admite reconocer un conocimiento en el comportamiento o en las respuestas del alumno, aun cuando ellas estén de hecho motivadas por causas diferentes a las pretendidas.

Ejemplo

El maestro pide al alumno factorizar esperando que el alumno reconozca la diferencia de cuadrados. El alumno dice al maestro que la x está al cuadrado y que el 1 se puede ver al cuadrado también, pero no sabe que hacer al 25, pero el profesor se adelanta y le dice que ya tiene la respuesta, que ya la resolvió, y le muestra . Es aquí donde el maestro admite reconocer un conocimiento en el alumno el cual tenía un significado trivial.

El deslizamiento metacognitivo: En el momento en que una situación de enseñanza ha fracasado, el profesor convierte los medios de enseñanza en objeto de estudio, sustituyendo el verdadero conocimiento matemático.

Ejemplo

El paso de utilizar los diagramas de Venn como medios para la comprensión de conjuntos u operaciones sencillas sobre éstos, a utilizarlos como objetos de estudios pidiendo a un alumno que represente mediante diagramas de Venn una operación de conjuntos más compleja.

El uso abusivo de la analogía: Se utiliza cuando los alumnos han fracasado en su aprendizaje, entonces el profesor propone problemas en los cuales sus soluciones se pueden encontrar por procedimientos ya conocidos impidiendo una implicación personal del alumno en el problema. Su utilización puede producir efectos “Topaze”.

Ejemplo

Se plantean varios ejercicios a los estudiantes, los cuales tienen el mismo procedimiento de resolución (algoritmo) que los ejemplos presentados anteriormente.

Por otro lado, considerar la enseñanza como la devolución de una situación del profesor al alumno, permite dice Brousseau (1986) identificar algunas paradojas, que es bueno considerar.

Devolución de las situaciones: El profesor debe en todo momento lograr que el estudiante

resuelva los problemas que él le propone para cumplir con su parte, (el contrato lo obliga enseñar un conocimiento), pero esto puede conducir a una contradicción: el profesor está en la obligación social de enseñar todo lo que concierne al saber al alumno. Si el profesor dice todo al estudiante, sobre todo cuando este ha fracasado, lo priva de todo el proceso de ensayo, fallo, corrección y superación y por tanto no hay aprendizaje. Pero si el estudiante rechaza todo tipo de información que proviene del profesor, la relación didáctica se rompe.

Adaptación de las situaciones

Inadaptación a la exactitud: En ciertas ocasiones el conocimiento se construye por etapas debido a que no hay suficientes situaciones, en estas etapas hay aproximación y cierta inexactitud entre el aprendizaje logrado y el conocimiento cultural.

En la primera etapa el profesor debe decidir si da el conocimiento, renunciando a la enseñanza por adaptación, es decir, da una clase magistral, y renuncia así a darle sentido a un saber, o enseña un saber más o menos inexacto que luego será preciso corregir.

No obstante si se recurre a la memorización de conocimientos formales repercutirá en el hecho de que el alumno no será capaz de aplicar el conocimiento, puesto que éste se ha transmitido por medio de ejercicios que carecen de sentido para él.

Inadaptación a la exactitud: El primer saber se convierte en un gran obstáculo para poder comprender y aprender el siguiente. Por ejemplo, la suma de fracciones en el conjunto de los números racionales, que requiere de las operaciones de los enteros.

Desarrollar un conocimiento a través de etapas presenta inconvenientes en el sentido de que es difícil cambiar un conocimiento falso que ha sido "bien" adquirido.

Aprendizaje por adaptación

Negación del saber: se produce por el hecho de que el estudiante puede resolver el problema con conocimientos anteriores, lo que le hace pensar que no tiene nada nuevo que aprender. El ve insignificante el asunto de lo que ya conoce la respuesta ya que desconoce si a otros se lo han planteado antes, o si no respondieron o si lo que él sabe sirve de base para probar otros resultados, es necesario que alguien de afuera (el profesor probablemente), venga a marcar sus actividades. Parece entonces responsabilidad del profesor relacionar estos saberes con otros, pero este trabajo en el fondo es lo que se esperaba que hiciera el estudiante (como científico en "pequeñito"), por lo que no hay entonces un resultado producido por la adaptación del alumno.

Destrucción de su causa: Al tratar de adaptarse el alumno encuentra un reto: angustia y placer, pero la solución espontánea de la situación destruye la motivación y el conocimiento pierde significado. Se da cuando las situaciones a-didácticas son repetitivas, lo que ocasiona que el estudiante se desmotive y pierda el interés por resolver un problema propuesto.

Paradoja del actor comediante: El profesor que hace de actor y espectador formulando él mismo las preguntas y respuestas tratando de perfeccionar así su técnica, le quita al alumno la posibilidad de hacerlo, perdiéndose un enorme recurso de solución de problemas. La mayéutica socrática prtendía obtener el conocimiento a través de preguntas y respuestas,

entre el maestro y el alumno. Pero Brousseau dice que la participación del profesor sea mínima, y que esas preguntas y respuestas se las haga el mimso estudiante en situación a-didáctica

2 El conjunto $\mathbb{Z}_n$ y sus operaciones

2.1

Vamos a tratar de ejemplificar las ideas anteriores estableciendo las operaciones en el conjunto $\mathbb{Z}_n$. Para ello, es necesario recordar primero el algoritmo de la división. Este señala que dados cualesquiera números enteros a y b $(b > 0)$, llamados respectivamente dividendo y divisor, existen para a y b, dos números enteros únicos c y r, llamados respectivamente conciente y residuo que cumplen

$$a = bc + r, \quad donde \quad 0 \leq r < b,$$

es decir,

$$a \div b = c + (r \div b), \quad donde \quad 0 \leq r < b$$

Así, se podrían realizar algunas divisiones antes de iniciar el tema, haciendo énfasís en que el residuo debe ser mayor o igual que cero y menor que el divisor para que se cumpla la unicidad, por ejemplo:

$$\begin{array}{r|l} -10 & 4 \\ \hline -(-12) & \\ \hline 2 & -3 \end{array}$$

En el ejemplo anterior note que para que el residuo r cumpla que $0 \leq r < 4$ es necesario que el residuo sea 4.

2.2 Definición del conjunto $\mathbb{Z}_n$

2.2.1 Motivación. (Situaciones adidácticas A)

A partir de la notación siguiente, donde a es cualquier número entero,

$$[a]_5 : \text{ residuo de la división de } a \text{ entre } 5$$

Se le proponen al estudiantes las siguientes situaciones.

1. A1. Determine el valor de $[a]_5$ para todo a entre 5 y 11, y entre -11 y -5.
   A2. ¿Cuáles son los posibles valores de $[a]_5$?
   A3. ¿Qué relación existe entre la pregunta anterior y el algoritmo de la división?

A4. Determine el valor de $[0]_5, [1]_5, [2]_5, [3]_5, [4]_5$.

A5. Determnine si las siguientes igualdades son falsas o verdaderas

$$\begin{array}{ll} [20]_5 = [5]_5 & [67]_5 = [92]_5 \\ [54]_5 = [23]_5 & [48]_5 = [783]_5 \\ [15]_5 = [255]_5 & [7891]_5 = [8561]_5 \end{array}$$

A6. Justifique la siguiente afirmación: Si k es un número entero entre 0 y 5 se cumple una y solo una de las siguientes opciones:

$$[k]_5 = [0]_5 \quad ó \quad [k]_5 = [1]_5 \quad ó \quad [k]_5 = [2]_5 \quad ó \quad [k]_5 = [3]_5 \quad ó \quad [k]_5 = [4]_5 .$$

2.2.2 Los conjuntos $\mathbb{Z}_n$ (institucionalización del conocimiento)

Notación. Dado a un número entero y n un número entero positivo, se denota por $[a]_n$ el residuo obtenido al dividir a entre n.

De acuerdo con el agoritmo de la división, se tiene que el residuo, $[a]_n$, de la división entre a y n, cumple que $0 \leq [a]_n < n$, es decir

$$[a]_n \in \{0, 1, 2, ..., n-1\} \qquad (1)$$

Por otro lado, generalizando la situación a-didáctica $A3$, por el algiritmo de la división, se espera que el estudiante concluya que:

$$[k]_n = k, \quad con \quad k \in \{0, 1, 2, ..., n-1\} \qquad (2)$$

De (1) y (2) se obtiene que

$$[a]_n \in \{[0]_n, [1]_n, [2]_n, ..., [n-1]_n\}.$$

Así, si el estudiante logra lo que se le pedía, se institucionaliza el conocimiento enunciando la siguiente definición:
Definición. Se define el conjunto $\mathbb{Z}_n$ como el conjunto de posibles residuos al dividir cualquier entero entre n. Es decir,

$$\mathbb{Z}_n = \{0, 1, 2, ...n-1\}.$$

Note que por (2) se puede decir que $\mathbb{Z}_n$ puede ser representado por

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, ..., [n-1]_n\}.$$

Dicha resentación la llamaremos en adelante **representación canónica** de $\mathbb{Z}_n$.

De lo contrario, es menester que realice todas las situaciones a las que enfrentado, para que todos estos símbolos resulten naturales. Es decir, que pueda adaptarse a las situaciones propuestas por el profesor.

Ejemplos

1. $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, verifique que $[425]_{\ 5} = 0$ y $[4258]_5 = 3$.

2. $\mathbb{Z}_{20} = \{0, 1, 2, 3, 4, ..., 19\}$, veriffique que $[425]_{\ 20} = 5$ y $[4258]_{20} = 18$.

3. Determine $[-4562]_7$. En este caso no es funcional utilizar el "martillo" para realizar la división y bajar cifra por cifra, como se acostumbra en secundaria. Por lo tanto, se procede a encontrar un número negativo c que multiplicado por 7 sea menor que -4562 en menos de 7 unidades. Notemos que $7 \cdot -600 = -4200$; $7 \cdot -650 = -4550$; $7 \cdot -652 = -4564$, como $-4564 < -4562$, entonces $c = -652$ y corresponde al cociente. Así:

$$\begin{array}{c|c} -4562 & 7 \\ \hline -(-4564) & -652 \\ \hline 2 & \end{array}$$

   Y por lo tanto $[-4562]_7 = 2$.

4. Cambio de representantes en $\mathbb{Z}_n$

   Dado que $[16]_4 = [0]_4$; $[81]_4 = [1]_4$; $[-14]_4 = [2]_4$; $[-9]_4 = [3]_4$, otra representación de $\mathbb{Z}_4$ diferente a la canónica es

$$\mathbb{Z}_4 = \{[16]_4, [81]_4, [-14]_4, [-9]_4\}$$

5. Determinemos por extensión y compresión el conjunto A de todos los enteros a que cumplen que $[a]_6 = [1]_6$. Como $[1]_6 = 1$, la igualdad $[a]_6 = 1$ significa que el residuo de la división de a entre 6 es 1, por el algoritmo de la división existe un entero c que cumple que $a = c \cdot 6 + 1$, por lo tanto

$$A = \{6c + 1 \quad | \quad c \in \mathbb{Z}\} = \{... - 17, -11, -5, 1, 7, 13, 19, ...\}$$

   Es claro que el conjunto por extensión se obtiene sumando y restando de 6 en 6 a partir de 1.

2.2.3 Ejercicios

1. Determine los siguientes residuos

$a)$	$[1254]_5$	$g)$	$[-14]_2$	$m)$	$[1478952]_{100}$
$b)$	$[-5]_3$	$h)$	$[147]_4$	$n)$	$[-125]_{27}$
$c)$	$[8]_7$	$i)$	$[-1478]_{10}$	$o)$	$[-1478952]_{100}$
$d)$	$[56]_8$	$j)$	$[-789]_{13}$	$p)$	$[-5621]_{14}$
$e)$	$[-452]_9$	$k)$	$[456]_{19}$	$q)$	$[14502]_{16}$
$f)$	$[-487]_{12}$	$l)$	$[14792]_{20}$	$r)$	$[150249]_{147}$

2. Determine por extensión y comprensión los conjuntos formados por los enteros a que cumplen

$a)$	$[a]_7 = 3$	$c)$	$[a]_8 = [8]_3$
$b)$	$[a]_4 = [17]_4$	$d)$	$[a]_9 = [-12]_7$

3. Exprese $\mathbb{Z}_n$ para $n = 9$ y $n = 6$ en representación distinta a la canónica.

4. Justifique la veracidad de las siguientes proposiciones

   (a) $\mathbb{Z}_7 = \{[3]_7, [22]_7, [-10]_7, [-56]_7, [-15]_7, [-5]_7, [40]_7\}$

   (b) $\mathbb{Z}_n \subset \mathbb{Z}_m$ si $n \leq m$.

2.3 La suma en $\mathbb{Z}_n$

2.3.1 Motivación (Situaciones a-didácticas B)

1. B1. Determine el valor de $[63]_6, [8]_6, [63+8]_6$

   B2. Primera conjetura:

   ¿Existe alguna relación entre los valores anteriores?. Posiblemente los alumnos llegarán a la siguiente conjetura

   $$[a+b]_n = [a]_n + [b]_n .$$

   B3. Refutación de la primera conjetura: En esta fase de acción, el estudiante debe ser capaz de formular como en la conjetura anterior, pero también debe validar, por lo que

es necesario que en esta fase se dé cuenta que es falsa. El profesor puede proponerle, en caso de bloqueo y sin caer en los efectos mencionados arriba, que

calcule el valor de $[40]_7\,, [76]_7$ y $[40+76]_7$. ¿Se mantiene la conjetura anterior? Se espera que se dé cuenta que es falsa. Si no hay más ideas, podríamos caer en un efecto Topaze, ayudándole un poco, sin decirle la respuesta que

B4. Determine el valor de $[[40]_7 + [76]_7]_7$. ¿Qué modificación sugiere realizarle a la primera conjetura?

Se espera que respondan $.[a+b]_n = [[a]_n + [b]_n]_n$

2.3.2 Definición de la suma (institucionalización del conocimiento)

Se define sobre $\mathbb{Z}_n$ la operación residuo de la suma de residuos por

$$[a]_n \oplus [b]_n = [[a]_n + [b]_n]_n = [a+b]_n$$

Ejemplos.

1. Determine el valor de $[13]_7 \oplus [15]_7$.

   Solución:

   $[13]_7 \oplus [15]_7 = [6]_7 \oplus [1]_7 = [6+1]_7 = [7]_7 = 0$

2. Determine el valor de $[2568]_5$.

   Solución:

   Haciendo uso de la operación anterior, como $2568 = 2560 + 8$ se tiene que

   $$[2568]_5 = [2560]_5 \oplus [8]_5 = [0]_5 \oplus [3]_5 = [3]_5 = 3$$

Con base en los ejemplos y razonaminetos previos, se pretende generalizar que la expresión $[a]_n \oplus [b]_n$ se reduce a $[j]_n \oplus [k]_n$ donde j y k son elementos de $\mathbb{Z}_n,$. por lo tanto basta conocer el funcionamiento de la operación con los valores de $\mathbb{Z}_n$ en representación canónica. Por ejemplo, para el caso de $\mathbb{Z}_7$ se puede realizar la siguiente tabla de los resultados de la operación residuo de la suma:

Tabla de $(\mathbb{Z}_7, \oplus)$

$\oplus$	$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[\mathbf{5}]_\mathbf{7}$	$[6]_7$
$[0]_7$	0	1	2	3	4	5	6
$[1]_7$	1	2	3	4	5	6	0
$[\mathbf{2}]_\mathbf{7}$	2	3	4	5	6	**0**	1
$[3]_7$	3	4	5	6	0	1	2
$[4]_7$	4	5	6	0	1	2	3
$[5]_7$	5	6	0	1	2	3	4
$[6]_7$	6	0	1	2	3	4	5

De dicha tabla se logra ver por ejemplo que $[2]_7 \oplus [5]_7 = [2+5]_7 = 0$ (estos términos se encuentran en negríta en la tabla).

2.3.3 Ejercicios

1. Construya la tabla de $(\mathbb{Z}_3, \oplus), (\mathbb{Z}_5, \oplus)$ y $(\mathbb{Z}_{15}, \oplus)$
2. Determine el valor de las siguientes expresiones

$$\begin{array}{llll} a) & [456]_5 \oplus [42]_5 & d) & [-14]_3 \oplus [489]_3 \\ b) & [345]_6 \oplus [1521]_6 & e) & [-784]_8 \oplus [-458]_8 \\ c) & [123]_4 \oplus [-147]_4 & f) & [46]_9 \oplus ([-46]_9 \oplus [-75]_9) \end{array}$$

2.4 La multiplicación de $\mathbb{Z}_n$

2.4.1 Motivación (Situaciones adidácticas C)

1. Determine el valor de $[63]_6, [7]_6, [63 \cdot 7]_6$
2. Primera conjetura:¿ Existe alguna relación entre los valores anteriores?. Se espera que los alumnos lleguen a la siguiente conjetura

$$[a \cdot b]_n = [a]_n \cdot [b]_n .$$

3. Refutación de la primera conjetura: Se procede como en la suma.

   Calcule el valor de $[41]_7, [5]_7$ y $[41 \cdot 5]_7$. ¿Se mantiene la conjetura anterior?
4. Determine el valor de $[[41]_7 \cdot [5]_7]_7$. ¿Qué modificación sugiere hacerle a la primera conjetura?

   Se espera que concluyan $.[a \cdot b]_n = [[a]_n \cdot [b]_n]_n$

2.4.2 Definición de la suma (institucionalización del conocimiento)

Se define sobre $\mathbb{Z}_n$ la operación residuo de la multiplicación de residuos por

$$[a]_n \odot [b]_n = [[a]_n \cdot [b]_n]_n = [a \cdot b]_n$$

Ejemplos.

1. Determine el valor de $[13]_7 \odot [15]_7$.

   Solución:

   $[13]_7 \odot [15]_7 = [6]_7 \odot [1]_7 = [6 \cdot 1]_7 = [6]_7 = 6$

2. Determine el valor de $[346 \cdot 2568]_5$.

   Solución:

   Haciendo uso de la operación anterior, tenemos que

   $$[346 \cdot 2568]_5 = [346]_5 \odot [2568]_5 = [1]_5 \odot [3]_5 = [3]_5 = 3$$

Al igual que en la operación suma ($\oplus$) basta conocer el funcionamiento de la operación $\odot$ con los valores de $\mathbb{Z}_n$ en representación canónica. Por ejemplo en el caso de $\mathbb{Z}_7$:

Tabla de $(\mathbb{Z}_7, \odot)$

$\odot$	$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[\mathbf{5}]_\mathbf{7}$	$[6]_7$
$[0]_7$	0	0	0	0	0	0	0
$[1]_7$	0	1	2	3	4	5	6
$[\mathbf{2}]_\mathbf{7}$	0	2	4	6	1	**3**	5
$[3]_7$	0	3	6	2	5	1	4
$[4]_7$	0	4	1	5	2	6	3
$[5]_7$	0	5	3	1	6	4	2
$[6]_7$	0	6	5	4	3	2	1

Note por ejemplo que $[2]_7 \odot [5]_7 = [2 \cdot 5]_7 = 3$, estos términos se encuentran en negríta en la tabla.

2.4.3 Ejercicios

1. Construya la tabla de $(\mathbb{Z}_3, \odot), (\mathbb{Z}_5, \odot)$ y $(\mathbb{Z}_{15}, \odot)$

2. Determine el valor de las siguientes expresiones

$a)$ $[456]_5 \odot [42]_5$ $d)$ $[-14]_3 \odot [489]_3$
$b)$ $[345]_6 \odot [1521]_6$ $e)$ $[-784]_8 \odot [-458]_8$
$c)$ $[123]_4 \odot [-147]_4$ $f)$ $[46]_9 \odot ([-46]_9 \odot [-75]_9)$

3 Propiedades de las operaciones en $\mathbb{Z}_n$

3.1 Situaciones a-didácticas D.

1. A1. Realice la tabla de $(\mathbb{Z}_5, \oplus)$

   A2. Determine si existe un elemento n de $\mathbb{Z}_5$ que cumpla que para cualquier $a \in \mathbb{Z}$ se tenga que $[a]_5 \oplus n = [a]_5$. En caso de que tal n exista, determine si existen varios valores para n.

   A3. Determine si para cada $[a]_5$ con $0 \leq a < 7$ existe un valor $[b]_5$ tal que

   $$[a]_5 \oplus [b]_5 = 0$$

   A4. Realice la tabla de $(\mathbb{Z}_6, \oplus)$

   A5. Determine si existe un elemento n de $\mathbb{Z}_6$ que cumpla que para cualquier $a \in \mathbb{Z}$ se tenga que $[a]_6 \odot n = [a]_6$. En caso de que tal n exista, determine si existen varios valores para n.

   A6. Determine si para cada $[a]_6$ con $0 \leq a < 7$ existe otro valor $[b]_6$ tal que

   $$[a]_6 \odot [b]_6 = 1$$

   A7. Finalmente, para establecer el hecho de que $(\mathbb{Z}_n, \odot)$ es un grupo solamente si n es primo, se asigna a cada seis estudiantes construir una tabla diferente de las siguientes:$(\mathbb{Z}_2, \odot)$,$(\mathbb{Z}_3, \odot)$, $(\mathbb{Z}_4, \odot)$, $(\mathbb{Z}_8, \odot)$, $(\mathbb{Z}_7, \odot)$ y $(\mathbb{Z}_9, \odot)$ para luego pedirles que investiguen si para cada $[a]_n$ con $0 \leq a < 7$ existe otro valor $[b]_n$ tal que

   $$[a]_n \odot [b]_n = 1,$$

   según el n que corresponda a cada grupo. Posteriormente se debe completar la siguiente tabla en la pizarra:

	Cumple o no la propiedad
$(\mathbb{Z}_2, \odot)$	si
$(\mathbb{Z}_3, \odot)$	si
$(\mathbb{Z}_4, \odot)$	no
$(\mathbb{Z}_8, \odot)$	no
$(\mathbb{Z}_7, \odot)$	si
$(\mathbb{Z}_9, \odot)$	no

El caso de $\mathbb{Z}_9$ lo pedimos porque una de las cojeturas que podría saltar a la vista es que $\mathbb{Z}_n$ cumple dicha propiedad si n es impar.

3.2 Propiedades de la suma.

1. **Conmutatividad**. Para todo $[a]_n$, $[b]_n$ se tiene que

$$[a]_n \oplus [b]_n = [a]_n \oplus [b]_n$$

Justificación: $.[a]_n \oplus [b]_n = \underbrace{[a+b]_n = [b+a]_n}_{\text{Conmutatividad en } (\mathbb{Z},+)} = [b]_n \oplus [a]_n$

2. **Asociatividad**. Para todo $[a]_n$, $[b]_n$, $[c]_n$ se tiene que

$$[a]_n \oplus ([b]_n \oplus [c]_n) = ([a]_n \oplus [b]_n) \oplus [c]_n$$

Justificación: $.[a]_n \oplus ([b]_n \oplus [c]_n) = [a]_n \oplus [b+c]_n = \underbrace{[a+(b+c)]_n = [(a+b)+c]_n}_{\text{Asociatividad en } (\mathbb{Z},+)} =$ $([a]_n \oplus [b]_n) \oplus [c]_n$

3. **Neutro aditivo.** Para todo $[a]_n$se tiene que

$$[a]_n \oplus 0 = [a]_n$$

Justificación: $.[a]_n \oplus 0 = [a]_n \oplus [0]_n = [a+0]_n = [a]_n$

4. **Inverso aditivo**. Para todo $[a]_n$se tiene que

$$[a]_n \oplus [-a]_n = 0$$

Justificación: $.[a]_n \oplus [-a]_n = [a-a]_n = [0]_n = 0.$

Dado que $(\mathbb{Z}_n, \oplus)$ cumple las propiedades anteriores se dice que es un grupo abeliano.
Ejemplos

1. Determinemos el inverso aditivo de $[417]_5$ en su representación canónica. Este es

$$[-417]_5 = [-420+3]_5 = [-420]_5 \oplus [3]_5 = \underbrace{[0]_5 \oplus [3]_5 = [3]_5}_{[0]_5 \text{ es el neutro de } \oplus}$$

2. Determinemos el valor $[-534]_8 \oplus ([-2]_8 \oplus [534]_8)$. Las propiedades nos permiten simplificar algunos cálculos:

$$\begin{aligned}
&[-534]_8 \oplus ([-2]_8 \oplus [534]_8) \\
&= [-534]_8 \oplus ([534]_8 \oplus [-2]_8) && \text{(Conmutatividad)} \\
&= ([-534]_8 \oplus [534]_8) \oplus [-2]_8 && \text{(Asociatividad)} \\
&= 0 \oplus [-2]_8 && \text{(Inverso aditivo)} \\
&= [-2]_8 && \text{(Neutro)} \\
&= 6
\end{aligned}$$

3.3 Propiedades de la multiplicación

1. **Conmutatividad**. Para todo $[a]_n$, $[b]_n$ se tiene que

$$[a]_n \odot [b]_n = [a]_n \odot [b]_n$$

Justificación: .$[a]_n \odot [b]_n = \underbrace{[ab]_n = [ba]_n}_{\text{Conmutatividad en } (\mathbb{Z}, \cdot)} = [b]_n \odot [a]_n$

2. **Asociatividad**. Para todo $[a]_n$, $[b]_n$, $[c]_n$ se tiene que

$$[a]_n \odot ([b]_n \odot [c]_n) = ([a]_n \odot [b]_n) \odot [c]_n$$

Justificación: .$[a]_n \odot ([b]_n \odot [c]_n) = [a]_n \odot [bc]_n = \underbrace{[a\,(bc)]_n = [(ab)\,c]_n}_{\text{Asociatividad en } (\mathbb{Z}, \cdot)} = ([a]_n \odot [b]_n) \odot [c]_n$

3. **Neutro multiplicativo.** Para todo $[a]_n$se tiene que

$$[a]_n \odot 1 = [a]_n$$

Justificación: .$[a]_n \odot 1 = [a]_n \odot [1]_n = [a \cdot 1]_n = [a]_n$

4. **Inverso multiplicativo**.Si n es primo entonces para todo $[a]_n$ existe un $[v]_n$ que cumple

$$[a]_n \odot [v]_n = 1$$

Justificación: Asumamos el siguiente resultado: si a y b son primos relativos entonces

existen únicos enteros u y v tales que $au + bv = 1$. (1)

Supongamos que $[a]_n = r$ entonces $r < n$ y como n es primo entonces n y r son primos relativos y por (1) se tiene que existen u y v únicos tales que $nu + rv = 1$ y por lo tanto

$$1 = [nu + rv]_n = [nu]_n \oplus [rv]_n = [rv]_n = [r]_n \odot [v]_n = r \odot [v]_n = [a]_n \odot [v]_n ,$$

por lo tanto el inverso multiplicativo de $[a]_n$ es $[v]_n$. Se suele denotar $[v]_n$ por $[a]_n^{-1}$

Finalmente se tiene que la operación $\odot$ distribuye con respecto a $\oplus$, es decir para cualesquiera $[a]_n , [b]_n , [c]_n$ se tiene que

$$[a]_n \odot ([b]_n \oplus [c]_n) = ([a]_n \odot [b]_n) \oplus ([a]_n \odot [c]_n)$$

La justificación es directa a partir de la distributividad en $(\mathbb{Z}, +, \cdot)$ y se deja como ejercicio al lector.

Ejemplos

1. Encontremos el inverso multiplicativo de $[417]_5$ en su representación canónica. Dado que $[417]_5 = [2]_5$, por lo tanto el inverso de $[2]_5 : [v]_5$ cumple que

$$\begin{gathered} [v]_5 \odot [2]_5 = 1 \\ [2v]_5 = 1 \end{gathered}$$

   De esta manera, basta encontrrar un b múltiplo de 2 que al dividirlo entre 5 dé residuo 1 y éste es 6 :

$$\begin{aligned} [2v]_5 &= [6]_5 \\ [v]_5 &= [3]_5 \end{aligned}$$

2. Determinemos el inverso multiplicativo $[v]_{31}$ de $[7]_{31}$ en su representación canónica. En este caso se tiene que

$$\begin{gathered} [v]_{31} \odot [7]_{31} = 1 \\ [7v]_{31} = 1 = [63]_{31} \end{gathered}$$

   por lo tanto $[v]_{31} = [9]_{31}$ (En este ejemplo y el anterior se utilizó la ley de la cancelación la cuál es válida en todo grupo).

3. Determinemos el valor $[-12]_7^{-1} \odot \left([5]_7^{-1} \odot [-1234]_7\right)$. Las propiedades nos permiten

simplificar algunos cálculos:

$$\begin{aligned}
&[-1234]_7^{-1} \odot \left([5]_7^{-1} \odot [-1234]_7\right) \\
&= [-1234]_7^{-1} \odot \left([-1234]_7 \odot [5]_7^{-1}\right) && \text{(Conmutatividad)} \\
&= \left([-1234]_7^{-1} \odot [-1234]_7\right) \odot [5]_7^{-1} && \text{(Asociatividad)} \\
&= 1 \odot [5]_7^{-1} && \text{(Inverso multiplicativo)} \\
&= [5]_7^{-1} && \text{(Neutro)} \\
&= [3]_7
\end{aligned}$$

3.4 Ejercicios

1. Pruebe que el neutro aditivo y el neutro multiplicativo es único
2. Pruebe que el inverso aditivo de $[a]_n$ es único
3. Determine el inverso aditivo en su representación canónica de los siguientes valores

$$\begin{array}{llll} a) & [-789]_6 & d) & [-125]_8 \\ b) & [45]_{32} & e) & [-7894]_5 \\ c) & [478]_4 & f) & [-780000456]_3 \end{array}$$

4. Determine el inverso multiplicativo en su representación canónica de los siguientes valores

$$\begin{array}{llll} a) & [2]_5 & d) & [7]_{17} \\ b) & [37]_7 & e) & [-456]_2 \\ c) & [-11]_3 & f) & [9]_{31} \end{array}$$

5. Simplifique al máximo las siguientes expresiones

$$a) \quad [2]_3 \oplus ([-7]_3 \odot [9]_3)$$

$$b) \quad ([-7]_3 \oplus [2]_3) \odot ([9]_3 \oplus [2]_3)$$

$$c) \quad [-85]_5 \oplus \left([-2]_5^{-1} \odot [87]_5\right)$$

$$d) \quad \left[7^{42}\right]_6 \odot ([-45]_6 \oplus [8]_6)$$

4 Justificación matemática

Tradicionalmente se define $[a]_n = \{b/\exists k \in \mathbb{Z} : b = kn + a\}$, Sin embargo en la presentación anterior se definió la clase como un número y no como un conjunto. Esto podría parecer un error conceptual matemático, no obstante esto tiene su asidero en los siguientes teoremas en los cuales se considera al conjunto $\mathbb{Z}_n$ en su presentación tradicional con las operaciones suma $(+)$ y multiplicación $(\cdot)$

Teorema 1. Sobre $A = \{0, 1, 2, ..., n-1\}$ con las operaciones ya vistas $\oplus$ y $\odot$, .donde $a \oplus b$ es el residuo que se obtiene al dividir $a + b$ entre n, y $a \odot b$ es el residuo de ab entre n. La terna $(A, \oplus, \odot)$ es un anillo conmutativo con unidad.
Prueba.
La demostración es consecuencia directa de la sección 3.

Teorema. Existe un isomorfismo de anillos entre $(\mathbb{Z}_n, +, \cdot)$ y $(A, \oplus, \odot)$

Prueba.

Considere la función $\begin{array}{ccc} \varphi : \mathbb{Z}_n & \longrightarrow & A \\ [a]_n & \longrightarrow & \varphi\left([a]_n\right) \end{array}$, donde $\varphi\left([a]_n\right)$ es el residuo de la división de a entre n.
Probemos que φ es un isomorfismo de anillos.
φ **es un homorfismo de anillos.**
En efecto, supongamos que

$$\varphi\left([a]_n\right) = s, \quad \varphi\left([b]_n\right) = t \qquad (1).$$

De acuerdo al algoritmo de la división existen k_1, k_2 enteros que cumplen

$$a = k_1 n + s, \quad b = k_2 n + t,$$

de donde se obtiene que

$$a+b=(k_1+k_2)\,n+(s+t)\,,\quad ab=(k_1k_2n+k_1t+k_2s)\,n+st$$

Por lo tanto

$$\varphi\left([a+b]_n\right)=\varphi\left([s+t]_n\right),\quad \varphi\left([ab]_n\right)=\varphi\left([st]_n\right),\quad \textit{donde}\quad s,t\in A \qquad (2)$$

Note que $\varphi\left([s+t]_n\right)$ es el residuo de $(s+t)$ entre n y esto es precisamente $s\oplus t$, por lo tanto de (1) y (2) :

$$\varphi\left([a]_n\right)\oplus\varphi\left([b]_n\right)=s\oplus t=\varphi\left([s+t]_n\right)=\varphi\left([a+b]_n\right)$$

De manera similar se tiene

$$\varphi\left([a]_n\right)\odot\varphi\left([b]_n\right)=s\odot t=\varphi\,[st]_n=\varphi\left([ab]_n\right).$$

φ es inyectiva.
Note que

$$\begin{aligned} N(\varphi) &= \{[a]_n/\varphi\left([a]_n\right)=0\} \\ &= \{[a]_n/a \text{ es divisible entre } n\} \\ &= \{[0]_n\} \end{aligned}$$

Por lo tanto φ es inyectiva.
φ es sobreyectiva.
Si $a\in A$ se tiene que $\varphi\left([a]_n\right)=a$.
Se concluye que φ es un isomorfirmo de anillos. y por lo tanto $(A,\oplus,\odot)$ es una copia de $(\mathbb{Z}_n,+,\cdot)$, quedando justificada la presentación dada en las secciones anteriores.

5 Las reglas de divisibilidad.

5.1 Definición de divisibilidad

Se dice que un entero a es divisible por un entero positivo n si el residuo de la división de a entre n es 0 es decir

$$[a]_n=0$$

Ejemplos

1. Note que -12 es divible entre 6 pues $[-12]_6=0$.
2. Como $[-79]_{13}=12$ por lo tanto -79 no es divisible entre 13.

5.2 Notación posicional de un número entero

Todo número entero a puede ser representado por

$$a = a_m 10^m + a_{m-1}10^{m-1} + ... + a_1 10 + a_0, \text{ con } a_m \neq 0$$

donde cada $a_i \in \{-9, -8, -7, ..., 7, 8, 9\}$.
Ejemplos

1. La notación posicional de 2378 es

$$2378 = 2 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10 + 8.$$

2. La notación posicional de -70375 es

$$-70375 = -7 \cdot 10^4 + -3 \cdot 10^2 + -7 \cdot 10 + -5$$

5.3 Reglas de divisibilidad.

Considérese la notación posicional de un número entero a:

$$a = a_m 10^m + a_{m-1}10^{m-1} + ... + a_1 10 + a_0, \text{ con } a_m \neq 0$$

y utilizando la aritmética estudiada deduzcamos algunas reglas de divisibilidad

1. **La divisibilidad entre** 2

$$[a]_2 = \left[a_m 10^m + a_{m-1}10^{m-1} + ... + a_1 10 + a_0\right]_2$$

$$= [a_m]_2 \odot [10^m]_2 \oplus [a_{m-1}]_2 \odot \left[10^{m-1}\right]_2 \oplus ... \oplus [a_1]_2 \odot [10]_2 \oplus [a_0]_2$$

$$= [a_m]_2 \odot ([10]_2)^m \oplus [a_{m-1}]_2 \odot ([10]_2)^{m-1} \oplus ... \oplus [a_1]_2 \odot [10]_2 \oplus [a_0]_2$$

$$= [a_m]_2 \odot 0 \oplus [a_{m-1}]_2 \odot 0 \oplus ... \oplus [a_1]_2 \odot 0 \oplus [a_0]_2 = [a_0]_2 .$$

Por lo tanto el residuo de dividir a entre 2 es $[a_0]_2$, y se ha llegado a la siguiente regla

$$a \text{ es divisible entre 2 si y solo si } [a_0]_2 = 0.$$

2. **La divisibilidad entre** 3

$$[a]_3 = \left[a_m 10^m + a_{m-1}10^{m-1} + ... + a_1 10 + a_0\right]_3$$

$$= [a_m]_3 \odot [10^m]_3 \oplus [a_{m-1}]_3 \odot \left[10^{m-1}\right]_3 \oplus ... \oplus [a_1]_3 \odot [10]_3 \oplus [a_0]_3$$

$$= [a_m]_3 \odot ([10]_3)^m \oplus [a_{m-1}]_3 \odot ([10]_3)^{m-1} \oplus ... \oplus [a_1]_3 \odot [10]_3 \oplus [a_0]_3$$

$$= [a_m]_3 \odot 1 \oplus [a_{m-1}]_3 \odot 1 \oplus ... \oplus [a_1]_3 \odot 1 \oplus [a_0]_3$$

$$= [a_m]_3 \oplus [a_{m-1}]_3 \oplus ... \oplus [a_1]_3 \oplus [a_0]_3$$

$$= [a_m + a_{m-1} + ... + a_1 + a_0]_3$$

Por lo tanto el residuo de dividir a entre 3 es $[a_m + a_{m-1} + ... + a_1 + a_0]_3$, y se concluye

a es divisible entre 3 si y solo si $[a_m + a_{m-1} + ... + a_1 + a_0]_3 = 0$.

3. **La divisibilidad entre** 11.

$$[a]_{11} = \left[a_m 10^m + a_{m-1}10^{m-1} + ... + a_1 10 + a_0\right]_{11}$$

$$= [a_m]_{11} \odot [10^m]_{11} \oplus [a_{m-1}]_{11} \odot \left[10^{m-1}\right]_{11} \oplus ... \oplus [a_1]_{11} \odot [10]_{11} \oplus [a_0]_{11}$$

$$= [a_m]_{11} \odot ([10]_{11})^m \oplus [a_{m-1}]_{11} \odot ([10]_{11})^{m-1} \oplus .... \oplus [a_1]_{11} \odot [10]_{11} \oplus [a_0]_{11}$$

$$= [a_m]_{11} \odot ([-1]_{11})^m \oplus [a_{m-1}]_{11} \odot ([-1]_{11})^{m-1} \oplus ... \oplus [a_1]_{11} \odot [-1]_{11} \oplus [a_0]_{11},$$

$$(pues \quad [10]_{11} = [-1]_{11})$$

$$= \left[a_m \cdot (-1)^m + a_{m-1} \cdot (-1)^{m-1} + ... + a_1 \cdot (-1)^1 + a_0\right]_{11}$$

Por lo tanto el residuo de dividir a entre 11 es

$$\left[a_m \cdot (-1)^m + a_{m-1} \cdot (-1)^{m-1} + ... + a_1 \cdot (-1)^1 + a_0\right]_{11}$$

, y se concluye que a es divisible entre 11 si y sólo si

$$\left[a_m \cdot (-1)^m + a_{m-1} \cdot (-1)^{m-1} + ... + a_1 \cdot (-1)^1 + a_0\right]_{11} = 0.$$

Lo novedoso de lo anterior es que además de justificar algunas reglas de divisibilidad en $\mathbb{Z}$ (no solo en N), nos brinda algoritmos para determinar el residuo de un número a entre n **Ejemplos**.

1. Determine el residuo de -12307 entre 11.Como $-1\,(-1)^4+-2\,(-1)^3+-3\,(-1)^2+-7=-9$ entonces $[-12307]_{11}=[-9]_{11}=2$. Por lo tanto el residuo es 2.

2. Determine el valor de $[-253694]_2$. Por la regla se sabe que $[-253694]_2=[-4]_2=0$, de donde se obtiene que -253694 es divisible en 2.

3. Determine el valor de $[-267]_7$. Se tiene que

$$\begin{aligned}[-267]_7 &= [-2]_7\odot([10]_7)^2\oplus[-6]_7\odot[10]_7\oplus[-7]_7\\ &= [-2]_7\odot([3]_7)^2\oplus[1]_7\odot[3]_7\oplus[0]_7\\ &= [-2]_7\odot[9]_7\oplus[1]_7\odot[3]_7\oplus[0]_7\\ &= [5]_7\odot[2]_7\oplus[1]_7\odot[3]_7\oplus[0]_7\\ &= [10]_7\oplus[3]_7\oplus[0]_7\\ &= [13]_7=6\end{aligned}$$

4. Determine el dígito de las unidades de 9^{428}. El ejercicio se reduce a determinar el residuo dela división de 9^{428} entre 10 :

$$\left[9^{428}\right]_{10}=([9]_{10})^{428}=([9]_{10})^{2\cdot 214}=([81]_{10})^{214}=([1]_{10})^{214}=1,$$

por lo tanto el dígito de las unidades es 1.

5.4 Ejercicios.

1. Determine las regas de divisibilidad entre $5, 9$ y 10..

2. Para cada uno de los siguientes números determine el residuo que se obtiene al dividir estos números entre $2, 3, 5, 7, 9, 10$ y 11.

$a)$	789	$d)$	-1234	$g)$	$25^5+34^3+345\cdot 90$
$b)$	1234	$e)$	-96345	$h)$	-5^4
$c)$	-7845	$f)$	82540	$i)$	-70^{123}

3. Justifique la siguiente afirmaciíon: "Si un número es divisible entre 9 entonces es divisible entre 3". Será cierto que "si un número es divisible entre 3 es divisible entre 9".

6 Comentario final

Pese a que la didáctica de la matemática se ha considerado como ciencia en Francia desde hace más de veinte años, con su objeto de estudio el sistema didáctico, y que se han publicado muchos trabajos en torno de ella, en muchos países de habla hispana se conoce poco al respecto. Costa Rica no escapa a este desconocimiento lo cual viene a representar una debilidad, puesto que todo lo que tenga que ver con propuestas para mejorar la enseñanza de la matemática, deben ser analizadas, ya sea para descartarlas o bien para tomar algunas ideas que puedan ponerse en prática en un contexto muy particular. La didáctica de la matemática francesa, está muy teorizada, y representa un invaluable aporte a los docentes e investigadores en el campo, dado que se desarrolla desde una perspectiva constructivista.
El trabajo realizado es un primer comienzo hacia la necesidad de replantearse los programas de estudio nacionales. Su objetivo es mostrarle al docente una herramienta útil para abordar principalmente los conceptos de inverso y neutro respecto a una operación y al mismo tiempo justificar las reglas de divisibilidad sin hablar de módulos explícitamente.

Se pretende que el docente tome estos apuntes y los adapte para ser objeto de enseñanza de acuerdo a su experiencia, quizás disfrazado por medio de trabajos extraclases debido a que actualmente no es un tema de secundaria.

Generalmente el estudio de $\mathbb{Z}_n$ es muy complicado y demanda una madurez matemática más o menos aceptable de quien la estudia. Es por ello que hemos tratado de establecer, a lo largo de estas páginas, este concepto de la manera más natural y comprensiva. Después de todo esa es una de nuestras obligaciones como docentes: Intentar propuestas didácticas que hagan de la matemática un mundo más sencillo.

Además, este aporte se puede ver a la luz de una concepción futura de ingeniería didáctica, que nace justamente muy ligado a la teoría de situaciones de Brousseau y con el afán de proponer buenas situaciones didácticas. Esperamos que dichos apuntes le sean de gran utilidad al lector.

7 Bibliografía

1. Brousseau, Guy (1986). “Fundamentos y Métodos de la Didáctica de las Matemáticas”, traducción de “Fondements et méthodes de la didactiques des mathématiques”. Revista Recherches en Didactique des Mathématiques, Vol 7, n 2, pp.33-111.

2. Chevallard, Yves (1991). "La Transposición Didáctica. Del saber sabio al saber enseñado". Aique grupo Editor S.A., Argentina.

3. Dorronsoro, José; Hernández, Eugenio. (1996). Números, Grupos y Anillos. Addison-Wesley/ Universidad Autónoma de Madrid, España.

4. Herstein, I. (1988). Álgebra Abstracta. Grupo Editorial Iberoamérica. México, D.F.

5. Artigue, Michèle; Douady, Règine; y otros. 1995. Ingeniería didáctica en educación matemática, Grupo Editorial Iberoamérica, Colombia.

6. Polya, G. 1953. Matemáticas y razonamiento pluasible. Madrid: Tecnos [1966].

7. Vergnaud, G. 1990. "La thèorie des champs conceptuals", Rècherches en Didactique des Mathémathiques 10 (23) : 133-170.