Relime Vol. 7, Núm. 2, julio, 2004 pp. 117-144

Generación del conflicto cognitivo a través de una actividad de criptografía que involucra operaciones binarias[◊]

Priciliano Aguilar[*]
Asuman Oktaç[*]

RESUMEN

Llevar al estudiante a un conflicto cognitivo puede ser una manera de hacerle ver que los conceptos o métodos que maneja no son los adecuados para llegar a una conclusión satisfactoria en la resolución de un problema. Aparte de las discusiones en un ambiente de aprendizaje colectivo y el uso de juegos matemáticos, las situaciones matemáticas deben portar elementos que favorezcan un conflicto y faciliten el enfrentamiento de los conocimientos anteriores con nuevos conocimientos a adquirir. Asimismo, los maestros necesitan tener experiencias directas con este tipo de actividades en su nivel antes de aplicarlas en sus clases. En este artículo reportamos los resultados de una investigación que involucró la aplicación de una actividad de criptografía a grupos de maestros donde los conceptos de *conjuntos* y *operaciones binarias* entraron en juego.

PALABRAS CLAVE: conflicto cognitivo, operaciones binarias, diseño de actividades, criptografía, formación de maestros

Generating cognitive conflict by means of a cryptography activity that involves binary operations

ABSTRACT

Causing a cognitive conflict can be one way to make students aware of the inadequacy of the concepts that they possess and the methods that they use in solving a problem. Apart from discussions in a cooperative group and the use of mathematical games, the mathematical situations themselves have to possess certain characteristics to be able to provoke a conflict and furthermore facilitate the confrontation between the previous knowledge and new knowledge to be acquired. Moreover teachers need to have direct experiences at their level with this kind of activities, before they can employ them in their classes. In this paper we report the results of a study in which a cryptography activity was applied with a group of university and high school teachers, where the concepts of *sets* and *binary operations* came into play.

KEY WORDS: cognitive conflict, binary operations, design of activities, cryptography, teacher training

Provoquer un conflit cognitif à travers une activité de cryptographie qui utilise opérations binaries

RESUMÉ

Amener les étudiants a un conflit cognitif peut être une bonne manière de leur faire se rendre compte que les concepts ou les méthodes qu'ils emploient ne sont pas les plus adéquats dans la résolution d'un problème. À part les discussions dans une ambiance d'apprentissage collaboratif

Fecha de recepción: febrero de 2003
◊ Esta investigación ha sido financiada parcialmente por el proyecto Conacyt 2002-C01-41726
* Unidad Profesional Interdisciplinaria de Ingeniería y Tecnologías Avanzadas del IPN, México.
* Departamento de Matemática Educativa, Cinvestav-IPN, México.

VERSIÓN PRELIMINAR

et l'emploie des jeux mathématiques, les situations mathématiques mêmes devraient porter des éléments qui favorisent le conflit et qui facilitent le confrontation entre les connaissances antérieures et les nouvelles connaissances à acquérir. En outre, les proffesseurs ont besoin d'expériences directes avec ce genre d'activités à leurs niveaux, avant de pouvoir les employer dans leurs classes. Dans cet article, nous rapporterons les resultats d'une recherche dans laquelle une activité de cryptographie a été utilisée avec un group de professeurs, où les concepts *ensembles* et *opérations binaires* entrent en jeu.

MOTS CLÉS: conflit cognitif, opérations binaries, préparation des activités, cryptographie, formation des professeurs

Geração de conflito cognitivo através de uma atividade de criptografía que envolve operações binárias

RESUMO

Levar o estudante a um conflito cognitivo pode ser uma maneira de fazê-lo ver que os conceitos ou métodos que ele utiliza não são adequados para chegar a uma conclusão satisfatória na resolução de um problema. Além das discussões em um ambiente de aprendizagem coletivo e o uso de jogos matemáticos, as mesmas situações matemáticas devem fornecer elementos que favoreçam um conflito e facilitem a utilização dos conhecimentos anteriores com novos conhecimentos a serem adquiridos. Assim mesmo, os professores necessitam de experiências diretas com este tipo de atividades em seu nível, antes de poder aplicá-las em suas salas de aula. Neste artigo apresentamos os resultados de uma investigação que envolve a aplicação de uma atividade de criptografía aos grupos de professores, onde os conceitos de *conjuntos* e *operações binárias* entraram em cena.

PALAVRAS CHAVE: conflito cognitivo, operações binárias, planejamento de atividades, criptografia, formação de professores

1. Antecedentes

1.1. Operaciones binarias y estructuras algebraicas

La comprensión de las operaciones binarias involucra nociones como elemento neutro, elemento inverso, asociatividad, conmutatividad, y cerradura, entre otras. Aún más importante, requiere considerar un conjunto con una operación asociada, noción que pertenece al pensamiento matemático avanzado. Los estudiantes generalmente tienen dificultades para considerar una estructura como un total; la falta de conocimiento y manejo de operaciones binarias tienen sus implicaciones en todo su pensamiento matemático, y especialmente en su pensamiento algebraico.

Estas dificultades se amplían cuando la enseñanza favorece el estudio de cierto tipo de estructuras, dando al estudiante la impresión de que ciertas reglas que poseen estas estructuras son universales y que se pueden aplicar en cualquier contexto. En este sentido, cambiar de contexto le ofrece al estudiante la oportunidad de que trabaje con diferentes estructuras y puede ayudarles a tomar en cuenta que las reglas dependen de las definiciones y los axiomas empleados en cada sistema.

Hay pocos trabajos realizados sobre las concepciones que tienen los estudiantes y los maestros acerca de las operaciones binarias. En su investigación, Brown, et al. (1997), considerando a la operación binaria como una función, hicieron una descomposición genética para describir las concepciones de este concepto en términos de la teoría APOE (Acción- Proceso- Objeto- Esquema). Según esta descomposición, la concepción acción consiste en

VERSIÓN PRELIMINAR

realizar una operación solamente cuando una fórmula explícita es dada. En la concepción proceso, el estudiante piensa en la operación binaria como un proceso que acepta dos objetos y produce un nuevo objeto y, al mismo tiempo, sabe que el conjunto de dominio puede variar. Cuando llega a la concepción objeto, puede pensar en distintas operaciones binarias sobre el mismo conjunto y en varias propiedades que una operación binaria puede tener. Los resultados empíricos que ofrecen Brown, et al., sobre la operación binaria se reducen al análisis de una pregunta de entrevista sobre las simetrías del cuadrado y algunas otras preguntas que se aplicaron, en forma de exámenes a los estudiantes de un curso de álgebra abstracta.

En cuanto a las propiedades que pueden tener las operaciones binarias, Zaslavsky y Peled (1996) reportan un estudio que involucró la generación de contra-ejemplos por los maestros y futuros maestros. En esta investigación, los participantes debían dar un ejemplo de una operación binaria conmutativa, pero no asociativa. Las autoras reportan acerca de la generalización equivocada de las propiedades de las operaciones binarias básicas. Su investigación confirmó un dominio muy limitado de búsqueda que empleaban los participantes.

1.2. Conflicto cognitivo

La noción del conflicto cognitivo se relaciona con un estado de desequilibrio que surge cuando una concepción que tiene un individuo entra en conflicto con alguna otra concepción que lleva el mismo individuo, o bien con el ambiente externo (por ejemplo, el resultado de un experimento, o el punto de vista de un compañero).

Llevar al estudiante a un conflicto cognitivo puede ser una manera de hacerle ver que los conceptos o métodos que maneja no son los adecuados para llegar a una conclusión satisfactoria en la resolución de un problema. Para que el estudiante se dé cuenta de la existencia de una inconsistencia, es decir, para poder hablar de un conflicto cognitivo real donde el estudiante siente la necesidad de emplear estrategias diversas para salir del mismo, se debe contar con una base mínima de lógica y de estructura matemática.

Por otro lado, con respecto al papel que juega el maestro como creador de situaciones matemáticas para que los estudiantes experimenten un conflicto cognitivo en clase, estamos de acuerdo con lo que dice Steffe (1990): “Experimentar el conflicto es un asunto del actor”. Sin embargo, el resto de su frase nos parece poco optimista: “y es un poco ingenuo creer que un maestro tiene tal experiencia bajo su control”. Nosotros creemos que mediante una actividad bien diseñada el maestro puede tener tal control hasta cierto nivel. Es indudable que nadie puede vivir un conflicto en lugar de otra persona, pero los maestros sí pueden preparar un ambiente para favorecer el surgimiento de conflictos cognitivos con fines didácticos.

Una manera de provocar el conflicto utilizando alguna actividad es que el estudiante se enfrente con distintas soluciones de un mismo problema y empiece a cuestionarlas. Esta situación ocurre frecuentemente dentro de un ambiente de grupos de aprendizaje cooperativo:

> Trabajar en pequeños grupos proporciona a los estudiantes oportunidades para interaccionar con sus compañeros en la resolución de problemas. Intentando salir del conflicto que surge cuando miembros del grupo encuentran diferentes “respuestas” al mismo problema, los estudiantes se esfuerzan activamente en procesos que conducen directamente al desarrollo cognitivo (Reynolds et al., 1995).

Es decir, la interacción dentro de un grupo de aprendizaje cooperativo consiste en que los estudiantes se involucran en discusiones y reflexiones entre las que se encuentran propiamente las de sus concepciones erróneas; así, la necesidad de modificar conceptos y métodos genera un nuevo conocimiento. Según Swan (1983, citado por Underhill, 1991), los estudiantes transitan por una etapa *"destructiva"* donde las viejas ideas se muestran insuficientes e inactivas después de que se introducen nuevos métodos y conceptos.

VERSIÓN PRELIMINAR

Con respecto al conflicto cognitivo en un ambiente de grupos de aprendizaje cooperativo, Underhill (1991) hace los siguientes planteamientos:

1. El conflicto cognitivo y la curiosidad son los dos mecanismos principales que motivan a los estudiantes a aprender.
2. La interacción con los compañeros es un factor principal para producir el conflicto cognitivo
3. El conflicto cognitivo induce actividad reflexiva (metacognitiva)
4. La reflexión es el factor principal que estimula reestructuración cognitiva
5. Las afirmaciones (1), (2), (3) y (4) forman un ciclo
6. El ciclo siempre ocurre dentro y se retroalimenta con la experiencia del alumno
7. Este ciclo habilita a los alumnos; es decir, los pone en control de su propio aprendizaje (Underhill, 1991).

De tal modo que en la interacción de los miembros de un equipo con los maestros, el conflicto cognitivo que se produce en los estudiantes puede inducir a una actividad metacognitiva, la cual estriba en un proceso que altera estructuras cognitivas existentes o creencias acerca de las relaciones matemáticas, o bien elimina concepciones erróneas. A esta actividad metacognitiva se pueden comprometer los estudiantes cuando llegan a un conflicto cognitivo y tratan de solucionarlo. En este sentido se dice que pueden llegar a *habilitarse*, es decir, pueden encargarse de su propio aprendizaje.

Sin embargo, debemos subrayar que la provocación del conflicto cognitivo en el estudiante no necesariamente se garantiza con la aplicación de una actividad, ni la reestructuración de su conocimiento ocurre forzosamente como resultado de la emergencia de un conflicto cognitivo. Laborde dice:

> Como lo subraya Lefebvre-Pinard (1989), un simple *feed-back* no es suficiente para "inducir en el individuo un verdadero estado conflictivo", para que dicho estado "pueda ser fuente de reestructuración cognitiva", y finalmente suceda que "esta reestructuración sea transferible a otras situaciones" (Laborde, 1991, refiriendo a Lefebvre-Pinard, 1989).

Vidakovic (1997) estudió las características que diferencian entre el proceso del aprendizaje del concepto de la función inversa en una situación individual y grupal, e identificó cuatro características que, según ella, hacen que la resolución del problema en un grupo sea más efectiva: favorecer el desequilibrio, la diversidad de acercamientos, la construcción de lenguaje matemático y asumir diferentes papeles. Vidakovic comenta que "en una situación individual de resolución de problemas el desequilibrio usualmente se induce sólo por el problema mismo, mientras que en una situación grupal de resolución de problemas hay una fuente adicional –los otros miembros del grupo. Además, es mucho más fácil que un individuo ignore una contradicción, comparado con un grupo".

Cabe mencionar que la existencia de una situación de conflicto para el maestro no es suficiente para que el estudiante llegue a experimentarlo. Por otro lado, aunque la discusión en equipo puede proporcionar elementos para que el estudiante se dé cuenta tanto de sus concepciones inconsistentes (debido a la existencia de diferentes puntos de vista) como de la necesidad de convencer a los otros de la solución a un problema, o simplemente de las diferentes interrogantes que formulan los participantes en la discusión, sostenemos que la actividad matemática debe tener ciertas propiedades para lograr tal objetivo. Consideramos que una secuencia bien diseñada es un paso importante hacia la provocación de un conflicto cognitivo, el cual tendría que seguir estrategias didácticas adecuadas con miras a la adquisición del nuevo conocimiento.

Un aspecto importante de tales actividades se halla en la retroalimentación. Los comentarios del maestro sobre la solución de un problema tienen un carácter externo y se basan en su autoridad; en el mejor de los casos, el estudiante puede convencerse de los argumentos y darle un significado a las sugerencias, pero no siempre se logra. En cambio, si se da cuenta de que su

VERSIÓN PRELIMINAR

respuesta es incorrecta, es muy probable que tome la iniciativa de corregirla a través de diversas estrategias. Si el diseño resulta adecuado hasta puede reconocer la fuente de su error, un paso primordial para confrontar el conocimiento anterior con el nuevo.

En este artículo daremos un ejemplo de las actividades que se pueden utilizar para crear un conflicto cognitivo en un ambiente de aprendizaje cooperativo. Explicaremos el problema matemático que forma la base de esta actividad y luego comentaremos sobre su aplicación en un grupo de profesores, analizando los resultados obtenidos. Creemos que los maestros necesitan participar activamente en este tipo de situaciones antes de utilizarlas en sus clases.

2. La investigación

2.1 El problema

La actividad se basa en un problema de criptografía donde cada letra del alfabeto está representada por un número entre 0 y 26 de acuerdo con la siguiente tabla.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14

Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25	26	0

Para codificar una palabra se usa una matriz 2×2 como transformación cuyas entradas están en el conjunto $Z_{27,}$ que se puede pensar como un reloj de 27 números. En este sistema todos los números enteros tienen una representación por un número entre 0 y 26, el cual se define por el residuo de la división entre este número y el 27. Por ejemplo, 56 equivale a 2.

A continuación, explicamos con detalle el proceso de codificación (Anton, 1994).

Paso 1. *Elegir el texto que se va a codificar y agrupar las letras por parejas de izquierda a derecha. En caso de que sea impar el número de letras, convencionalmente colocamos* Z *al final del mensaje. Después hay que sustituir cada letra por su representante en el alfabeto.*

Paso 2. Elegir una matriz invertible $A(2 \times 2)$ cuyas entradas son elementos de $Z_{27.}$

Paso 3. Poner como vectores (de dos coordenadas) las letras, tal como aparecen en el primer paso, y hacer la multiplicación de cada uno por la matriz *A*, poniendo atención a las operaciones de multiplicación y suma en Z_{27}. Aquí como resultado se obtendrán vectores, a los que les extraeremos las coordenadas para escribirlas en el orden en que se iban multiplicando los vectores. Estos estarán distribuidos como *abcd*, etc., donde *a*, *b*, *c*, *d*, etc., están en el rango 0–26.

Paso 4. Convertir los números así obtenidos en sus letras equivalentes.

En lo que sigue, no utilizamos una simbología especial para indicar las operaciones de la aritmética modular; sin embargo, enfatizamos que todas las operaciones se realizan en $Z_{27,}$

VERSIÓN PRELIMINAR

según sus reglas correspondientes.

Tomemos un ejemplo para ilustrar el proceso de decodificación:

Paso 1. Consideremos el texto CARO. Agrupamos dos por dos las letras y encontramos sus respectivos representantes numéricos de la siguiente manera:

$$\text{C, A; R, O} \rightarrow 3, 1; 19, 16.$$

Paso 2. Elegimos la matriz $A = \begin{pmatrix} 5 & 1 \\ 2 & 3 \end{pmatrix}$ como matriz de decodificación.

Paso 3. A partir del texto, tenemos los siguientes vectores: $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 19 \\ 16 \end{pmatrix}$

Hacemos la multiplicación de la matriz *A* por los vectores en el orden que están:

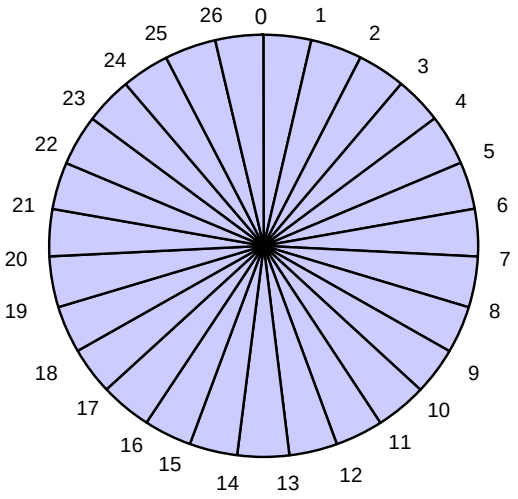
$$\begin{pmatrix} 5 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 16 \\ 9 \end{pmatrix},$$

$$\begin{pmatrix} 5 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 19 \\ 16 \end{pmatrix} = \begin{pmatrix} 111 \\ 86 \end{pmatrix}.$$

Tenemos que los representantes numéricos para el texto codificado son:

$$16, 9; 111, 86.$$

Debemos dar una interpretación a lo que significan números “mayores” de 27. Como habíamos mencionado, una manera de hacerlo es hallar el residuo de la división del número obtenido entre 27. Otra alternativa consiste en relacionarlo con un reloj de 27 números, como el que se muestra en la figura siguiente.



Si queremos encontrar el significado de un numero mayor de 27, debemos recorrer los numeros del reloj en el sentido de las manecillas, avanzando tantos lugares después del cero como lo indique dicha cantidad (podemos dar las vueltas necesarias) y se concluirá en uno de los representantes asignados al alfabeto. Encontramos que, dentro de este sistema, 111 equivale a 3

VERSIÓN PRELIMINAR

y 86 a 5.

Paso 4. Ahora, se hace corresponder una letra con cada uno de los números. Se tienen las asignaciones 16, 9; 3, 5 $\rightarrow$ O, I; C, E, por lo cual se concluye que, al codificar el mensaje CARO mediante la matriz *A* en el reloj de 27 elementos, obtenemos OICE.

La pregunta es ¿cómo decodificar? O, equivalentemente, ¿cómo regresar de OICE a CARO? Esto haremos a continuación.

Dado que en la codificación multiplicamos la matriz *A* por vectores ***x***'s y obtuvimos ***y***'s, en los símbolos $Ax = y$ para decodificar podemos utilizar un *proceso inverso*, que se resume en la fórmula $y = A^{-1}x$. Por consiguiente, nuestro objetivo es encontrar $A^{-1} = [ad - bc]^{-1} adjA$ con *a*=5, *b*=1, *c*=2 y *d*=3. Nótese que debemos hallar el inverso de la matriz en Z_{27}, lo cual posiblemente haga más complicada la decodificación.

Tenemos que $ad - bc = 5 \times 3 - 2 \times 1 = 13$, y así $13^{-1} = 25$ porque $13 \times 25 = 325$, el cual, dividido por 27, nos da como residuo 1, que es el inverso multiplicativo en el reloj.

También en este sistema: $\boldsymbol{adjA} = \begin{pmatrix} \boldsymbol{d} & 27 - \boldsymbol{b} \\ 27 - \boldsymbol{c} & \boldsymbol{a} \end{pmatrix} = \begin{pmatrix} 3 & 26 \\ 25 & 5 \end{pmatrix}$. Luego

$$A^{-1} = 25\begin{pmatrix} 3 & 26 \\ 25 & 5 \end{pmatrix} = \begin{pmatrix} 75 & 650 \\ 625 & 125 \end{pmatrix} = \begin{pmatrix} 21 & 2 \\ 4 & 17 \end{pmatrix}$$

ya que 75, 650, 625 y 125 dejan como residuos 21, 2, 4 y 24 al realizar la división por 27, respectivamente.

Así, lo único que falta para decodificar es multiplicar A^{-1} por los vectores que se asocian con la palabra codificada en la forma siguiente:

O, I; C, E $\rightarrow$ 16, 9; 3, 5

$$\begin{pmatrix} 21 & 2 \\ 4 & 17 \end{pmatrix}\begin{pmatrix} 16 \\ 9 \end{pmatrix} = \begin{pmatrix} 354 \\ 217 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix},$$

porque 354 y 217 dejan como residuos 3 y 1 al hacer sus divisiones por 27, respectivamente.

Análogamente, se obtiene que $\begin{pmatrix} 21 & 2 \\ 4 & 17 \end{pmatrix}\begin{pmatrix} 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 19 \\ 16 \end{pmatrix}$.

Finalmente, tenemos la asociación 3, 1; 19, 16, que corresponde al texto original CARO.

Otra manera de decodificar consiste en usar el sistema de ecuaciones resultante $Ax = y$, donde los vectores *x*'s son las incógnitas, mientras que los *y*'s son conocidos porque provienen de la palabra codificada OICE. Una opción para resolver el problema de criptografía mediante sistemas de ecuaciones lineales es O, I; C, E $\rightarrow$ 16, 9; 3, 5.

Dado que queremos decodificar, debemos encontrar *r*, *s*, *t* y *u*, tales que

VERSIÓN PRELIMINAR

$$\begin{pmatrix}5 & 1\\ 2 & 3\end{pmatrix}\begin{pmatrix}r\\ s\end{pmatrix}=\begin{pmatrix}16\\ 9\end{pmatrix},\ \begin{pmatrix}5 & 1\\ 2 & 3\end{pmatrix}\begin{pmatrix}t\\ u\end{pmatrix}=\begin{pmatrix}3\\ 5\end{pmatrix},$$

es decir, resolver los sistemas

$$\begin{array}{lll}(1)\ \ 5r+\ s=16 & y & (3)\ \ 5t+\ u=3\\ (2)\ \ 2r+3s=9 & & (4)\ \ 2t+3u=5\end{array}$$

en Z_{27}.

Al multiplicar (1) por 5 y sumando la ecuación resultante con (2), obtenemos la ecuación $8s=8$ (dado que 27 es igual a cero), que equivale a $s=1$. Sustituyendo en (1), tenemos $5r+1=16$, es decir, $5r=15$, de donde $r=3$. De esta manera, obtenemos el vector $x_1=\begin{pmatrix}3\\ 1\end{pmatrix}$, y en forma similar $x_2=\begin{pmatrix}19\\ 16\end{pmatrix}$. En este proceso, además de las dos operaciones de 27 (suma y multiplicación) de Z_{27}, están involucrados los conceptos de elemento neutro y elemento inverso bajo una operación.

Por consiguiente, para la decodificación tenemos la asociación O, I, C, E $\rightarrow$ 3, 1; 19, 16 $\rightarrow$ C, A; R, O. Así, la palabra que se codificó fue CARO.

Cabe mencionar que un cambio en el tamaño de la matriz de codificación repercutiría en el tamaño de los vectores que se forman por agrupación de letras.

2.2 Los participantes y la aplicación de la actividad

La aplicación se llevó a cabo durante un taller para profesores de álgebra lineal o álgebra abstracta introductoria en el nivel superior o bachillerato, o a cualquier persona que tuviera interés en aprender sobre un acercamiento interactivo de la enseñanza. Asistieron cerca de 70 maestros de varios países; 40 por ciento tenía formación de matemático y los restantes en profesiones afines (ingenierías). Todos daban clases de álgebra y un 75 por ciento se desempeñaba en el nivel superior.

Para la aplicación de la actividad se formaron varios grupos de 4 a 5 personas y hubo tres etapas: resolución de la actividad de criptografía, discusión en grupo y aplicación de un instrumento (Anexo 1) con el fin de mostrar a los participantes más formalmente la estructura de la aritmética modular. La información que presentaremos a continuación proviene de grabaciones tanto de un equipo que estaba llevando a cabo la primera etapa como de la discusión grupal. Esta fase duró aproximadamente dos horas.

Primero describimos los pasos que se siguieron para efectuar la actividad de criptografía.

Se dio a conocer el ejemplo mostrado en la sección anterior, donde se codifica la palabra CARO utilizando la misma matriz de codificación, y enseguida se pidió que cada grupo codificara una palabra de su elección (sin que los otros supieran cuál era). Una vez realizada esta etapa, los equipos intercambiaron la palabra codificada con la de otro equipo con el fin de decodificarla.

Cabe mencionar que no se mencionó la forma en que se decodificaba una palabra, ya que queríamos observar cómo los maestros llevaban a cabo un proceso inverso como un proceso nuevo, enfocándonos en los tipos de conflictos que les surgían y en sus estrategias para resolverlos. Por la misma razón, tampoco hubo una discusión preliminar sobre las propiedades que debe cumplir la matriz *A* para que funcione como codificadora.

VERSIÓN PRELIMINAR

Si bien no esperábamos que los maestros tuvieran dificultades para codificar una palabra, en la decodificación esperábamos que los maestros hicieran un intento por usar los métodos presentados en la sección anterior, pero obteniendo resultados inconsistentes, de modo que manifestaran un conflicto cognitivo. Veamos qué podría suceder si intentaban hallar la matriz inversa: como el determinante de la matriz es 13, operando con números reales, en la primera entrada de la inversa podrían obtener 3/13, o bien 0.23; tendrían como entradas números que no eran enteros.

Fijándose en el conjunto de los números reales y no en los elementos de Z_{27} con sus respectivas operaciones y estructura propia, llegarían a números que en la decodificación no se corresponderían con las letras del alfabeto. En caso de trabajar con sistemas de ecuaciones lineales, utilizando las mismas operaciones del conjunto de los números reales, podrían llegar a ecuaciones del tipo $5t+u=3,\ 2t+3u=5$, que a su vez se podrían combinar para obtener $t=4/3,\ u=19/13$. Cuando los maestros se dieran cuenta de que no podrían asociar letras del alfabeto a estos números surgiría un conflicto cognitivo, ya que el no resolverían el problema satisfactoriamente.

En ambas estrategias de solución, la inconsistencia se refiere a la obtención de números decimales por el uso de una operación que no corresponde a la definida en el conjunto Z_{27}. Para llegar a la respuesta correcta, los participantes tendrían que fijarse en la estructura del conjunto Z_{27} junto con su operación binaria presentada, en lugar de suponer que el uso de los números reales y las operaciones familiares les daría el resultado.

2.3. Resultados

Aquí describiremos las etapas por las que transitaron los maestros al involucrarse en esta actividad, examinaremos sus dificultades –relacionadas con el cambio de estructura– y las estrategias con las que intentaron salir del conflicto. Después de que todos los equipos habían intentado resolver el problema y habían encontrado resultados inconsistentes, se hizo una discusión grupal; sus resultados los presentaremos al final de esta sección.

Los miembros del equipo cuya discusión se presentará a continuación se etiquetarán con los siguientes renombres: P1, P2, P3 y P4.

2.3.1. Análisis de la resolución de la actividad de criptografía

Los maestros de cada equipo efectuaron correctamente la codificación de una palabra de tres o cuatro letras que previamente habían propuesto, sin que los demás se enteraran. Esto es, hicieron bien la operación multiplicación del reloj e intercambiaron su texto con otro equipo.

Durante el proceso de decodificación, los maestros llevaron a cabo varios intentos en los que se observaba un ciclo repetitivo:

- Etapa 1: Empiezan a decodificar
- Etapa 2: Llegan al conflicto (expresiones del enfrentamiento: insatisfacción, incomodidad, etc.)
- Etapa 3: Utilizan diferentes estrategias para salir del conflicto. Aquí se observan diversas estrategias para llegar a una solución satisfactoria. Cuando esta etapa no había una respuesta correcta, volvían a la primera etapa para empezar de nuevo con otra técnica

El siguiente fragmento constata que los maestros, en el primer intento para decodificar su palabra, estaban volviendo a codificar. No se daban cuenta que debían aplicar un proceso

VERSIÓN PRELIMINAR

inverso para regresar a la palabra original.

–P2: Como que no me sale lógico.
.....
–P3: El problema es que, aunque no salga lógico, eso es lo que tenemos. ¿Qué pasa?
–P2: Esta palabra como que no tiene sentido.
.....
–P4: Terminamos.
–P3: UTZM.
–P2: No creo que ellos hicieran eso, a ver. A ver si esos malvados hicieron eso...
–P3: No.
–*Instructor 2*: En idioma español (risa).
–P3: En español.
–*Instructor 2*: Les dijimos a ellos que en español, ¿eh?
–P1: No, yo creo que lo que pasa con esto ahora estamos volviendo a codificar; se supone que esta es una palabra.
–P3: Yo pienso que hicimos algo parecido a lo que tenemos ahorita.

Como se puede observar, los maestros inicialmente buscan alternativas para corregir el error. En este caso, piensan si el equipo que les envió la palabra en clave consideró una palabra común; sin embargo, P1 se da cuenta que estaban volviendo a codificar y P3 agrega que habían seguido un proceso semejante al de codificar.

El siguiente fragmento muestra que los miembros del equipo están pensando en distintas estrategias para corregir la situación; en este momento no hay mucha interacción entre ellos.

–P4: Nosotros partimos de la matriz, por ejemplo.
.....
–P3: ¡Ah! Vamos a revertir.
–P4: Nos dieron eso.
–P2: Yo voy a revertir el de nosotros, a ver si ellos cometieron error.
–P4: Si nos dieron esto.
.....
–P4: Vimos la matriz original.
–*Instructor 2*: ¡Ajá!
–P4: Y fuimos aquí y...
.....
–P2: Si el mío no me da esto es un gancho.

Nótese que mientras P4 se concentraba en la matriz de codificación y posiblemente buscaba una solución, P2 todavía no dejaba de creer en la solución que habían obtenido, aunque en la discusión anterior el equipo había comentado que tal proceso llevaba de nuevo a la codificación. Es importante señalar que P2 se sentía incómoda de que no se les había enseñado a codificar.

En los fragmentos que siguen veremos un progreso de los maestros, ya que piensan en un proceso inverso y vuelven a resolver el problema de una manera distinta. Los puntos suspensivos (...) indican que el maestro hacía una pausa mientras razonaba.

–P3: En vez de multiplicar por esta, vamos a hacer 1 sobre...
–P2: Ok.
–P3: Porque no se divide, sino que se haría con la inversa.
–P2: Hay un problema.
–P3: Se multiplica por 1 sobre...
–P2: Hay un problema. Espérate, espera si tengo su número.
–P4: Es la inversa.
–P2: Atención. Si tengo algo inverso, o tengo el opuesto aditivo o el inverso multiplicativo.
–P4: Uh-uh.
–P2: La duda que me ha entrado es si decodificar es el opuesto aditivo de o es el inverso multiplicativo.

VERSIÓN PRELIMINAR

–P3: No, el inverso multiplicativo.
–P4: Eh.
–P3: Porque en una multiplicación...
.....
–P3: Es la inversa.
–P2: Decodificar es la inversa.
–P3: Multipli….
–P2: Entonces, ahora mi amiga me dice el inverso multiplicativo y yo digo, ¿y si fuese el opuesto aditivo?
–P3: No porque es una multiplicación. ¡Ah!, pero si fuera una suma...
–P4: Es con el inverso.
–P3: Si fuera una suma cabría la posibilidad de que sea el aditivo, pero como es una multiplicación sólo existe su recíproco y entonces...
–P2: Entonces hay que dividir.
–P3: La matriz no se divide, sino que se multiplica.
–P2: Se multiplica.
–P4: Sí, por su inversa.
–P3: Por su recíproco.
–*Instructor 3*: Buena idea.

En esta discusión se observa que no están claros los objetos a los cuales se aplicaría la operación inversa y todavía no hay un acuerdo en el equipo. Aunque P4 puede estar pensando en la matriz inversa, no se verbaliza el proceso a seguir para resolver el problema.
En los fragmentos siguientes los maestros abordan el inverso de una manera incorrecta, ya que multiplican la matriz por un "vector inverso" (el inverso de un vector no está definido). Hallan "los inversos" con la división de los números reales entre las coordenadas del vector original; siguen su búsqueda y exploran los "procesos inversos", sin tener control sobre la situación, en este caso, una matriz inversa definida como un vector cuyas entradas se obtienen como recíproco de las entradas del vector original.

–P4: Vámonos con la inversa.
–P2: A codificar.
–P4: Digo, vamos con la inversa. Nos dan una matriz.
–P2: Vamos a decodificar.
.....
–P4: Entonces, vamos...
–P2: A multiplicarlo por el vector inverso
–P4: Ajá.
.....
–P4: Los vectores serían (23, 11).
–P2: Ok.
–P4: Y (26, 5).
–P2: Ok.
–P4: Y eso es 5, 2 y 1, 3, 5, 2 y 1, 3, que vamos a construir esto por su inversa.
–P2: Uh-uh. 1 sobre 23.
–P4: Por ejemplo, 5, 2.
–P3: Me queda...
–P4: Y tres por 1/23 y por 1/11.

Notamos que al poner a los maestros en situaciones nuevas, nos es posible advertir cómo construyen sus ideas y estrategias.

Obsérvese que en el fragmento anterior los maestros no piensan *transferir* el significado de números como 1/11 al contexto de Z_{27}. Por eso obtienen decimales, como se constata en los fragmentos siguientes.

–P2: Me quedan decimales... si no puede ser, yo creo que no. Estamos en problemas.
–P4: Mira: 5 sobre 16 te dio...

VERSIÓN PRELIMINAR

–P2: 0.22.
–P4: 0.22, y 3/11...
–P2: 0.09.
.....
–P2: No me gusta esto.
–P3 No me gusta esto.
–P2: Me dan unos decimales ahí.

Aquí los maestros tienen un conflicto cognitivo debido a que obtienen decimales; tal situación los induce a contradecir los conocimientos previos con que habían enfrentado la actividad. Es importante señalar las manifestaciones del desequilibrio, ya que revelan un estado de insatisfacción: "Me queda decimales... si no puede ser". Como no pueden asociar una letra a los números obtenidos (decimales), los maestros se dan cuenta que algo está mal; en efecto, el problema no está solamente en el resultado de los decimales, sino en que no identifican el proceso inverso correspondiente. La obtención de decimales en este caso funciona como una retroalimentación para ver que la solución planteada no puede ser correcta.

A continuación mostramos cómo los maestros recurren a diferentes estrategias para salir del conflicto.

–P2: Aquí, en la escala numérica, están los negativos. Observa, porque si yo empiezo el abecedario 1, 2, 3, 4, 5, 6 y llego hasta el 0 es como si a partir de la Z volviera a repetir el abecedario, pero negativo; entonces esos decimales me quedan entre dos enteros.
–P4: Sí; necesitaríamos entre A y C en el primero, después entre A y B.
–P2: No, entre 0 y A;. 0.31 menor que 1.
–P4: Sí, ah sí.
–P2: Me doy: necesito una luz acá.
–P3: Luz debe ser...
–P2: O tengo que poner inversas las letras...
–P3: Tenemos que proponer la inversa.
–P4: Sí.
–P3: ¿Inversa a quién dices?
–P2: Las letras.
–P4: Había que trabajar, modificar la estructura de las letras.
–P2: ¡Ah! Las letras.
–P2: Trabajar con el inverso también... Necesitamos...
–P2: Como si fuese un eje donde yo desplazara esta para acá, para acá, para acá y después y para allá.
–P3: Sí pareciera, pero...
–P2: O pongo inversas las letras porque ese inverso multiplicativo...
–P4: Sí.
–P2: No me gustó.
–P4: No.
–P2: Ya yo no sigo con esa estrategia, por ese camino no voy. Por esa vía no podemos llegar porque nos da decimales.
.....
–P4 (*Mira la solución que obtuvo otro equipo*): A ellos también les da sin sentido...
–P3: ¡Ay! Por eso nosotros necesitamos un poco de luz.
–P2: Ya tenemos dos caminos y no vemos...
–P3: Por la vía que intentamos, no.
–P2: Un tercero podría ser...
–P3: Si trabajamos así nos darían decimales.
–P4: Trabajamos con la inversa y nos da decimales.
–*Instructor 2*: Bueno, si les da decimales por ahí deben de ir las preguntas.
.....
–P3: Es que nos da decimales. Allí no tendríamos letras para establecer la correspondencia.
.....
–*Instructor 2*: En realidad, deben de preguntarse sobre el significado de...
–P4: Sobre el resultado.
–P2 De un once.

VERSIÓN PRELIMINAR

–*Instructor 2*: El significado de 1/11.
–P2: Ya.
–P3: ¡Ah!, tú dices del decimal que lo genera.

Este y otro intento del *Instructor 2* no genera una reflexión sobre las operaciones de Z_{27}. Pareciera que esta idea no les ocurriría naturalmente a los maestros ni después de recibir una pista.

En los fragmentos que siguen notamos varios intentos de los maestros para entender lo que está pasando y cómo corregir la situación. Identificamos que el hecho de concentrarse en soluciones locales, en lugar de reflexionar globalmente sobre la estructura y la actividad, les impide localizar el problema.

–P1: Podemos utilizar ecuaciones, ¿verdad?
.....
–*Instructor 2*: Podría ser, pero a lo mejor se encuentren otra vez con esto...
–P3: Con esto de, o sea, que van a aparecer...
–*Instructor 2*: Es posible, es posible.
–P1: ¡Ajá! Bueno...
–*Instructor 2*: Porque... pónganse a pensar qué significan esos números.
–P4: Así vamos a hacer la conjetura.
–P3: Eso quiere decir que, irremediablemente, ese es el camino...

Vemos que P1 quiere usar un sistema de ecuaciones como un nuevo método para resolver el problema. Sin embargo, el *Instructor 2* le menciona la posibilidad de que se encuentren con las mismas dificultades y quiere llamar su atención sobre el significado de los decimales obtenidos. De aquí surge la posibilidad de que los maestros no aborden el problema mediante tal aproximación; no obstante, al revisar los apuntes de los cuadernos, descubrimos que mayoría del tiempo P1 intentó decodificar con un sistema de ecuaciones. Sus dificultades, al igual que las de sus compañeros de equipo, radicaron en la obtención de decimales.

–*Instructor 2*: ¿Verdad? Como, como que se están trabajando en un reloj...
–P3: Ahí no, no, dice que ya aquí estamos instruccionando en otro medio...
–P4: Que se sale de lo establecido.
–P2: Sí.
–P3: Que se sale de lo establecido, y no tenemos con qué se pueden hacer comparaciones.
.....
–P2: La pregunta es que, al tener decimales, decimos: no tenemos código para los decimales. Vamos a tener que crear un código.
.....
–P4: Un nuevo modelo.
–P3: Vamos a seguir, a ver qué pasa...
–P2: Vamos a inventar un nuevo código.
–P3: Un nuevo código para los decimales.

Las expresiones de los maestros indican que están conscientes de que están frente a una estructura desconocida, y esto los desestabiliza. Hasta ese momento, sus estrategias para salir del conflicto eran:

- Hay que cambiar la estructura de las letras
- Hay que idear un nuevo modelo, posiblemente un nuevo código para los decimales
- Mirar lo que habían obtenido otros equipos

Parece que cuando los maestros piensan en cambiar la estructura de las letras creen que ya han obtenido los números a los que habrán de asociarle las letras; sólo les falta idear un nuevo modelo. No obstante, siguen sin hallar el método correcto para la decodificación. Empero, en su

VERSIÓN PRELIMINAR

interacción observamos que hay un intento por cambiar la *manera de pensar* (P2*:* Me doy, necesito una luz acá; P3: Luz debe ser; P2: O pongo inversas las letras), lo cual les servirá para superar el conflicto cognitivo.

En los fragmentos que siguen mencionamos un aspecto de la interacción en el equipo. P1 aborda el problema con una idea, mientras que P2 no la quiere usar.

–P2: ¿Qué piensas?
–P1: Sí, es que yo quiero sacarla por ecuaciones...
–P2: ¡Ay, no! Yo no me voy a meter.
.....
–P1: Estoy analizando. Todo parte de aquí: si tenemos esto y sabemos cómo llegar a esto, porque a lo que tenemos que llegar es a 12, 14 y 16. Yo pienso que el problema está aquí.

Como veremos a continuación, los maestros, cuando buscan otras salidas al conflicto, reflexionan sobre su acercamiento al problema y lo relacionan con sus profesiones:
–P2: De que faltan códigos...
.....
–P2: Porque los resultados están en otro conjunto...
.....
–P2: Yo siento que nosotros también estamos limitados en el sentido de que, al tener otros referentes por ser profesores, eso nos inhibe, porque ya P1 quiere buscar ecuaciones. Nosotros, P3, P4 y yo, estábamos hablando de...
–P1: Como de...
–P2: De conjunto numérico referente.
–P3: Sí, porque nos da decimales.
–P2: Entonces, eso nos puede ayudar, pero también nos puede limitar, a diferencia del que está aprendiendo por primera vez o el que se está acercando a ese conocimiento porque nosotros estamos deseables, pero...
–P3: Sí, pero nosotros aplicamos lo que sabemos.

Parece que P2 tiene claro el conjunto subyacente; sin embargo, no lo coordina con la operación (la suma en el reloj). Reflexiona sobre la novedad de la situación y la limitante que puede jugar el conocimiento anterior ante uno nuevo.

En los siguientes fragmentos es importante destacar el papel del *Instructor*.

–*Instructor 3*: A ver, vamos a pensar un poquito. Es que dice muchas cosas, ¿no? Entonces, como siempre, la matemática va pasito a pasito. Usted hablaba de un inverso multiplicativo.
–P3: Ajá. Esa fue la primera idea.
–*Instructor 3*: Ahora, ¿qué quiere decir eso de un inverso multiplicativo?
–P3: O sea, que aquí nosotros, en vez de multiplicar los dos vectores, tendríamos que hacerlo por el inverso del segundo.
–*Instructor 3*: Sí.
–P3: Del primero.
–*Instructor 3*: ¿Y por qué multiplicamos por el inverso? ¿Qué buscamos?
–P2: Buscamos...
–*Instructor 3*: Al multiplicar por ese inverso.
–P2: Buscamos la unidad.
.....
–*Instructor 3*: Y aquí nosotros estamos restringidos a este reloj, ¿verdad?
–P2: Sí.
–*Instructor 3*: Y podríamos multiplicar por ese inverso buscando la unidad. ¿No podríamos buscarle por ahí? Esa idea se me hace interesante...
–P3: La unidad... pero no nos daba la unidad P4.
–P2: No, él dice que busquemos... Puede ser...
–*Instructor 3*: Sí.
–P2: Vamos a tratar de buscar.

VERSIÓN PRELIMINAR

–*Instructor 3*: A ver, ¿no?
–P2: A ver qué pasa.
–*Instructor 3*: O sea, el chiste en esto es importante porque quiere decir que descubrimos que tenemos una...
–P3: Buscar...
–*Instructor 3*: Limitación, ¿no?
–P3: La matriz identidad... o un... identidad.
–*Instructor 3*: Además, esto nos puede guiar a otras búsquedas, ¿no?
–P3: Sí.
–*Instructor 3*: Entonces, yo trato de seguir sus propias ideas para...
–P3: A ver qué pasa, qué sale de ahí.
–*Instructor 3*: Sí, sí; esperamos que sí salga.
–P3: Ok.
–P2: La matriz de un vector identidad porque el inverso multiplicativo de 1 sobre 23 es que por 23 da 1, entonces a ver, a ver...

.....

–*Instructor 1*: Es un sistema muy particular.
–P4: Muy restringido.
–*Instructor 1*: Sí, y tiene una estructura diferente. Entonces, por ejemplo, ¿qué quiere decir, si, por ejemplo, tú tienes, no sé... 1 x 3 o 1 x 23? ¿Qué significa eso en este sistema?
–P3: Si tienes 1 x 23 o 1 x 13.
–P4: Si un qué...
–P3: Ajá.
–P4: Si tienes un entero por una fracción, en este caso...
–P3: No, no. Si tienes 1 por cualquier número significa que tiene una que le va a dar el mismo número.
–*Instructor 1*: Ajá.
–P3: El producto va a ser el mismo número, o sea, un neutro.
–*Instructor 1*: Sí.
–P2: El neutro.
–*Instructor 1*: Hay que, hay que...
–P4: Implicaría...
–*Instructor 1*: Pensar en este sistema. Hay que pensar en esta estructura.

.....

–*Instructor 1*: Entonces, cuando pensamos, por ejemplo, resolver ecuaciones, tenemos que pensar en este sistema. ¿Cómo se puede resolver una ecuación en este sistema? ¿Cómo se puede sacar la inversa de una matriz?
–P2: En este sistema...

Dado que los maestros no han salido del conflicto cognitivo y posiblemente han agotado todas sus estrategias para solucionarlo, el *Instructor 3* participa. Como el conflicto indujo a que dos de los maestros (P1 y P3, no presentamos esos fragmentos) se desviaran de la actividad, el *Instructor 3* motiva a los maestros. Les dice que aborden el problema con algunas ideas que anteriormente habían usado, se las recuerda y les hace preguntas para que sus respuestas los induzcan a continuar trabajando la actividad. También, aunque menciona que sigue propiamente las ideas de ellos, los ayuda (*Instructor 3:* ¿Y por qué multiplicamos por el inverso?) e incluso el *Instructor 1* los auxilia para que piensen en el inverso.

Sin embargo, en estas participaciones de los instructores se mostró que los maestros pensaban en algunas propiedades (*Instructor 3*: Al multiplicar por ese inverso; P2: Buscamos la unidad). Parece que cuando P3 menciona el neutro y P2 a la unidad no lo hacen en forma general, es decir, no aluden a cualquier estructura; más bien se refieren a cómo lo ven en la estructura de los números reales con las cuatro operaciones básicas. En efecto, los fragmentos que ya hemos analizado indican que no las transfieren al reloj y les resulta difícil pensar en el inverso de elementos dentro de una estructura general. Por tal motivo, encontramos otra etapa donde el *Instructor 1* intenta guiar a los maestros para que piensen en la estructura.

Un progreso importante que logra P3 es pensar en la identidad del conjunto de las matrices porque sirve para concebir la inversa de la matriz. Los fragmentos que a continuación

VERSIÓN PRELIMINAR

presentamos revelan que, ahora sí, los maestros usan la matriz inversa, aunque la hallaron a través de las operaciones básicas de los números reales. Sin embargo, no resuelven el conflicto porque nuevamente obtienen decimales.

–P3: 5, 2; 1, 3 y busquémosle la inversa por...
.....
–P2: O sea, vamos a buscar la inversa de la matriz original.
.....
–P2: Ajá. Vamos a llamarle matriz a esto.
.....
–P3: Eh... *A'*, que es sobre el determinante de *A.*
.....
–P3: Sobre el determinante de *A.*
–P2: O A^{-1}, que sería 3, 5, -2... Ahí me salen decimales.
–P3: Hay que buscarle por ahí.
–P2: 5 por 3 15; menos 2, 13. ¿Está bien entre 13? Porque ya no hay fraccionarios acá
.....
–P4: Sí.
–P2: Estamos tratando de buscar la inversa de una manera nueva a la que conocemos...
–P4: Sí.
–P2: Porque con los procedimientos conduce a decimales.
–P3: Porque la otra era una multiplicación. Por todos los procedimientos que conocemos de buscar inversa nos da decimales, esto nos está llevando a encontrar una...
–P4: Una...
–P2: Inversa de manera nueva.
.....
–P2: Como quiera te va a dar fraccionarios.

Los maestros continúan en el conflicto asociado con los decimales. En este momento los decimales salen de encontrar la inversa de la matriz usando la regla de Cramer; cabe señalar que, aunque los maestros intentan distintas alternativas (método de suma y resta para sistemas de ecuaciones lineales, regla de Cramer, inversa de matrices), se quedan en el contexto de las operaciones básicas de los números reales. Ningún equipo, antes de que se resolviera el instrumento y hubiera una discusión grupal sobre su aplicación, logró decodificar previendo el cambio de contexto. Dicho instrumento tenía la finalidad de mostrar formalmente la estructura del conjunto Z_n y la aritmética modular.

Durante la actividad confirmamos que, cuando los maestros tienen un conflicto cognitivo, se involucran en discusiones y reflexiones donde salen a relucir los elementos de sus concepciones erróneas. Esto abre el camino hacia la aceptación de nuevos conocimientos que se requieren para resolver el problema; los prepara para la fase "destructiva" donde las viejas ideas son insuficientes e inactivas. Por tanto, los maestros están en un proceso que altera sus estructuras cognitivas o sus creencias acerca de las relaciones matemáticas; en otras palabras, experimentan una actividad metacognitiva.

2.3.2. Discusión a nivel de grupo

Debido a que hasta ese momento la dificultad principal concernía a los inversos, los instructores hicieron una discusión entre el grupo. Cada equipo describió sus avances en la resolución de la actividad, es decir, expuso todas las aproximaciones con las que abordó el problema. Los instructores pidieron a los maestros que pusieran atención a todas las estrategias que se iban a presentar. Transcribimos algunos fragmentos de esta discusión en los cuales se pone en evidencia que los equipos se toparon con un mismo obstáculo.

–*Instructor 1*: Silencio por favor, vamos a discutir... ¿Ya quieren saber la respuesta?
–Todos: Sí, ya.

VERSIÓN PRELIMINAR

–*Instructor 1*: Están haciendo construcciones, lo cual está muy bien, pero vamos a discutir porque veo que todos los equipos tienen el mismo problema.

.....

–*Instructor 1*: Están en este... ¡Ah!, ¿llegaron a algún lugar?

–P4: Tope.

–*Instructor 1*: Y no pueden analizar. Entonces, vamos a discutir.

.....

–P5: Nosotros resolvimos un sistema de ecuaciones manejando la matriz multiplicada por el vector que forma... Eso nos dio igual al código de las letras que nos están dando. Con eso formamos un sistema de ecuaciones y nos dio un... ahí ya nos atoramos.

.....

–P6: Tiene inversa. Si la matriz no es inversible, la única manera que habría para resolverla sería lo que están planteando ellas, un sistema de...

.....

–*Instructor 1*: Para resolver este sistema pueden trabajar con ecuaciones o con inversas de la matriz inversa, pero sale la misma ecuación.

.....

Aquí, P5 señala que el *atorón* estuvo a la hora de resolver el sistema de ecuaciones en el reloj, indicando que obtenía decimales. Cabe señalar que P5 y P6 pertenecían a diferentes equipos.

Para clarificar, presentamos aquí la estrategia que el equipo de P5 usó para tratar de decodificar:

Multiplicar la matriz *A* por los vectores, que son los que van a encontrar. Esto es, dado que se conocen los vectores de la palabra decodificada, se propone encontrar los vectores (*r*, *s*) y (*t*, *u*), de manera que

$$\begin{pmatrix} 5 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \text{ y } \begin{pmatrix} 5 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} t \\ u \end{pmatrix} = \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}.$$

Por consiguiente, al multiplicar e igualar los vectores correspondientes se obtienen los sistemas de ecuaciones lineales

$$\begin{aligned} 5r + s &= a_1 \qquad y \qquad 5t + u = a_2 \\ 2r + 5s &= b_1 \qquad\quad\; 2t + 3u = b_2 \end{aligned}$$

donde a_1, a_2, b_1 y b_2 son conocidos porque provenían de la palabra codificada. Cuando el equipo de P5 intentó resolver estos sistemas obtenía decimales en los valores de x y y, por lo cual se toparon con un obstáculo.

Otro equipo se valió de un método de prueba y error para resolver el sistema de ecuaciones. El símbolo [---] significa que en la grabación a veces se perdía la voz de los maestros.

–*Instructor 1*: Vamos a ver qué hizo este equipo [---], si tiene sentido. Vamos a observar lo que están haciendo [---].

–P7: Me refiero a esa palabra... Tiene asociados unos números [---]. Nosotros nos fijamos en las parejas [---] y, desde luego, la pregunta es de dónde provienen. Entonces, estas parejas provienen de multiplicar, digamos, las matrices, ouh... esta matriz.

.....

–P7: Números, digamos, este para que diera eso... y, por ejemplo, había dos números que se multiplicaban y arrojaron esta, esta pareja. Pero esta pareja nosotros decimos que tiene la forma [varios le dicen: 27] a partir de 27, digamos, la... [le ayudan a decir: *m*] y esta tiene la forma de que...

.....

–*Instructor 1*: ¿Entienden esto que?…

VERSIÓN PRELIMINAR

.....
–P8: Porque no, los números que se obtienen al codificar no siempre están dentro de los 27, sino que pueden ser 27 más...
.....
–P1: Ajá, exacto.
–P7: Así es, en realidad lo que sabemos es que estos números que aparecen aquí son los residuos de resultados de [otras personas dicen: *claro*] dividir entre... Entonces, debe tener esta forma y luego resolvimos... calculamos la inversa de esta matriz, hicimos la multiplicación y nos resultó un sistema de ecuaciones lineales, pero está en términos de *x* y *y*, de *m* y *k* [varios afirman al mismo tiempo: *de m* y *k, sí*], entonces este es un sistema que tenemos que resolver. Desde luego, ahora me estoy dando cuenta de que hay otros dos números que están asociados con este, con los que vamos a...
–*Instructor 1*: Entonces, no saben cómo resolver este...
.....
–P8: Claro, pero... son en su caso también números enteros. Por tanto, son nueve a empezar a probar para distintos números enteros *m* y *k* para encontrar el *x*, y de aquí podemos *m* y *k* reemplazarlos por diferentes números enteros [otra persona dice: *¿x?*] hasta que *x*, *y* sean números enteros [P4 exclama: *pero*] el problema es que nosotros nunca llegamos a encontrar los enteros y eso nos queda...
–P7: Sí, desde luego que todos son enteros, no este –con los que estamos trabajando son enteros precisamente– se trata de encontrar la solución de enteros.
.....
–P7: Pero es que eso ---se traduce de todas maneras en $5x+y$ congruente con 7 módulo 27 --- y $2x+3y$ congruente con 0 módulo 27.
.....
–Una voz: Claro.
–P9: Es que esto era en lo que estábamos; esto lo podemos escribir $5x+y$ (P4 $5x+$) congruente con 7 módulo 27, y la otra $2x+3y$ (*P4* más 3, $3y$) congruente con 0 módulo 27.
–*Instructor 2*: ¿Qué significa esa notación?
–P9: Esto significa simplemente que la diferencia entre $5x+y$-7 es un múltiplo de 27, por lo que es lo mismo que $5x+y$ es de la forma $27m$ [P4 afirma: *¡Ajá!*] +7, si el resto al hacer la división por 27 es 7 y el resto al hacer la división por 27 [P2 dice: *por* 27 *es cero*; P4 agrega: *es cero*] es 0.
.....
–P9: Sí, pero entonces estamos ahí en ese sistema...
.....
–*Instructor 1*: ¿Entienden ese sistema?
.....
–*Instructor 1*: ¿Quién quiere intentar resolver ese sistema?
.....
El Instructor 1 comienza a resolver el sistema.
–P1: ¿Por determinantes?
–P2: Determinantes [---]
–P2: Él está encontrando a *x* y *y*...
–P4: También va a dar...
–P2: También da decimales.
.....
–P4: No sólo decimales, sino negativos.
–P2: Pero queda decimales, 21 entre 3 te da decimales porque nomás estás encontrando...
.....
–*Instructor 1*: Aquí tenemos la resolución de ustedes para este sistema, pero ignorando en el reloj.
.....
–*Instructor 1*: Eso, te salieron fracciones. ¿Qué pasó? ¿Por qué no podemos hacer esto en el reloj? ¿Qué tenemos que hacer?
–P10: Tratar de adaptar este procedimiento a...
.....
–*Instructor 1*: ¿Vas a adaptar esa manera de resolver? Pero, ¿qué quiere decir adaptar en?

Es claro que los maestros ya están enterados de que para la decodificación se debe usar un proceso inverso; sin embargo, no lo han aplicado correctamente. Es posible que estén en el pasaje de operaciones "normales" a pensar en otra operación binaria en forma genérica. Como se presentó en los fragmentos, en este momento un equipo recurre a un método de prueba y

VERSIÓN PRELIMINAR

error para salir del conflicto. A continuación lo presentamos.

P7 encuentra la inversa de la matriz, la multiplica por un vector que es el que va a encontrar y, dado que resultan cocientes, trata de dar valores numéricos a algunas variables del numerador, de tal manera que estos cocientes se conviertan en enteros. Esto es, multiplica la inversa de la matriz (calculada con las operaciones multiplicación y división básicas de los números reales) por un vector ($r + 27k$, $s + 27m$), donde (r, s) es el que se había obtenido en la codificación. Después iguala al vector (x, y), que es el que encontraría para decodificar, de la siguiente manera:

$$\frac{1}{5x3-2x1}\begin{pmatrix} 3 & -1 \\ -2 & 5 \end{pmatrix}\begin{pmatrix} r+27k \\ s+27m \end{pmatrix}=\begin{pmatrix} x \\ y \end{pmatrix}.$$

Al multiplicar e igualar los vectores correspondientes, obtiene el sistema de ecuaciones

$$3r - s + 81k - 27m = 13x$$
$$-2r + 5s - 54k - 135m = 13y$$

donde m y k son variables. Busca distintos valores para m y k, de tal suerte que x y y resulten enteros y así poder hacer corresponder las letras del alfabeto. Empero, al resolver el sistema a x y y le salían con decimales, lo cual provoca el conflicto.

De la discusión entre el grupo se observó que, aunque algunos maestros identificaron el problema con la aritmética modular, no pudieron resolver el problema, tal vez porque nunca habían resuelto ecuaciones en este sistema. Así, la actividad resultó novedosa incluso para quienes el conjunto y sus operaciones.

Finalmente, mostramos otro intento por salir del conflicto valiéndose de la siguiente estrategia.

–P1: ¿No podríamos utilizar lo que es grados? O sea, meternos con lo que son los grados minutos y hasta a lo mejor hasta los segundos...
–*Instructor 1*: ¿Usar qué?
–P1: Grados, grados.
.....
Se entabla una discusión acerca de esta sugerencia. Después se da el siguiente diálogo:

–*Instructor 1*: Pero vamos a tener un problema ahí...
.....
–P4: Por supuesto, van a seguir siendo decimales.
–P1: Sí.
–*Instructor 1*: Porque estás convirtiendo este reloj a otro.

P1 quiso modificar el reloj; sin embargo, tal sugerencia no se lleva a cabo porque seguirían trabajando con un reloj quizá más complicado. La sesión ya se estaba terminando.

Como se mencionó, después de esta discusión se aplicó un instrumento cuyo propósito fue introducir el conjunto Z_n y la aritmética modular (ver Anexo 1). Los participantes trabajaron sobre ejercicios que involucraron operaciones, elemento neutro, elemento inverso, resolución de ecuaciones y condiciones que determinan que una ecuación tenga solución única o no.

Los miembros del equipo en cuestión resolvieron satisfactoriamente los primeros dos ejercicios. Para el tercero dieron la respuesta $x=m-k$ si $m\geq k$ y $x=m-k+9$ si $m<k$, lo cual reflejó su desempeño al resolver una ecuación general en aritmética modular; también aportaron una solución adecuada para el cuarto.

VERSIÓN PRELIMINAR

En el caso del quinto ejercicio, un integrante del equipo (P4) al principio pensó en decimales y para resolver la ecuación $2x = 1$ sugirió que se multiplicara por ½. Sus compañeros le explicaron que había que multiplicar por un elemento del conjunto y resolvieron las ecuaciones correctamente. Para el sexto, después de dar una vuelta en todo el conjunto y verificar los valores, concluyeron que no había solución; llamó la atención el hecho de que P4 empezó a dar valores, pero no mencionó a los decimales.

Al trabajar sobre el ejercicio 7, afirmaron que la ecuación $ax = 1$ se solucionaba cuando a tenía inverso multiplicativo; sin embargo, no discutieron las condiciones que debían existir para que a tuviera inverso multiplicativo. Este equipo no llegó a debatir los últimos dos ejercicios por falta de tiempo; no obstante, su desempeño en los otros ejercicios mostró su buen nivel de entendimiento de la estructura del conjunto y sus operaciones binarias.

Después de esto, los maestros regresaron a la actividad de criptografía. Al final, un equipo mostró cómo había resuelto el problema a través de un método que tenía elementos de prueba y error; sin embargo, esta vez tomó en cuenta la estructura del conjunto. Los otros equipos quedaron satisfechos con tal resolución.

2.4. Rediseño de la actividad

Como la primera aplicación fue exitosa en los términos de que causó un conflicto cognitivo en los maestros, pero resultó difícil de resolver, evaluamos la actividad y la rediseñamos. Coincidimos en que un sistema de dos ecuaciones en dos variables, además de involucrar dos ecuaciones nuevas, fue demasiado complejo como una situación novedosa; por ello, decidimos realizar la actividad en dos partes, esto es, introduciendo una primera parte antes de la segunda, la cual consistiría en el ejercicio de criptografía de la primera aplicación.

En esta primera parte, en lugar de una matriz 2×2 tomamos un número (que se puede pensar como una matriz de 1×1). Así, la fórmula de codificación $Ax = y$, donde A es una matriz, mientras que x y y son vectores, se redujo a $ap=c$, donde a, p y c son números (elementos de Z_{27}). Elegimos $a=4$, resultando $4p=c$, donde p es el equivalente numérico de una letra en el alfabeto y $\boldsymbol{c}$ corresponde al código numérico obtenido. De esta manera, no hay una agrupación de letras; la decodificación se hace letra por letra. Tras esta etapa, antes de la actividad con la matriz se aplicó un instrumento con la intención de que los maestros entendieran fácilmente la nueva estructura. Por su parte, la discusión incluyó aspectos sobre las condiciones necesarias para obtener la solución única a una ecuación y para que tuviera sentido hablar de una codificación.

En su nueva forma, la actividad fue aplicada a 26 maestros que se distribuyeron en seis equipos. La información que tenemos proviene de la grabación de tres equipos, elegidos al azar.

La primera parte no generó un conflicto muy grande en los maestros. A pesar de que dos grupos inicialmente usaron división y obtuvieron decimales, al final todos emplearon un método que consistía en relacionar la fórmula $p=c/4$ con $\boldsymbol{p}= (\boldsymbol{c}+27k)/4$, donde $0 \leq k \leq 4$, y en hallar el valor de k para que $\boldsymbol{p}$ fuera un entero; así, se fijaron en el número de vueltas que tenían que dar en el reloj. Esto sirvió para retroalimentar la segunda etapa.

En la segunda fase todos los equipos pensaron en utilizar una matriz inversa y todos lo hicieron, sin poner atención en el conjunto. Al obtener decimales como resultado, experimentaron un conflicto cognitivo. Los maestros intentaron varias alternativas para evitar los cocientes.

Al final, uno de los equipos recurrió a un método similar al que había manejado en la primera parte para obtener la solución, aunque esta vez utilizó matrices, mientras que otro hizo la resolución de un sistema de ecuaciones, valiéndose del factor de vueltas. El tercero intentó un

VERSIÓN PRELIMINAR

método que combinó prueba y error y resolución de ecuaciones en el nuevo sistema; sin embargo, no pudo lograr la solución a tiempo. Para mayor información sobre el rediseño y la segunda aplicación de esta actividad, se puede consultar la tesis de Aguilar (1999).

Las estrategias que emplearon los equipos, tanto en la primera aplicación como en la segunda, indicaron que los maestros prefirieron utilizar métodos diferentes a los formales, a pesar de que conocieran estos últimos. Sierpinska (2000) dice que hay una resistencia para utilizar métodos analítico-estructurales y que los estudiantes prefieren los métodos analítico-aritméticos, aunque resulten ineficientes. Sólo después de darse cuenta del poder y eficiencia de las propiedades estructurales, a través de demostraciones y la resolución de secuencias especialmente diseñadas, el estudiante empieza a manejarlas por iniciativa propia. Esto indica la atención especial que se requiere para provocar y motivar el uso de las propiedades estructurales, ya que al parecer no surge de manera natural.

Finalmente, se aplicó otro instrumento de ejercicios y preguntas para desarrollar su entendimiento de la aritmética modular. Aquí, el desempeño de los maestros fue satisfactorio.

3. Conclusiones

Los procesos inversos son difíciles de construir, ya que se requiere de un entendimiento completo de la estructura involucrada para poder deshacer un proceso, regresando los objetos iniciales a partir de sus productos.

Esta actividad, que utiliza la idea de un proceso inverso, sirvió para provocar un conflicto cognitivo en los maestros. Su diseño aseguró que todos los equipos se enfrentaran con el mismo obstáculo, al no trabajar dentro del contexto planteado. Los maestros utilizaban los conjuntos conocidos como los números reales y racionales, junto con sus operaciones básicas, para tratar de resolver un problema donde se planteaba otro conjunto con operaciones propias.

Basándonos en los productos de la resolución del instrumento de ejercicios y el desempeño de los maestros para solucionar el problema original, llama la atención el hecho de que, a pesar de que algunos grupos no pudieron resolver el problema tras sufrir el conflicto, sí estaban suficientemente preparados para recibir la información que les permitiera, por un lado, entender porqué obtenían un resultado incorrecto, por otro lado, tener una pista para resolver la actividad.

Esto puede ser un indicador para futuras investigaciones a fin de determinar cómo la construcción de un nuevo conocimiento puede ser facilitado con la aplicación de ejercicios de tal índole. Además, la observación de un concepto aplicado, donde el conocimiento fue útil en la resolución de un problema, jugó un papel de motivación para los participantes.

Además de que generan una motivación para lograr la solución correcta, estas actividades hacen que los maestros puedan entender los pasos involucrados en el proceso de resolución de un problema y las dificultades que los estudiantes pueden tener al enfrentarse con un conflicto cognitivo. Esta experiencia les puede ayudar en el diseño y aplicación de ejercicios con propósitos didácticos.

Esta actividad puede ser aplicada con estudiantes o maestros de diferentes niveles, debido a su flexibilidad para incorporar conceptos. Por ejemplo, la decisión de discutir los campos, los divisores de cero, las condiciones para obtener una solución única, la no-solución o una infinitud de soluciones queda a criterio del maestro. Además, la secuencia se puede presentar de manera más sencilla o compleja, según los antecedentes de los participantes; asimismo, se puede decidir la cantidad de información preliminar que se quiere dar.

Observamos que todos los equipos usaron varias estrategias para salir del

VERSIÓN PRELIMINAR

conflicto, las cuales involucraron:

- El uso de diferentes maneras de hacer lo mismo (por ejemplo, usar ecuaciones en lugar de matrices, pero cometiendo errores semejantes)
- Darse cuenta de la existencia de un nuevo contexto y de la necesidad de trabajar con un nuevo significado

Aunque no tenemos suficiente evidencia, los resultados de este trabajo nos lleva a pensar en la siguiente hipótesis: la conciencia de una nueva estructura facilita el pasaje del enfrentamiento entre el conocimiento anterior y el nuevo hacia la construcción de la nueva estructura. Se necesita más investigación para profundizar en tal aspecto.

Esta actividad también confirma la necesidad de capacitar a los maestros en cuanto a la introducción de nuevas estructuras. Quedarse en el contexto de los números reales y las cuatro operaciones les impide, por un lado, pensar en otras posibilidades, por otro, conocer la estructura algebraica global. Así, todos los conceptos adquieren su significado como ejemplos, no como nociones generales; por ejemplo, no se asimila la definición del concepto de elemento neutro sino se piensa en 1 ó 0 como identidades de multiplicación y suma, sin poner atención a las propiedades.

Además, este acercamiento permite incorporar las propiedades generales del concepto, ya que la abstracción y la generalización no se pueden realizar trabajando con un ejemplo específico. La manera como se abordan las operaciones y propiedades en los números reales puede no servir como una base inmediata para la generalización de propiedades a operaciones binarias en otros conjuntos.

Enfatizamos la importancia de incluir actividades y juegos del tipo usado en este trabajo para incentivar a los estudiantes y, al mismo tiempo, introducirlos a conceptos nuevos para llevarlos hacia el conflicto cognitivo, ya que el desequilibrio forma un ripio hacia la transición y reestructuración cognitiva, atizando el desarrollo intelectual de los estudiantes.

Sobre las operaciones binarias, creemos que estas actividades deben ir encaminadas a ayudar a que los estudiantes entrelacen el conjunto y la operación binaria en una estructura. Mostramos que los maestros se enfrentan a un obstáculo cuando no asimilan la idea de la estructura del conjunto de los números reales como una organización que contempla un conjunto de números y una o varias operaciones binarias con ciertas propiedades. Por ello, debemos prepararlos para que hagan frente a los cambios y ajustar sus maneras de pensar y entender con el fin de guiarlos hacia otras formas de percibir las cosas.

Por otro lado, el trabajo con grupos de aprendizaje cooperativo, haciendo una discusión grupal cuando sea necesario, propicia un efecto positivo en el aprendizaje debido a que los participantes tienen la posibilidad de percatarse y apropiarse de las ideas con que otros equipos abordan un problema. Más aún, forja al instructor a ver más de cerca y clasificar las dificultades que se presenten.

Bibliografía

Aguilar, P. (1999). *Entendimiento de las operaciones binarias: ¿Qué puede suceder en un cambio de contexto?* Tesis de maestría, Cinvestav, México.

Anton, A. (1994). *Elementary linear algebra*. USA: John Wiley & Sons, Inc.

VERSIÓN PRELIMINAR

Brown, A.; DeVries, D. J.; Dubinsky, E., y Thomas, K. (1997). Learning binary operations, groups and subgroups. *Journal of Mathematical Behavior 16* (3), 187-239.

Laborde, C. (1991). Deux usages complémentaires de la dimension sociale dans les situations d'apprentissage en mathématiques. En C. Garnier y N. Bednarz (Eds.), *Après Vygotski et Piaget* (pp. 29-49). Editions De Boeck.

Lefebvre-Pinard, M. (1989). Le conflit socio-cognitif en psychologie du développement: est-ce toujours un concept heuristiquement valable? En N. Bednarz y C. Garnier (Eds.), *Construction des savoirs* (pp. 151-156). Montreal, Canadá: Agence d'ARC.

Reynolds, B.; Hagelgans, N.; Schwingendorf, K.; Vidakovic, D.; Dubinsky, E.; Shahin, M., y Wimbish, G. (1995). *A practical guide to cooperative learning in collegiate mathematics*. MAA Notes, 37.

Sierpinska, A. (2000). On some aspects of students thinking in linear algebra. En J. L. Dorier (Ed.), *On the teaching of linear algebra* (pp. 209-246). Kluwer Academic Publishers.

Steffe, L. P. (1990). Inconsistencies and cognitive conflict: a constructivist's view. *Focus on Learning Problems in Mathematics 12* (3-4), 99 - 109.

Swan, K. (1983). Teaching decimal place value: a comparative study of "conflict" and "positive only" approaches. En R. Hershkowitz (Ed.), *Proceedings of the Seventh International Conference for the Psychology of Mathematics Education* (pp. 211-216). Rehovot, Israel: Weizmann Institute of Science.

Underhill, R. (1991). Two layers of constructivist curricular interaction. En E. Von Glasersfeld (Ed.), *Radical Constructivism in Mathematics Education* (pp. 229-248). Dordrecht, Holland: Kluwer.

Vidakovic, D. (1997). Learning the concept of inverse function in a group versus individual environment. En E. Dubinsky; D. Mathews, y B. Reynolds (Eds.), *Readings in Cooperative Learning* (pp. 173-195). MAA Notes, 44.

Zaslavsky, O. y Peled, I. (1996). Inhibiting factors in generating examples by mathematics teachers and student teachers: the case of binary operation. *Journal for Research in Mathematics Education 27* (1), 67-78.

Asuman Oktaç
Departamento de Matemática Educativa
Cinvestav-IPN
E-mail: oktac@enigma.red.cinvestav.mx

Priciliano Aguilar
Unidad Profesional Interdisciplinaria de Ingeniería y Tecnologías Avanzadas del IPN.
México.
E-mail: ppriss@hotmail.com

VERSIÓN PRELIMINAR

ANEXO 1

EJERCICIOS DEL INSTRUMENTO APLICADO DESPUÉS DE LA ACTIVIDAD DE CRIPTOGRAFÍA

Consideremos un reloj de 9 elementos (0, 1, 2, 3, 4, 5, 6, 7, 8). Denotemos este conjunto como Z_9, es decir, $Z_9=\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

Realice las siguientes actividades

1. ¿Existe elemento identidad aditivo en Z_9? ¿Por qué?

2. Resolver las siguientes ecuaciones

a) $x + 3 = 0$, ¿Cómo llamarías a x?
b) $x + 6 = 0$, ¿Cómo llamarías a x?
c) $x + 2 = 7$
d) $8 + x = 1$
3. Discutir la ecuación $x + k=m$

4. ¿Existe elemento identidad respecto a la multiplicación? ¿Por qué?

5. Resolver las siguientes ecuaciones

a) $2x=1$, ¿Cómo llamarías a x?
b) $7x=1$, ¿Cómo llamarías a x?
c) $8x=1$, ¿Cómo llamarías a x?

6. Resolver la ecuación $3x=1$.

7. Discutir la ecuación $ax=1$ (considere casos). ¿Cómo llamarías a x?

8. Resolver las siguientes ecuaciones

a) $5x=3$ b) $6x=8$ c) $3x=6$

9. Discutir la ecuación $ax=b$ (considere casos).

VERSIÓN

Relime