

Curso de Actualización

Matemática Discreta usando Isetl

**Centro de Postgrado y Actualización Profesional del Instituto de
Computación (InCo) de la Facultad de Ingeniería (Fing) de la
Universidad de la República (Udelar)**

Responsable del curso:

Sylvia da Rosa (docente del InCo)

8 de octubre al 14 de noviembre de 2007

Modalidad semipresencial

Presentación del informe final:

27 de diciembre de 2007

IPES - Montevideo



El lugar de los Naturales en la Sociedad de la Información



Mercedes Villalba

PROUESTA DE ENSEÑANZA DE CONTENIDOS DE MATEMÁTICA DISCRETA USANDO EL SOFTWARE “ISETL”

SUMARIO

<u>Curso de Actualización.....</u>	<u>1</u>
 <u>PROUESTA DE ENSEÑANZA DE CONTENIDOS DE MATEMÁTICA DISCRETA</u>	
<u>USANDO EL SOFTWARE “ISETL”.....</u>	<u>4</u>
<u>SUMARIO.....</u>	<u>4</u>
<u>DEFINICIÓN DE TÉRMINOS.....</u>	<u>5</u>
<u>NIVEL DE APLICACIÓN DE LA PROUESTA:.....</u>	<u>8</u>
<u>CONTENIDO MATEMÁTICO: Conjuntos numéricos finitos. Aritmética módulo p.....</u>	<u>8</u>
<u>OBJETIVOS.....</u>	<u>9</u>
<u>CONTENIDOS.....</u>	<u>10</u>
<u>1. INTRODUCCIÓN AL LENGUAJE DE ISETL.....</u>	<u>10</u>
<u>2. CONCEPTOS MATEMÁTICOS.....</u>	<u>13</u>
<u>3. SITUACIONES QUE DAN SIGNIFICADO A:.....</u>	<u>14</u>
<u>4. DE LAS CONGRUENCIAS A LOS DÍGITOS DE CONTROL.....</u>	<u>19</u>
<u>REFERENCIAS BIBLIOGRÁFICAS.....</u>	<u>31</u>
<u>PROYECCIÓN DE LA PROUESTA.....</u>	<u>32</u>
<u>EVALUACIÓN DEL CURSO.....</u>	<u>32</u>

DEFINICIÓN DE TÉRMINOS

- **La Matemática Discreta** (MD) trabaja con conjuntos discretos, a diferencia de la Matemática Continua que trabaja con conjuntos continuos, como los Números Reales. Incluye contenidos de los programas de Educación Secundaria: Teoría de Conjuntos, Relaciones, Funciones, Combinatoria, Inducción Completa, Divisibilidad.
- **El lenguaje matemático** describe los objetos matemáticos y permite reconocerlos como tales por su formalismo, diferenciándolos de expresiones que pueden utilizar los mismos signos, pero carentes de sentido. Por ejemplo: $(2+5) * 1/3$ y $2 + * 5$ $1/ (3)$.
Las expresiones matemáticas se evalúan aplicando reglas de transformación que pueden seguir distintas estrategias, pero que llegan a la misma forma canónica (si existe).
- **El lenguaje de programación** también es un formalismo, que representa objetos mediante expresiones del lenguaje, las cuales se evalúan utilizando reglas (algoritmos) de transformación sobre las expresiones.

IsetL es un software libre de lenguaje de programación matemática, que usa una sintaxis similar a la notación matemática estándar y fue desarrollado específicamente para la enseñanza de contenidos matemáticos a nivel de grado. Es un programa interactivo que permite al usuario la comunicación a través de mensajes construidos a partir de objetos y funciones predefinidas.

RELACIÓN ENTRE LENGUAJE MATEMÁTICO Y LENGUAJE DE PROGRAMACIÓN

Ambos lenguajes han sido diseñados por humanos, pero mientras el lenguaje matemático es manejado por personas, el de programación lo es por un computador. Los humanos pueden advertir inexactitudes o ambigüedades, pero el computador no: se limita a ejecutar instrucciones sin detenerse a reflexionar ni en la pertinencia ni en el significado de las mismas, actuando siempre como si fueran completas y exactas. Por ello programar exige rigurosidad en el uso del lenguaje.

Esta rigurosidad solo es posible si los conceptos matemáticos involucrados están claramente definidos por el usuario, y por tanto, necesariamente comprendidos, elaborados y comunicados. O sea que la traducción del concepto matemático al lenguaje de programación asegura una construcción previa de dicho contenido y de las relaciones implicadas. Este es el valor didáctico de Isetl como auxiliar en la enseñanza de la Matemática.

CIENCIA DE LA COMPUTACIÓN

Es una nueva rama de las matemáticas dedicada a la teoría y práctica de la confección de programas y tiene por misión traducir los cálculos a programas, de cuya ejecución se encargarán computadoras electrónicas de gran velocidad, "potentes auxiliares" en el quehacer matemático.

Concierne a la relación entre la manipulación simbólica mecanizada y la humana, referidas como computar y programar respectivamente.

Computar es una actividad matemática y programar es computar por medio de una máquina, por lo tanto es también una actividad matemática. En el mapa de las disciplinas académicas, la ciencia de la computación debe ser ubicada entre la matemática formal y la lógica aplicada.

FUNDAMENTACIÓN DEL USO DE ISETL COMO RECURSO DIDÁCTICO PARA LA ENSEÑANZA DE LA MATEMÁTICA.

Explica Sylvia da Rosa¹: *la matemática se ha desarrollado hacia direcciones que están fuera del sistema educativo, sin embargo, sus aplicaciones son fundamentales para la formación actual del estudiantado. El pensamiento algorítmico, el razonamiento lógico, la formalización de soluciones, ataúden a docentes de matemática y de computación. Los problemas que dependen del razonamiento humano, nunca podrán prescindir del mismo. En pocas palabras: las computadoras computan (calculan), pero nunca van a llegar a razonar (Hamilton, 1978). Creemos que esta realidad, incide directa y profundamente sobre el sistema educativo, cambia radicalmente objetivos, contenidos y metodologías de lo que enseñamos, cómo lo enseñamos, para qué enseñamos, siendo imprescindible poner el acento en enseñar a razonar, abstraer, analizar, representar, lo cual, a nuestro juicio ha sido descuidado por el enorme peso que la enseñanza pone en desarrollar destrezas en el cálculo y en la demostración mecánica de teoremas.*

El computador digital moderno es básicamente un sistema discreto y muchas de sus propiedades pueden ser entendidas y descritas modelándolas en un sistema matemático discreto.

Hoy día, la Economía, las Ciencias Sociales, las Ciencias gerenciales, la Ingeniería eléctrica, la Física simbólica, por solo nombrar algunas, tienen necesidad de resolver problemas que se modelan utilizando herramientas de MD. En el mercado laboral, es cada

¹ LA MATEMATICA DISCRETA COMO FORMACION BASICA Instituto de Computación, Facultad de Ingeniería, Universidad de la República, Montevideo, Uruguay

vez más frecuente que las personas deban enfrentarse a situaciones que involucran toma de decisiones, procesos de abstracción y razonamientos lógicos.

El lenguaje de programación Isetl se utiliza para representar objetos matemáticos.

El paso de la Matemática a las Ciencias de la Computación consiste en la automatización.

Para ello es necesario usar símbolos, cuyos significados deben estar claramente identificados, de manera que al trabajar con ellos, se ponen en juego los conceptos sustituyendo el mero cálculo, que pasa a ser realizado por la máquina. Los conceptos y procesos cognitivos dejan a la máquina la ejecución de cálculos complejos y/o tediosos, a gran velocidad, permitiendo avances significativos en la construcción conceptual.

Da Rosa plantea “*un enfoque alternativo que rescate la naturaleza discreta de los contenidos matemáticos y al mismo tiempo permita dedicarles mayor tiempo y profundidad, relacionándolos entre ellos.*”

Para encarar el proceso de resolución de un problema dado se plantea una metodología que incorpora el método formal desde el nivel secundario en los siguientes pasos:

- *Crear un algoritmo (método) para resolver el problema, expresándolo en algún lenguaje informal (por ejemplo, en español)*
- *Expresar el algoritmo matemáticamente*
- *Construir un programa que implemente el algoritmo definido matemáticamente*
- *Verificar la correctitud del algoritmo (o del programa)*

El tercer punto planteado puede obviarse, sin que el enfoque sea alterado, en caso de que no sea posible incorporar en el curso un lenguaje de programación.”

EN SÍNTESIS:

Se trata de estudiar los conceptos matemáticos desde un **enfoque computacional**. Escribir en Isetl lo que se ha definido matemáticamente hace necesario conocer aspectos de la sintaxis, que son mínimos. Isetl es un instrumento alternativo en el proceso de resolución de un problema que genera aprendizajes matemáticos importantes.

NIVEL DE APLICACIÓN DE LA PROPUESTA:

Los destinatarios, en principio, son estudiantes de primer año de Formación Inicial de Maestros, aunque tal vez podría también resultar adecuada para alumnos de Primer Ciclo de Enseñanza Secundaria, lo cual dejaría a consideración de quienes tienen experiencia en el subsistema.

CONTENIDO MATEMÁTICO: Conjuntos numéricos finitos. Aritmética módulo p.

Fundamentación de la selección del contenido:

Introducir el concepto de congruencia numérica módulo un natural, supone el aprendizaje previo por parte de los alumnos de las cuestiones básicas sobre divisibilidad y, por otra parte, los familiariza con las definiciones y propiedades que se ponen en juego, estableciendo conexiones que favorecen un abordaje sistémico de la Matemática.

La diversidad de aspectos de la vida cotidiana que se fundamentan en el concepto objeto de estudio, y que trascienden ampliamente lo abordado en este trabajo, permite cargarlo de significatividad sicológica, sin descuidar la potencialidad para el desarrollo de los procesos cognitivos.

Los códigos detectores de errores representan un desafío que intentan superar los especialistas en Teoría de Números: actualmente, la información se representa en forma de sucesión de números, pero los códigos empleados deben ser capaces de transmitir los mensajes con eficacia, detectar y corregir errores.

Es posible plantear a los alumnos algunas situaciones de este tipo, que ellos pueden resolver con sus conocimientos matemáticos.

La existencia de diferentes sistemas de signos que permiten representar o transmitir la información constituyen diferentes códigos, diferentes representaciones de un mismo significado. Así, el código lingüístico, el matemático y el informático son formas diferentes de un mismo contenido. En esta propuesta, Isetl es uno de los lenguajes en que han de expresarse los conceptos.

Las actividades con Isetl constituyen una alternativa dentro de las planificadas para llevar a cabo la propuesta.

Conceptos relacionados para introducir y desarrollar el tema LOS DÍGITOS DE CONTROL

- ❖ Conjuntos numéricos, específicamente N y Z
- ❖ División entera
- ❖ Clases de equivalencia
- ❖ tuplas
- ❖ Base de nuestro sistema de numeración
- ❖ Algoritmo
- ❖ Función
- ❖ Trasmisión de información
- ❖ códigos
- ❖ detección y corrección de errores
- ❖ Inicio en Isetl: de acuerdo a las necesidades de cada actividad, se introduce:
 - ❖ Simbología básica
 - ❖ Sintaxis
 - ❖ Términos reservados
 - ❖ Funciones predefinidas
 - ❖ Bool



Similitudes y
diferencias con el
lenguaje matemático

OBJETIVOS

- ❖ Favorecer los procesos de conceptualización relacionados con la divisibilidad
- ❖ Plantear la precisión en la comunicación matemática como indicador de apropiación conceptual
- ❖ Habilitar la interacción con el software Isetl como mediador en los aprendizajes matemáticos.
- ❖ Incluir el uso social de la aritmética como uno de los contextos significativos

CONTENIDOS

1. INTRODUCCIÓN AL LENGUAJE DE ISETL

Se explicita a los alumnos que vamos a trabajar paralelamente con código lingüístico (en nuestras consignas y explicaciones), con el código matemático (con la simbología que ya conocen y con la que vayamos incorporando) y con un lenguaje de programación matemática llamado ISETL (Interactive SET Language), lenguaje interactivo, basado en el concepto matemático de conjunto (finito).

ACTIVIDADES

a. A es el conjunto formado por los números 3, 5, 11, 56, 21, 184 y B es el subconjunto de A formado por los números mayores que 50. Determinar en lenguaje matemático dichos conjuntos.

b. En la computadora se presenta este programa:

> **A:={3, 5, 11, 56, 21, 184};**

> **B:={x:x in A|x>50};**

> **B;**

{56, 184};

Se ha representado lo mismo que se resolvió en (a).

1. comparar las notaciones y establecer las equivalencias entre lenguaje matemático e informático.

2. en el lugar donde está el cursor, escribir el subconjunto C de los números incluidos en A menores que 50 y luego evaluar dicha expresión más de una vez.

Se espera que los alumnos establezcan similitudes y diferencias

similitudes	diferencias	
	isetl	matemática
Se determinan conjuntos por extensión y por comprensión	A:={ };	A={ };
Los elementos de los conjuntos se separan con comas y se escriben entre llaves	x: x in 	x / x ∈ /
Los elementos del conjunto no están ordenados	El uso de coma o "y" para separar propiedades de la variable da mensaje de error.	Las propiedades de la variable (x) pueden separarse con coma o con el nexo "y"

Se conceptualiza “evaluar una expresión”:

1. intuitivamente como “preguntar cuál es el valor de la expresión”
2. formalmente como “dar el valor a una expresión, aplicando reglas de transformación definidas, que la llevan a su expresión canónica”.

El lenguaje de programación obedece a reglas sintácticas porque sus expresiones son evaluadas automáticamente, a diferencia de la evaluación que realiza una persona.

c. Interpretar la sintaxis de Isetl, teniendo en cuenta las **definiciones** y las **respuestas**:

```
>A:={-3, 5, 11, 56, -21, 184};  
>C:={x<50|x in A};  
>C;  
{true, false};  
>  
>D:={x: x in A|x < 50};  
>D;  
{-21, -3, 5, 11};  
>
```

d. En las siguientes expresiones de Isetl se realizan dos procedimientos: **definir** y **evaluar**. Identifica cada uno de ellos e interpreta en qué consiste el procedimiento realizado por la computadora: exprésalo en lenguaje matemático. Por ejemplo:

<pre>> a:=1/4; > a; 0.250;</pre>	<p>defino “a” como “1 dividido 4” pido el valor de “a” o sea pido que evalúe la expresión, Isetl realiza el cálculo y devuelve su expresión canónica.</p>
<pre>> d:=sqrt25; > d; OM; > d:=sqrt(25); > d; 5.000;</pre>	<p>Se espera que los alumnos comparan las dos definiciones de “d” y sus correspondientes respuestas y que reconozcan la operación matemática aplicada. La primera definición no puede ser evaluada porque el objeto no está definido (OM) En la segunda definición “25” toma el valor de una variable (por lo que se escribe entre paréntesis): en Isetl, “sqrt” es una función predefinida que calcula la raíz cuadrada</p>
<pre>> is_integer(3); true; > is_integer(4/2); false;</pre>	<p>Por similitud con el caso anterior, se espera que los alumnos identifiquen “is_integer” como una función predefinida, pero de distinto codominio. Si el valor que toma la variable es un entero, devuelve “true”, si no lo es, devuelve “false”.</p>
<pre>> 4+3**2; 13;</pre>	<p>En este caso se trata de identificar la codificación de la operación potenciación</p>
<pre>> 13/0; !Error: Divide by zero</pre>	<p>Se pone en juego la definición de división</p>

<pre>> b:=3*75 + a; > b; 225.250; > a:=3; > b:=3*75 + a; > b; 228;</pre>	<p>Se evalúa una expresión donde está involucrada “a”, definida previamente. Al volver a evaluarla, devuelve un valor diferente, porque “a” fue redefinida. Se discute la validez matemática del procedimiento y la consecuente importancia del orden en Isetl.</p>
<p>Se propone definir expresiones similares y evaluarlas en lenguaje matemático e informático</p>	

e. Un comercio A vende un electrodoméstico en 5 cuotas de \$ 1750 y otro comercio B en 6 cuotas de \$ 1000 y una entrega inicial de \$ 3000. Juan opina que paga lo mismo en cualquier caso ¿y tú? Expresa la situación en código matemático y luego compara con la solución de Isetl.

Matemática	Isetl
$A = 5 * 1750$	e> A:= 5*1750;
$B = 6 * 1000 + 3000$	> B:= 6*1000+3000;
$A = B$	> A=B;
8750 = 9000 falso	false;
<p>En Matemática se usa el signo = para definir y para evaluar, en Isetl, solo para preguntar.</p>	
<p>El símbolo := se lee “se define como”.</p>	
<p>La sintaxis de una definición es: nombre:=expresión</p>	

2. CONCEPTOS MATEMÁTICOS.

a. ¿Cómo defines el Número Natural, a partir del concepto de Número Entero? Escríbelo en código lingüístico y matemático. Intenta definir la función “natural” y luego la comparas con la definición siguiente, que copias y evalúas en Isetl.

```
> is_natural:=func(x);
>>     return (is_integer(x) and x>=0);
>>     end;
```

Matemática	Isetl
Natural: $Z \rightarrow N$	is_natural: $Z \rightarrow \text{Bool}$
Natural(x) = $x / x \in Z \text{ y } x \geq 0$	
<i>Natural es un conjunto infinito por lo que no puede definirse por extensión; para cada Entero del dominio Isetl devuelve “true” en caso de ser mayor o igual a cero; “false” en caso contrario.</i>	
<i>func, return y end son palabras reservadas de Isetl para identificar la función, devolver un valor y terminar la definición respectivamente.</i>	
<pre> graph TD X([X]) --> Cond{¿x ≥ 0?} Cond -- SI --> True["devolver \"true\""] Cond -- NO --> False["devolver \"false\""] </pre>	<p>Se interpreta la evaluación en cada caso, teniendo en cuenta el algoritmo que realiza la computadora.</p>

Observación: se suponen conocidos los conceptos de “múltiplo”, “divisor”, “división entera”.

3. SITUACIONES QUE DAN SIGNIFICADO A:

a. COCIENTE Y RESTO

Felipe debe envasar 590 l de vino en damajuanas, en lo posible, iguales. Para calcular el número de damajuanas necesarias realiza esta operación en la que se borraron algunos números. Debes

1. completarla y justificar el procedimiento
2. decir qué información se lee en

a. El dividendo-----

b. El divisor-----

c. El cociente-----

d. El resto-----

590
196

3. ¿Cómo resuelve Felipe el envasado de todo el vino?-----

Los alumnos pueden realizar cálculos estimativos, proceder por ensayo y error, pero deben justificar poniendo en juego la definición de división entera. Se solicita la interpretación de cada término a efectos de dar contenido a la “etiqueta” y representarse mentalmente la situación concreta a resolver, pues se trata de un curso para futuros docentes, donde el significado de las operaciones es un contenido didáctico muy importante. Por otra parte, y también si fueran estudiantes liceales, la contextualización extra matemática ayuda a la construcción del concepto, que, en su momento, incluirá varias de las situaciones concretas previamente resueltas.

La pregunta 3 hace necesario leer el cociente y el resto como los dos resultados de la división entera, uno ya conocido (el cociente) que, en este caso no da respuesta al problema, como los generalmente planteados para resolver con división.

590 dividido un divisor (d) da 196 y un resto (r)

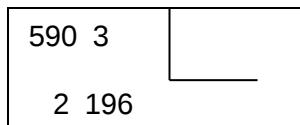
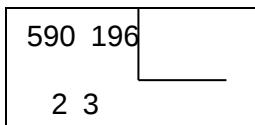
*$590 = d * 196 + r$ (por definición de división entera)*

*$590 - r = d * 196$*

(590 - r) es múltiplo de d y de 196 \rightarrow d y 196 son divisores de (590 - r)

Se discute si se pueden intercambiar d y 196 en la división, se formaliza el cálculo del resto y del cociente (en matemática).

Considerando que nuestros alumnos de magisterio han olvidado el algoritmo de la división entre tres cifras (debido al uso automático de la calculadora y de que trabajaron fundamentalmente con los números racionales y reales), es muy probable que dividan 590 entre 196 con la calculadora, obteniendo un cociente en notación decimal, con muchos dígitos después de la coma, pero ningún resto. Aproximar a enteros es un aprendizaje que se plantea en esta instancia.



El siguiente paso es darse cuenta que la división realizada es una estrategia para encontrar el mayor número que multiplicado por 196 es igual o menor que 590 (en este caso resultó menor y por lo tanto hay un resto distinto de cero). Pero en realidad, para reconstruir la división deben intercambiarse divisor y cociente entre sí. Recién estarán en condiciones de leer la información en cada término. Y para dar respuesta al punto 3 deben tener en cuenta el resto pues se pregunta cómo resolvió Felipe el envasado de todo el vino en damajuanas, en lo posible iguales: (196 damajuanas de 3 litros y 1 de dos litros).

Respecto a la posibilidad de intercambiar los divisores y cocientes entre sí, es posible matemáticamente porque se cumple la definición de división entera en cualquier caso, pero en el problema no es posible pues la división se realizó para obtener la cantidad de damajuanas necesarias o sea que debe mantenerse el cociente original (196).

Posteriormente se implementan los cálculos en isetl:

Implementar en Isetl el cálculo del resto

> 590 mod 196;

2;

Evalúa en Isetl estas expresiones, interpreta el código y escribes la expresión para un caso genérico. > (590 - 2) div 196;

> (590) div 196;

el cociente de la división entera entre a y b a div b

Se espera que los alumnos observen que tanto si el dividendo es múltiplo o no del divisor el cociente es un número natural, o sea que la función “div” está definida para la división entera.

Verificar en las divisiones realizadas manualmente para resolver el problema:

>590 mod 196;

2;

>(590) div 196;

3;

>(590) div 3;

196;

>590 mod 3;

2;

>

Se trata simplemente de verificar con las funciones predefinidas en isetl los resultados obtenidos en los algoritmos de cálculo matemático, a efectos de familiarizar con el lenguaje de programación.

b. CLASES RESIDUALES

Un crucero tarda 79 horas para desembarcar en el primer puerto disponible. Sale el domingo a las 6 de la tarde ¿Cuál es el día y hora de llegada?

En este caso se trata de poner en juego el concepto de división entera en relación a la medición del tiempo, desde los saberes sociales más que matemáticos, pues, aunque no se tenga conocimiento formal sobre el sistema de medición del tiempo, que es mixto y complejo, las personas realizan cálculos para resolver situaciones cotidianas. Esto permite decidir cuál es el divisor.

79 dividido 24 da cociente 3 y resto 7, con lo cual se lee que la duración de la travesía es 3 días y 7 horas. Luego, el conocimiento social del orden de los días, lleva a contar 3 días a partir del domingo. Finalmente se agregan 7 horas a las 6 de la tarde, o sea $18 + 7 = 25$; pero la hora 25 no existe en el día domingo, así que se concluye que el crucero arriba a la hora 1 del día lunes.

Lo importante es ver que cuando se cuentan objetos como los libros de una biblioteca, hacemos una correspondencia con cada uno de los naturales y el último nombrado da nombre al cardinal del conjunto de libros, que será diferente si agrego libros y que puedo agregar siempre uno más a la colección. ¿Sucede lo mismo cuando quiero encontrar el nombre del día después de transcurridos algunos días? Depende del número de días transcurridos ¿Por qué? Estamos trabajando en un conjunto finito, el de los días de la semana, que son 7, así que en adelante se empiezan a repetir en el conocido orden.

Cada 7 días llegaremos al mismo nombre ej. Del domingo al domingo

Cada 8 días llegaremos al nombre siguiente ej. Del domingo al lunes

Cada 9 días llegaremos al nombre siguiente del siguiente ej. Del domingo al martes

¿Cuándo volvemos al domingo? Dar una explicación matemática (se espera que hagan referencia al resto de la división y a su relación con el divisor).

Se transfiere el razonamiento a las horas del día, a los días del mes y a los meses del año, a efectos de determinar en qué casos de conjuntos finitos, se puede aplicar la regla.

Si dos números naturales tienen el mismo resto en la división por un número natural m , se dice que son congruentes módulo m

Completar la columna de los restos ¿qué se observa ? ¿Puede haber otros restos en la división por 5?

número	divisor	resto
9	5	
10	5	
13	5	
16	5	
21	5	
22	5	
25	5	
28	5	
34	5	
37	5	

10 y 25 tienen el mismo resto 0 en la división por 5

$10 \equiv_5 25$ se lee “10 es congruente con 25 módulo 5 “

$a \equiv_m b$ se lee “a es congruente con b módulo m “

Se puede probar que esta relación cumple las propiedades refleja, simétrica y transitiva: aplicarlas ahora a casos particulares, en módulo 5.

Decimos que “a es congruente con b módulo m “es una equivalencia, por lo que determina, en el conjunto N, una partición en clases de equivalencia¹, que llamamos **clases residuales**.

Notación: $\bar{0} \pmod{5}$ clase residual 0 módulo 5

“En general², la división entera entre p solo puede arrojar restos que estén en el conjunto $\{0, 1, \dots, p-1\}$ formado por el cero y los primeros $p-1$ naturales. Podemos considerar entonces que la aritmética módulo p que describimos actúa sobre el conjunto $\{0, 1, \dots, p-1\}$ ”. “Otra posibilidad es considerar que está definida sobre un conjunto de clases de equivalencia, en las que hemos identificado entre sí a todos los números que difieren en un múltiplo de p”³

Expresar en lenguaje matemático (si es posible como clases residuales) y en lenguaje Isetl, los cálculos realizados en el problema del crucero.

Matemática	Isetl	problema
$79 \equiv_{24} 7$	79 mod 24; > 79 mod 24; 7; > 79 mod 24 = 7 mod 24; true; >	Cálculo de la cantidad de horas (7) que no completan un día correspondientes a 79 horas
Cociente de 79 : 24	79 div 24;	Cálculo de la cantidad de días (3) correspondientes a 79 horas
$18 + 7$	$18 + 7;$	A la hora 18 (cuando han pasado exactamente 3 días) se agregan las 7 horas (que

¹ Se supone conocido el concepto de “clases de equivalencia” y sus propiedades.

² Expresa una generalización, respecto a casos particulares, que los autores plantean en su trabajo y que también se plantea aquí, pues se estaba trabajando con módulo 5.

³ Una introducción a los códigos detectores y correctores de errores. Omar Gil y Pablo Fernández <http://www.fing.edu.uy/~omargil/educmate/codyal31-71.pdf> página 11

		completan las 79)
$25 \equiv_{24} 1$	25 mod 24; > 25 mod 24 = 1 mod 24; true;	7 horas después de las 18 suma 25, con lo que se pasa a la hora 1 del día siguiente

Plantear una situación de la vida cotidiana que se resuelva usando esta expresión:

45 mod 7;

Se espera que algunos alumnos planteen situaciones para cuya solución deba tenerse en cuenta el resto de la división entera y otros planteen situaciones cuya interpretación tenga que ver con la clase correspondiente módulo 7, que se discuta en qué caso se trata de clases residuales o no. Por ejemplo:

1. La profesora dijo a Juan que a partir de hoy lunes tiene 45 días para entregar el informe. A mí también me dio 45 días a partir del miércoles pasado. Solo tenemos clase de lunes a viernes. ¿Qué día debe entregarlo cada uno? ¿Tenemos realmente la misma cantidad de días disponibles?
2. En un campamento se dispone de 45 kg de naranjas que se distribuyen equitativamente para cada día de la semana que dura la estadía y se regala a unos vecinos la cantidad que se prevé que podría quedar. ¿Cuántos kg les entregarán?

¿Cuántas semanas y días pasaron desde el 1º de julio hasta el 29 de agosto? Usar el lenguaje Isetl para contestar.

(31+29) div 7; (31 + 29) mod 7

Suma de clases residuales:

Para calcular la clase de esta suma (31 + 29) módulo 7 puedo llevar la expresión a su forma canónica y calcular la clase o sea $31 + 29 = 60$; $60 \equiv_7 4$

O puede calcular la clase de cada sumando y sumar las clases: $31 \equiv_7 3$; $29 \equiv_7 1$; $3+1 = 4$

Expresar en código lingüístico e Isetl esta propiedad.

La clase residual módulo m de la suma de dos naturales es igual a la suma de las clases residuales correspondientes.

>31 mod 7 + 29 mod 7 = 60 mod 7;

true;

4. DE LAS CONGRUENCIAS A LOS DÍGITOS DE CONTROL

En el planteo anterior se ha presentado la aritmética módulo un natural p , basada en los restos de la división entera entre p , de la cual deriva el concepto de congruencia y se define una relación de equivalencia en el conjunto de los números naturales, que establece una partición en clases residuales.

Surgen aplicaciones interesantes como la detección y corrección de errores en la transmisión de la información: Por ejemplo, el dígito de control de la cédula de identidad uruguaya se calcula multiplicando cada dígito del documento por el dígito correspondiente del número de control (2987634), luego se suman los resultados obtenidos y se calcula el opuesto.

Más eficientes resultan los códigos que emplean un módulo primo, porque se evitan los divisores de cero, y con ello, la posibilidad de introducir errores que los códigos no pueden detectar. Por ejemplo el ISBN, número de control de los libros, cuyas primeras nueve cifras dan información sobre el libro, y la última es un carácter de control que se calcula en módulo once, y cuyo resto diez se representa con X, permite detectar todos los errores de una cifra, puede recuperar un número cualquiera que se haya borrado (suponiendo que hay un error) y el intercambio de dos cifras cualesquiera.

La Teoría de códigos detectores y correctores de errores trata problemas relacionados con la trasmisión de la información, específicamente la búsqueda de fidelidad a través del diseño de estrategias para detectar y corregir errores en la trasmisión.

Todo mensaje tiene un emisor que lo envía a un potencial receptor, quien para interpretarlo debe conocer el código en que está registrado. Llega a través de un canal, que muchas veces tiene ruidos, por lo que resulta poco fiable y el mensaje original puede llegar alterado. Así cuando se graban datos en un disco, los dispositivos correspondientes (láser, cabezal) pueden cometer errores: una huella dactilar en la superficie del CD puede ser un “ruido”. Los códigos de barrra que identifican los productos, están diseñados para detectar posibles errores de lectura.

La posibilidad de digitalizar cualquier información hace posible definir operaciones entre listas de ceros y unos y emplear algunas ideas geométricas para estudiarlas.

1. Verificar el código de control de su CI de acuerdo al procedimiento indicado en la introducción de este tema, teniendo en cuenta que siempre se opera en clase residual 10, que corresponde a la base de nuestro sistema de numeración decimal. Esta tabla organiza la información

Cifras de la CI (C)	Módulo verificador (m)	$(C * m) \bmod 10$
	2	
	9	
	8	
	7	
	6	
	3	
	4	
Suma mod 10		
Opuesto mod 10		

Es necesario resignificar el concepto de **opuesto en un conjunto módulo 10**.

a es opuesto de **b** si $a + b = 0$

En la aritmética módulo 10 todos los múltiplos de 10 pertenecen a la clase residual 0

El **opuesto de a** es $10 - a$

2. Analizar cada paso y pensar cómo puede implementarse en Isetl:

- Cuál es la variable
- Cuál es la constante
- Cómo se pueden expresar para operar con ellas ordenadamente

Considerando que los dígitos van multiplicándose de acuerdo al lugar que ocupan en el número tanto de CI como de verificador, no es correcto expresarlos como conjunto de cifras y se introduce la **tupla** como un objeto predefinido en isetl similar al conjunto pero que sí cumple la relación de orden. Se trabaja con una tupla de tres términos como ejercicio.

3. Notación **t= [21, 6 ,5]** En el ejemplo, el primer término se nota $t(1)$ y vale 21, el 2^{o} se nota $t(2)$ y vale 6, etc.

Definir **t** y evaluar en Isetl cada término

```
> t:=[21, 6 ,5];
> t(1);
21;
> t(2);
6;
> t(3);
```

5;

Los siguientes ejercicios tienen por objetivo familiarizar a los alumnos con los algoritmos necesarios para el cálculo del dígito de control de la CI, pero aplicados a una tupla de menor cantidad de términos, a efectos de facilitarlos.

4. Definir en matemática y en Isetl otra tupla de tres términos
5. Indicar el producto de cada término de t por cada término de $T2$ en el orden correspondiente.
6. Expresar la clase residual módulo 10 de cada producto.
7. Sumar todos los resultados obtenidos y expresarlo módulo 10
8. Restarle a 10 la expresión anterior

matemática	Isetl
$T2 = [4, 10, 5]$	$T2 := [4, 10, 5];$
$t (1) * T2 (1) ; t(2) *T2 (2); t(3)*T2(3);$	$t (1) * T2 (1) ; t(2) *T2 (2); t(3)*T2(3);$
$t (1) * T2 (1) \bmod 10; t(2) *T2 (2) \bmod 10; t(3)*T2(3) \bmod 10;$	$t (1) * T2 (1) \bmod 10; t(2) *T2 (2) \bmod 10; t(3)*T2(3) \bmod 10;$
$t (1) * T2 (1) \equiv_{10}; t(2) *T2 (2) \equiv_{10};$ $t(3)*T2(3) \equiv_{10};$	
$t (1) * T2 (1) \bmod 10 + t(2) *T2 (2) \bmod 10 + t(3)*T2(3) \bmod 10;$	$t (1) * T2 (1) \bmod 10 + t(2) *T2 (2) \bmod 10 + t(3)*T2(3) \bmod 10;$
$(t (1) * T2 (1) \bmod 10 + t(2) *T2 (2) \bmod 10 + t(3)*T2(3) \bmod 10) \bmod 10;$	$(t (1) * T2 (1) \bmod 10 + t(2) *T2 (2) \bmod 10 + t(3)*T2(3) \bmod 10) \bmod 10;$
$10 - (t (1) * T2 (1) \bmod 10 + t(2) *T2 (2) \bmod 10 + t(3)*T2(3) \bmod 10) \bmod 10;$	$10 - (t (1) * T2 (1) \bmod 10 + t(2) *T2 (2) \bmod 10 + t(3)*T2(3) \bmod 10) \bmod 10;$

9. Escribir en Isetl el algoritmo realizado manualmente para el cálculo del dígito de control de su CI.

10. Usar Isetl para verificar el dígito de control de la CI 2780722-8

Módulo verificador 2987634

`t:=[2,7,8,0,7,2,2];`

`10 - (t (1) * 2 mod 10 + t(2) *9 mod 10 + t(3)*8 mod 10 + t (4) *7 mod 10 + t(5) *6 mod 10 + t(6)*3 mod 10 + t (7) * 4 mod 10) mod 10;`

11. Definir la función que permite encontrar el dígito de control de una CI uruguaya.

Matemática	Isetl
$A = \{a: a \in N \text{ y } 0 \leq a \leq 9\}$ Digcon: $A \rightarrow A$ $\text{Digcon}(t) = 10 - (t(1) * 2 \bmod 10 + t(2) * 9 \bmod 10 + t(3) * 8 \bmod 10 + t(4) * 7 \bmod 10 + t(5) * 6 \bmod 10 + t(6) * 3 \bmod 10 + t(7) * 4 \bmod 10) \bmod 10$	$A := \{a: a \in N \text{ and } 0 \leq a \leq 9\}$ Digcon: $A \rightarrow A$ $\text{Digcon} := \text{func}(t);$ $> \text{if is_tuple}(t) \text{then}$ $>> \text{if } \#(t) = 7 \text{ then}$ $>> \text{if } t(i) \in \{0..9\} \text{ then}$ $>> \text{return } 10 - (t(1) * 2 \bmod 10 + t(2) * 9 \bmod 10 + t(3) * 8 \bmod 10 + t(4) * 7 \bmod 10 + t(5) * 6 \bmod 10 + t(6) * 3 \bmod 10 + t(7) * 4 \bmod 10) \bmod 10;$ $>> \text{end};$ $>> \text{end};$ $>> \text{end};$ $>> \text{end};$

12. La CI **1 913 577- 9** fue trasmisita **1 914 577 - 9**

La CI **2 780 722 -3** fue trasmisita **2 730 722 – 3**

¿En qué consiste el error? ¿Se puede detectar siempre? En caso negativo intentar una explicación.

El error consiste en cambiar una cifra por otra, en el primer caso, 4 por 3 y en el segundo caso 3 por 8. En el primer caso, después de realizados los productos módulo 10, para el número original se obtiene su suma igual a 1 y el opuesto es 9, así que está correcto. Pero en el número trasmisido la suma de los productos es 8 y el opuesto es 2, así que no es correcto: se ha detectado el error.

En el segundo caso, para el número original, la suma de los productos módulo 10 es 7 y su opuesto es 3 que se corresponde con el dígito de control. En el número trasmisido se obtienen los mismos valores: no se ha detectado el error.

Se pueden plantear casos similares para que los estudiantes establezcan alguna regularidad entre las cifras intercambiadas. Cuando la diferencia entre las mismas es 5 y están ubicadas en un lugar impar, o sea que se multiplica por una cifra par, la clase residual es la misma porque 2 y 5 son los factores primos de 10 y en la multiplicación módulo 10 generan ceros.

*Ejemplo: en N $2 * 3 = 6$; $2 * 8 = 16$; $2 * 8 = 2 * (3 + 5) = 2 * 3 + 2 * 5 = 6 + 10$*

*$4 * 3 = 12$; $4 * 8 = 32$; $4 * 8 = 4 * (3 + 5) = 4 * 3 + 4 * 5 = 12 + 20$*

Pero todos los múltiplos de 10 $\equiv_{10} 0$

A efectos de prever confusiones en los alumnos, creo pertinente observar que si $2^*5 = 0 \bmod 10$, entonces \exists un natural $n \neq 0 / 2^* n = 0$; diferente a lo que sucede en el conjunto de los naturales con que se trabaja tradicionalmente.

13. La permuta de dos dígitos consecutivos se llama “trabucazo” ¿se puede detectar siempre? ¿qué explicación se encuentra?

La CI **2 780 722 -3** fue trasmisida **2 870 722 -3**

Probar con la CI personal y después comunicarlo al grupo.

2	7	8	0	7	2	2	-	3
2	9	8	7	6	3	4		
4+	3+	4+	0+	2+	6+	8=	7	10- 7

2	8	7	0	7	2	2	-	3
2	9	8	7	6	3	4		
4+	2+	6+	0+	2+	6+	8=	8	10- 8

El hecho de mostrar que en todos los casos probados (tantos como alumnos haya en el grupo) se puede detectar el trabucazo, alienta la conjetura en dicho aspecto. En caso que no se detectara habría que buscar la explicación, pero en general observarán que la suma es siempre distinta, que las cifras de las CI son las mismas solo que en diferente lugar y en cada lugar siempre es diferente la cifra del módulo verificador. Representamos cualquier CI como $a_7 a_6 a_5 a_4 a_3 a_2 a_1 - a_0$ y la “trabucada” como $a_7 a_5 a_6 a_4 a_3 a_2 a_1 - a_0$

Aplicamos el módulo verificador ($2 9 8 7 6 3 4$) en cada una y restamos miembro a miembro las igualdades, suponiendo que si no se detecta el error, el dígito de control es el mismo.

$$2a_7 + 9a_6 + 8a_5 + 7a_4 + 6a_3 + 3a_2 + 4a_1 - a_0 = 0$$

$$2a_7 + 9a_5 + 8a_6 + 7a_4 + 6a_3 + 3a_2 + 4a_1 - a_0 = 0$$

$$9a_6 - 9a_5 + 8a_5 - 8a_6 = 0$$

$a_6 - a_5 = 0$ lo cual solo es posible si ambos dígitos (a_6 y a_5) son iguales, en cuyo caso la permuta no afecta el número de CI.

Si los dígitos permutados son diferentes, se detecta que el dígito de control es incorrecto pues no verifica la igualdad.

14. Construir una [tabla](#) con todos los valores posibles, resultantes del producto por el módulo verificador, para cualquier CI e implementar el algoritmo¹ en Isetl.

Dígito verificador	2	9	8	7	6	3	4
Dígitos CI	Productos mod 10						
1	2	9	8	7	6	3	4
2	4	8	6	4	2	6	8
3	6	7	4	1	8	9	2
4	8	6	2	8	4	2	6
5	0	5	0	5	0	5	0
6	2	4	8	2	6	8	4
7	4	3	6	9	2	1	8
8	6	2	4	6	8	4	2
9	8	1	2	3	4	7	6
0	0	0	0	0	0	0	0

La tabla permite otra mirada sobre las propiedades del dígito de control, sus posibilidades y limitaciones:

- Los números que son el producto de dos dígitos y pertenecen a la misma clase residual no permiten descubrir el cambio de cifras.
- No pueden detectarse los cambios de 0 por 5, 1 por 6, 2 por 7, 3 por 8, 4 por 9. (observar que la diferencia entre ellos siempre es 5, factor de 10, que es el módulo en que trabajamos, y 5 por un número par pertenece a la misma clase que 10).
- En esos casos los dígitos ocupan un lugar impar (pero las cifras del código verificador son pares).
- El producto módulo 10 de cualquier dígito por cada uno de los consecutivos siempre es diferente, lo cual permite detectar siempre un “trabucazo”.

c= [2, 9, 8, 7, 6, 3, 4]

m10= {x/ x ∈ N y 0 ≤ x ≤ 9}

Producto: c → m10

t:=[1..9];

> c:=[2,9,8,7,6,3,4];

> producto:=func(i);

¹ Este algoritmo se expresa en la función producto que devuelve la columna de posibilidades para cada dígito de la CI. Para la tabla completa se necesita un proceso recursivo, que se introducirá posteriormente.

```

>> if is_tuple(t)then
>> if is_tuple(c) then
>> if i in c then
>> return [t(1)*i mod 10, t(2)*i mod 10,t(3)*i mod 10,t(4)*i mod 10, t(5)*i mod
10,t(6)*i mod 10,t(7)*i mod 10, t(8)*i mod 10,t(9)*i mod 10];
>> end;
>> end;
>> end;
>> end;
> producto(2);
[2, 4, 6, 8, 0, 2, 4, 6, 8];

```

Se evalúa la función para cada uno de los dígitos del módulo verificador, en relación a la CI seleccionada, y se van completando cada una de las columnas de la tabla.

Clases residuales módulo p primo

En la aritmética módulo 10 es fácil calcular porque se siguen los procedimientos comunes del Sistema de Numeración Decimal, pero existen divisores no triviales de cero ($a \mid b$ si $b * n = a$; $0 \mid 5_{10}$ porque $5_{10} * 2 = 0_{10}$) lo cual explica la posibilidad de introducir errores que los códigos no pueden detectar. Por eso, existen códigos módulo un número primo donde esto no es posible.

Definimos **número primo** al número natural que solo admite dos divisores distintos (el mismo número y la unidad).

Matemática	Isetl
$\text{esprimo: } N \rightarrow N$ $\text{esprimo}(x) = x / x \in N; x > 1;$ $\text{divisor}(x) = \{1, x\}$	$\text{is_prime: } N \rightarrow \text{Bool}$ $\text{is_prime} := \text{func}(x);$ $\text{is_prime} := \text{func}(x);$ $\text{if is_nat}(x) \text{ then}$ $\text{return } \{y : y \in [1..x] \mid x \text{ mod } y = 0\} = \{1, x\};$ $\text{end};$ $\text{end};$ $\text{is_prime}(7);$ $\text{true};$ $\text{is_prime}(8);$ $\text{false};$



Los códigos de barra de los artículos de consumo corriente admiten su lectura con

un escáner: el estándar de decodificación más corriente en los comercios de Uruguay es conocido con el nombre de **EAN-13**.

Está formado por 13 dígitos entre 0 y 9, que llamaremos a_i ($1 \leq i \leq 13$).

4	0	0	5	4	0	1	5	4	8	0	7	2
a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}
Identificación del fabricante					Referencia del producto					verificador		

El dígito 13 se calcula

$(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + a_{13}) + 3^*$	$(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) = 0 \bmod 10$
$(4+ 0+ 4+ 1+ 4+ 0+ a_{13}) + 3^*$	$(0+ 5+ 0+ 5+ 8 + 7) = 0 \bmod 10$

$$3 + a_{13} + 3^* 5 = 0 \rightarrow a_{13} + 8 = 0 \bmod 10 \rightarrow a_{13} = 2 \text{ correcto}$$

1. Implementar en Matemática y en Isetl una función que permita verificar la corrección de un código de barras. Probarla con el código ya verificado manualmente y después con otros códigos que encuentre en los artículos de consumo diario.

Matemática	Isetl
$m10 = \{x / x \in \mathbb{N} \text{ y } 0 \leq x \leq 9\}$ $t = [i / i \in m10 \text{ y } \# t = 13]$ $\text{ean: } t \rightarrow m10$ $\text{ean (t) = } (t(1)+t(3)+t(5)+t(7)+t(9)+t(11)+t(13)+3^*(t(2)+t(4)+t(6)+t(8)+t(10)+t(12))) \equiv_{10} 0$	<pre> ean: t → Bool > ean:=func(t); >> if is_tuple (t)then >> if #(t)= 13 then >> if t(i) in { 0..9} then >> return (t(1)+t(3)+t(5)+t(7)+t(9)+t(11)+t(13)+ 3 *(t(2)+t(4)+t(6)+t(8)+t(10)+t(12)))mod 10 = 0; >> end; >> end; >> end; >>end; > t:=[4,0,0,5,4,0,1,5,4,8,0,7,2]; > ean(t); true; </pre>

2. Modificar la función para que devuelva el dígito de control

Matemática	Isetl
$\text{Ean13: } t \rightarrow \text{conjunto de las clases residuales mód } 10$ $\text{Ean13: } t \rightarrow \{ x / x = \text{resto de } n: 10; x, n \in \mathbb{N} \}$ $\text{ean (t) = } 10 - (t(1)+ t(3) +t(5) +t(7) +t(9) +t(11) + 3^*(t(2)+ t(4)+ t(6)+ t(8)+ t(10)+ t(12))) \bmod 10;$	$\text{Ean13: } t \rightarrow \{ x n \bmod 10 = x \}$ <pre> > ean13:=func(t); >> if is_tuple (t)then >> if #(t)= 13 then >> return 10 - (t(1)+t(3)+t(5)+t(7)+t(9)+t(11)+ 3 *(t(2)+t(4)+t(6)+t(8)+t(10)+t(12)))mod 10; >> end; </pre>

t(10)+ t(12))mod 10

>> end;

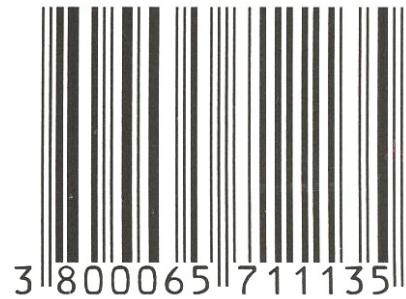
>> end;

>

> t:=[4,0,0,5,4,0,0,1,5,4,8,0,7,2];
> ean13(t);
2;

3. Observar que el dígito desconocido puede ser otro y para recuperarlo el algoritmo es similar. Se exemplifica con un caso particular y se pide una justificación matemática.

3	8	0	0	0	6	5	7	1	1	1	3	5	
3+0+0+5+1+1+5 + 3* (8+0+6+7+1+3) = 0													
2 + 3 x = 0 ; 3x = -2 = 8 ; 2 + 4 = 6													



$$(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + a_{13}) + 3(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) = 0 \pmod{10}$$



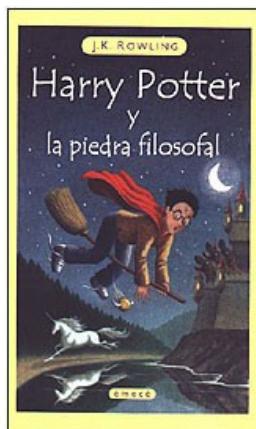
$$\text{pierdo} \rightarrow (a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + a_{13}) + 3(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) = 0$$

$$x_5 = - (a_1 + a_3 + a_7 + a_9 + a_{11} + a_{13}) - 3(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12})$$

$$\underbrace{a_1 + a_3 + a_7 + a_9 + a_{11} + a_{13}}_n - \underbrace{3(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12})}_n$$

$$x_5 = n - 3 \cdot n' \text{ (conocidos, aun cuando } n \text{ y } n' \text{ sean 0)}$$

Si fuera de lugar par, $3x = -n - n'$; $x_i = (-n - n') : 3$ (para evitar racionales, trabajo con un representante de la misma clase tal que el dividendo sea mayor que el divisor).



Temas: LITERATURA INFANTIL Y JUVENIL

Autor: ROWLING, J. K.

Editorial: SALAMANDRA

ISBN: 84-7888-611-7

254 páginas

Peso estimado: 335 gramos

El ISBN (INTERNATIONAL STANDARD BOOK NUMBER) identifica los libros modernos: las nueve primeras cifras dan información sobre el libro (editorial, título, edición, etc) y la última es un carácter de control que se calcula:

$$a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 = a_{10} \pmod{11}$$

Cada término a_i / $1 \leq i \leq 10$; 10 se representa con el símbolo romano X.

Este es el cálculo para el libro de Harry Potter.

El ISBN permite detectar todos los

8	4	7	8	8	8	6	1	1		7
1	2	3	4	5	6	7	8	9	*	
8+	8+	10+	10+	7+	4+	9+	8+	9	=	7mod 11

errores en una cifra, puede recuperar un número cualquiera que se haya borrado y el intercambio de dos cifras cualesquiera.

1. El ISBN **987-1007-54- X** corresponde al libro de Celso Antúnez “¿Cómo desarrollar contenidos aplicando las inteligencias múltiples? Calcular el dígito de control.
2. Instrumentarlo en Isetl y generalizar para cualquier libro que utilice el mismo código.
3. Justificar matemáticamente que se puede detectar el intercambio de dos cifras cualesquiera.

A:={1, 2 , 3 , 4 , 5, 6, 7 ,8, 9, X};

libro: A → conjunto de las clases residuales mód 11

libro: A → { x | n mod 11 = x }

```
> libro:=func(t);
>>if is_tuple (t)then
>>if #(t)=9 then
>>return (t(1)+ 2*t(2)+3*t(3)+4*t(4)+5*t(5)+6*t(6)+7*t(7)+8*t(8)+9*t(9))mod 11;
>>end;
```

```
>>end;
>>end;
>
>t:=[9,8,7,1,0,0,7,5,4];
>libro(t);
10;
```

Si se intercambian dos cifras, el dígito de control cambia.

$$a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 = d$$

$$a_1 + 2a_2 + 3a_4 + 4a_3 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 = d'$$

Por absurdo, supongo que $d = d'$

Resto miembro a miembro

$$a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 = -d$$

$$a_1 + 2a_2 + 3a_4 + 4a_3 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 = -d'$$

$$3a_3 - 3a_4 + 4a_4 - 4a_3 = 0$$

$3(a_3 - a_4) = 4(a_3 - a_4)$ propiedad cancelativa

$3 = 4$ absurdo

Para cualquier término: $i(a_p - a_q) = j(a_q - a_p)$

$i \neq j$ por el código

Como el módulo es 11 no se generan ceros más que con los múltiplos de 11.

REFERENCIAS BIBLIOGRÁFICAS

- ❖ Chamorro, M^a Carmen "Didáctica de las Matemáticas" (2003) Pearson, Madrid
- ❖ Chevallard (1991) "La Trasposición Didáctica. Del Saber Sabio al Saber enseñado" Bs As Aique
- ❖ da Rosa, Sylvia La Matemática Discreta como formación básica Instituto de Computación, Facultad de Ingeniería, Universidad de la República, Montevideo, Uruguay
- ❖ Duffour, Gustavo- Matemática de quinto- Ediciones Matemática 2000- Canelones. Uruguay - 2004
- ❖ Gil, Omar y Fernández, Pablo -Una introducción a los códigos detectores y correctores de errores. <http://www.fing.edu.uy/~omargil/educmate/codyal31-71.pdf>
- ❖ <http://www.fing.edu.uy/~darosa/curso.html>
- ❖ <http://www.fing.edu.uy/~darosa/Manual.rtf>
- ❖ <http://www.fing.edu.uy/~darosa/MatProg.doc>
- ❖ Lachaud, Gilles y Vladut, Serge – los códigos correctores de errores Mundo científico nº 161
- ❖ Tapia, Nelly y otros – Matemática 1 Estrada BsAs 1993
- ❖ Vergnaud Gérard LA TEORÍA DE LOS CAMPOS CONCEPTUALES *Recherches en Didáctique des Mathématiques*, Vol. 10, Nº 2, 3, pp. 133-170, 1990.

PROYECCIÓN DE LA PROPUESTA

El tema de los códigos detectores y correctores de errores permite abordar otros contenidos de Matemática, algunos incluidos en el curso de Formación Inicial de Maestros y otros no. En cualquier caso, pensar su implementación en ISETL constituye un desafío para quienes lo tenemos a cargo. En este caso, se pueden mostrar otras potencialidades y limitaciones de los sistemas de codificación, pero su justificación implica conocimientos de matemática y de programación más avanzados. Por ejemplo, en el ejercicio 14 se pide construir la [tabla](#) de la página 23 e implementarla con Isetl, pero el algoritmo realizado solo permite obtener los valores para cada columna: obtener la tabla completa implica operar con las listas y un procedimiento recursivo.

Una codificación eficaz tiene que hacer intervenir relaciones entre los símbolos transmitidos, que al asimilarse a números enteros permite utilizar todos los recursos de la aritmética, el álgebra y el análisis. Un código, en términos matemáticos, necesita un alfabeto finito y cada palabra es una secuencia de símbolos. El más sencillo es el sistema binario utilizado por la tecnología informática, donde cambiar un cero por un uno es la única posibilidad de error, pero puede resultar catastrófica para la interpretación del mensaje. La estrategia que emplean los códigos detectores y correctores de errores es agregar a cada palabra cierta cantidad de símbolos de control. A cada palabra de k símbolos le hace corresponder otra palabra de n símbolos, donde n es un entero mayor que k . En los códigos lineales, la transformación que a cada palabra de k caracteres (que llamaremos μ) le hace corresponder una palabra de n caracteres (que llamaremos μ'), se puede escribir $\mu' = \mu G$ donde G es la matriz compuesta por tantas filas y columnas como símbolos tengan las respectivas palabras.

La codificación en el sistema binario puede iniciarse en este curso como un juego de decodificación de mensajes sencillos, con el propósito de favorecer la comprensión de los sistemas de numeración posicionales independientemente de la base y pasar de uno a otro mediante el Algoritmo de Euclides y la recurrencia, con lo que se puede planificar otra secuencia de trabajo posterior a esta. En cambio la aplicación de las matrices corresponde a otros cursos.

EVALUACIÓN DEL CURSO

La inscripción a este curso estuvo motivada por contemplar dos áreas en las que realicé mi formación y mi enseñanza y de las que resulta una necesaria complementariedad, no siempre evidente, teniendo en cuenta los supuestos didácticos de su enseñanza.

La lectura de los materiales, previo a la primera instancia presencial, me mostró una relación entre la matemática y la informática que me recordó mis primeras experiencias en esta área, cuando abrieron los primeros institutos en el interior y que, sin lugar a dudas, no

tiene nada que ver con lo que se enseña hoy: un operador PC no tiene idea del funcionamiento de la computadora ni de los algoritmos implicados ni de su relación con la matemática.

A pesar de que sigue siendo común la idea de que la Matemática y la Informática son accesibles solo a las personas “inteligentes”, evidentemente con el concepto tradicional del término, y auto marginándose de dichas ciencias. Afortunadamente, los niños de nuestra generación ya son parte de la cultura informática pero los docentes, en general han quedado fuera, con lo que se restringe el uso educativo de la misma y en caso de usar la computadora es considerada solo un recurso, no un mediador ni un habilitador de procesos de desarrollo cognitivo.

Por motivos laborales no pude concurrir a la primera instancia presencial, de modo que aunque traté de seguir las instrucciones del manual no pude hacer nada en “máquina” por un detalle aparentemente pequeño: para evaluar hay que “pintar” la expresión (no Enter).

En la segunda presencial seguí con interés las explicaciones de nuestra profesora con un nivel de comprensión aceptable, aunque las intervenciones de los compañeros me dejaban fuera del contexto procedimental con que ellos ya estaban familiarizados. Mis primeras experiencias en máquina fueron bastante frustrantes porque detalles aparentemente mínimos como la falta de un “punto y coma” impedían a la computadora realizar algo tan simple como una suma y yo no entendía su respuesta por estar escrita en inglés, idioma que no conozco pero que, además me produce cierto bloqueo porque mi contacto con él suele reducirse a procedimientos sin los resultados esperados.

Con la ayuda de algún compañero y las correcciones de Sylvia comencé a entender un poco más de todo esto y mis primeros logros motivaron seguir en el intento.

He dedicado muchísimas horas para programar algoritmos sencillos y he aprendido algunos aspectos de computación relacionados con el contenido matemático seleccionado para esta propuesta. Pero queda el camino de estrategias abierto para continuar con otros aprendizajes que fueron tratados en este curso.

Creo, sin embargo, que lo más importante es haber resignificado el concepto y la importancia de los números Naturales y haber integrado la Matemática Discreta en aspectos relevantes de contenidos curriculares. Explicitar el paralelismo entre los códigos matemático e informático hizo necesario el análisis de propiedades en las que suele no profundizarse, porque, tradicionalmente los Naturales son considerados los números “para contar” que se enseñan en los primeros grados como objetos simples. La comunicación de la propuesta al grupo implica sintetizar los aspectos relevantes en función del eje estructurador de la misma y seleccionar ejemplos adecuados, con lo cual se habilita una nueva mirada sobre nuestro trabajo, que se verá potenciado con la devolución por parte de Sylvia y los aportes de los compañeros.