MATEMÁTICAS PARA LA TOMA DE DECISIONES

Antonio M. Oller-Marcén
oller@unizar.es
Departamento de Matemáticas-IUMA, Universidad de Zaragoza

CP Juan de Lanuza
24 y 30 de mayo de 2023

Centro de PROFESORADO
JUAN DE LANUZA

Plan de formación del profesorado 2022-23

VUESTROS OBJETIVOS PARA EL TALLER

MIS OBJETIVOS PARA EL TALLER

1. Presentar y motivar la existencia de la asignatura.

2. Compartir algunas sugerencias metodológicas generales.

3. Presentar una pequeña bibliografía introductoria.

4. Hacer una pequeña revisión de los saberes básicos de cada uno de los bloques de la asignatura.

5. Trabajar sobre algunos ejemplos que puedan servir como punto de partida para el diseño de situaciones de aprendizaje.

MOTIVACIÓN

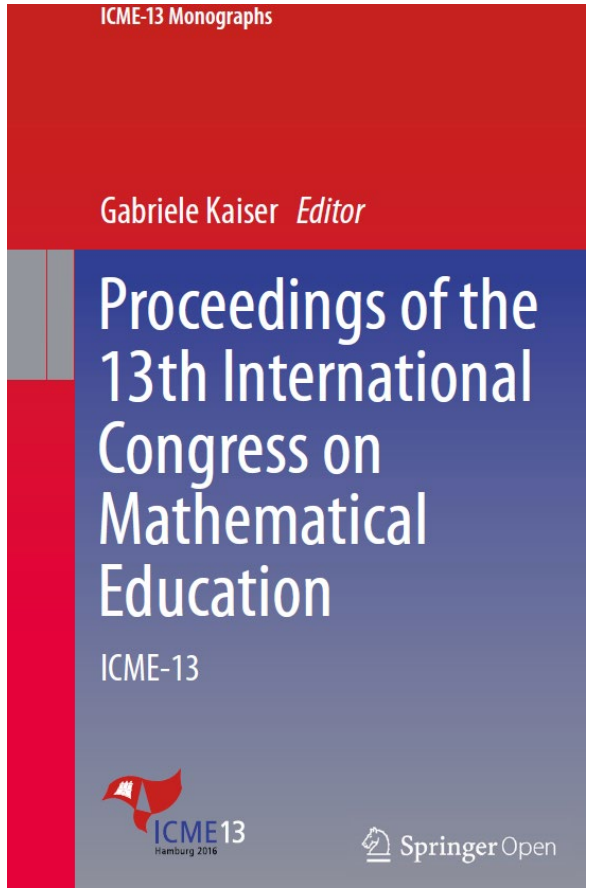
- Papel de la tecnología en la sociedad actual.
  big data, *machine learning*, IA, papel de los algoritmos en redes sociales…
- Los ciudadanos no deberían ser meros usuarios pasivos.
- Modelización, matemática discreta, pensamiento algorítmico y computacional, etc.
- El currículo obligatorio debería evolucionar y proporcionar herramientas actualizadas.
- Entre tanto, una optativa (2 periodos lectivos semanales, unas 35 semanas).

MOTIVACIÓN

"La matemática discreta es una rama relativamente joven de las matemáticas […] Es un campo con aplicaciones a una variedad de situaciones del mundo real, y como tal adquiere creciente importancia en la sociedad contemporánea".

"Consideramos que la matemática discreta incluye […] temas, como la lógica, **teoría de juegos**, **algoritmos**, **teoría de grafos**, geometría discreta, **teoría de números**, sistemas dinámicos discretos, problemas de división justa, criptografía, teoría de la codificación y recuento".

"La matemática discreta no siempre está claramente delimitada en los planes de estudios y puede aparecer de forma borrosa".



Topic Study Group No. 17: Teaching and Learning of Discrete Mathematics

Eric W. Hart, James Sandefur, Cecile O. Buffet, Hans-Wolfgang Henn and Ahmed Semri

LA ASIGNATURA: COMPETENCIAS

CE.MTD.1. Reconocer la importancia de la **aritmética modular** en un contexto tecnológico y digital, comprendiendo la necesidad y los fundamentos básicos de algoritmos de codificación sencillos y siendo capaz de aplicarlos de forma efectiva en situaciones concretas.

CE.MTD.2. Identificar la utilidad de la **teoría de grafos** para modelizar situaciones y problemas reales de la vida cotidiana y de materias del ámbito científico y tecnológico, empleándola para explorar distintas formas de proceder y para obtener y comunicar posibles soluciones.

CE.MTD.3. Utilizar la **teoría de juegos** para modelizar situaciones y problemas reales de la vida cotidiana y de materias del ámbito de las ciencias sociales y de la economía, reconociendo su aplicación a la toma de decisiones y obteniendo y expresando soluciones posibles en situaciones diversas.

LA ASIGNATURA: COMPETENCIAS

CE.MTD.4. Emplear herramientas de cálculo simbólico u otras herramientas digitales para representar resultados y procedimientos, explorar, conjeturar y comprobar propiedades, y resolver problemas, desarrollando e implementando **algoritmos matemáticos sencillos**.

LA ASIGNATURA: SABERES BÁSICOS

A. Aritmética modular y criptografía.

   Tratamiento moderno de la aritmética para llegar a la aritmética modular. Algoritmo RSA como ejemplo de cifrado basado en elementos puramente matemáticos.

B. Teoría de grafos.

   Nociones básicas de teoría de grafos para modelizar situaciones reales y resolver problemas asociados.

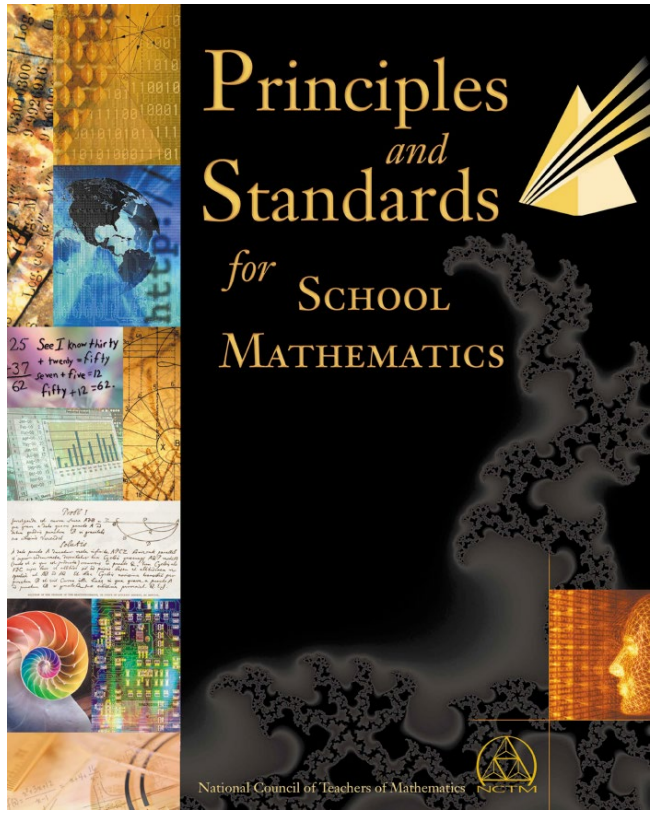
C. Teoría de juegos.

   Nociones básicas de teoría de juegos que permitan al alumnado modelizar y analizar situaciones reales vinculadas a la toma de decisiones.

SUGERENCIAS METODOLÓGICAS GENERALES

Enseñar matemáticas a través de **contenidos** y **procesos** (NCTM, 2000):

- Resolución de problemas [CE.M.1, CE.M.2].
- Razonamiento y prueba [CE.M.3, CE.M.4].
- Comunicación [CE.M.8].
- Conexiones [CE.M.5, CE.M.6].
- Representación [CE.M.7].



En español (SAEM Thales)

Los saberes abordados en esta asignatura permiten trabajar "naturalmente" todos estos procesos (competencias).

SUGERENCIAS METODOLÓGICAS GENERALES

[…] se recomienda un enfoque de enseñanza de las matemáticas a través de la **resolución de problemas**, […] se recomienda que los distintos contenidos abordados se presenten a partir de situaciones introductorias en las que el propio trabajo del alumnado proporcione los elementos para una posterior institucionalización […]

[…] debe fomentarse la redacción de informes y la presentación de los mismos tanto en forma escrita como oral y utilizando diversidad de medios y formatos. **Comunicar** resultados de investigación es una labor crucial […]

[…] debe hacerse un énfasis especial es en la necesidad de argumentar, justificar y explicitar los **razonamientos** realizados […] desde el uso de ejemplos y contraejemplos, hasta las **pruebas** preformales o incluso las demostraciones

SUGERENCIAS METODOLÓGICAS GENERALES

Para el trabajo “a través de” la resolución de problemas se pueden buscar situaciones motivadoras o introductorias (situaciones de aprendizaje) con distintos tipos de contextos:

- Problemas provenientes de la “realidad”.
- Problemas provenientes de situaciones “lúdicas”.
- Problemas de carácter matemático (sin un contexto concreto).
- Problemas planteados a partir de textos “históricos”.
- Etc.

Conviene presentar situaciones en todo tipo de contextos.

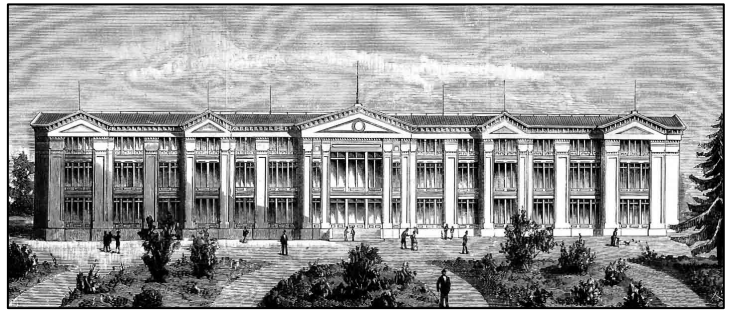
SUGERENCIAS METODOLÓGICAS GENERALES

Presencia de los procesos en los criterios de evaluación (algunos ejemplos):

Resolución de problemas	1.4. Resolver de forma constructiva sistemas de congruencias lineales con una incógnita, estudiando previamente la existencia de solución.
Razonamiento y prueba	2.4. Proporcionar argumentos y/o contraejemplos acerca de la existencia, o no, de ciertos tipos de grafos y respecto al cumplimiento, o no, de determinadas propiedades.
Comunicación	3.6. Expresar y comunicar los resultados de la resolución de un juego (ganancias, pérdidas, estrategias ganadores, etc.) en los términos del contexto concreto en que se está trabajando.
Conexiones	2.5. Utilizar grafos para modelizar matemáticamente situaciones de la vida cotidiana, la ciencia y la tecnología.
Representación	3.2. Utilizar la forma de representación apropiada para modelizar un juego o una situación determinada.

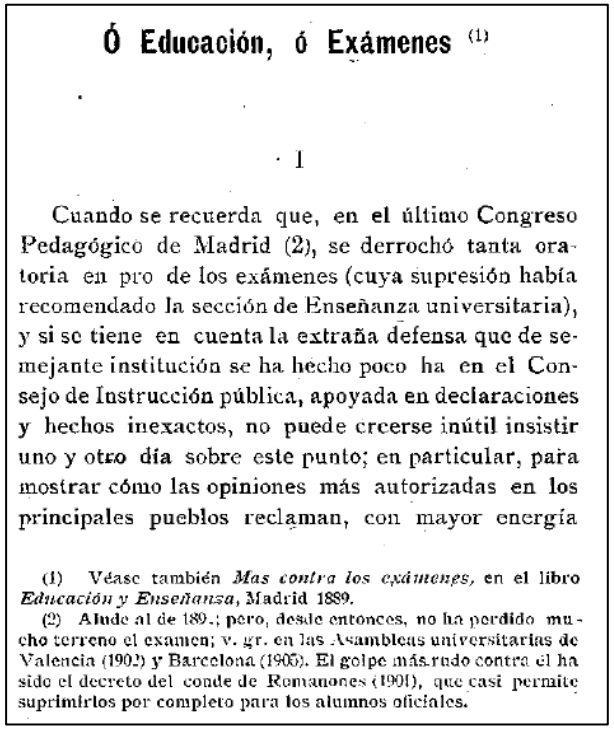
SUGERENCIAS METODOLÓGICAS GENERALES

Evitar el uso del examen.



Existen otros instrumentos de evaluación:

- ✓ Portafolios individuales.
- ✓ Mapas conceptuales.
- ✓ Proyectos de trabajo en grupo.
- ✓ Observación del docente.
- ✓ ...



Ó Educación, ó Exámenes (1)

I

Cuando se recuerda que, en el último Congreso Pedagógico de Madrid (2), se derrochó tanta oratoria en pro de los exámenes (cuya supresión había recomendado la sección de Enseñanza universitaria), y si se tiene en cuenta la extraña defensa que de semejante institución se ha hecho poco ha en el Consejo de Instrucción pública, apoyada en declaraciones y hechos inexactos, no puede creerse inútil insistir uno y otro día sobre este punto; en particular, para mostrar cómo las opiniones más autorizadas en los principales pueblos reclaman, con mayor energía

(1) Véase también *Mas contra los exámenes*, en el libro *Educación y Enseñanza*, Madrid 1889.

(2) Alude al de 189.; pero, desde entonces, no ha perdido mucho terreno el examen; v. gr. en las Asambleas universitarias de Valencia (1902) y Barcelona (1905). El golpe más rudo contra el ha sido el decreto del conde de Romanones (1901), que casi permite suprimirlos por completo para los alumnos oficiales.

BIBLIOGRAFÍA SUCINTA

Libros sobre el contenido matemático

Tattersall, J.J. (1999). *Elementary number theory in nine chapters*. Cambridge University Press.

Trudeau, R.J. (1976). *Dots and lines*. The Kent State University Press.

Prisner, E. (2014). *Game theory through examples*. The Mathematical Association of America.

BIBLIOGRAFÍA SUCINTA

Libros sobre enseñanza-aprendizaje del contenido matemático

Coriat, M., Sancho, J.M., Gonzalvo, P., & Martín, A. (1989). *Nudos y nexos. Redes en la escuela*. Editorial Síntesis.

Hart, E.W., & Sandefur, J. (eds.) (2018). *Teaching and Learning Discrete Mathematics Worldwide: Curriculum and Research*. Springer.

Sierra, M., González, M.T., Gacía, A., & González, M. (1989). *Divisibilidad*. Editorial Síntesis.

BIBLIOGRAFÍA SUCINTA

Recursos

Hopkins, B. (ed.) (2008). *Resources for Teaching Discrete Mathematics: Classroom Projects, History Modules, and Articles*. The Mathematical Association of America.

https://demonstrations.wolfram.com/topic.html?topic=Graph+Theory&t=20
https://demonstrations.wolfram.com/topic.html?topic=Prime+Numbers&limit=20

https://www.geogebra.org/search/teor%C3%ADa%20de%20grafos
https://www.geogebra.org/m/A5MvDFuC

https://www.jasondavies.com/planarity/

BLOQUE A. CONCRECIÓN DE SABERES

A. Aritmética modular y criptografía.

A1. Aritmética en Z.

A2. Aritmética modular.

A3. El conjunto Z/mZ.

A4. Criptografía.

BLOQUE A. CONCRECIÓN DE SABERES

A1. Aritmética en *Z*.

- ✓ $a|b$ si y solo si existe c tal que $b = ac$. División con resto $a = bq + r$.
  Resolución en Z de $ax = b$.
- ✓ Definición de primo: p es primo si $p|ab$ implica que $p|a$ o $p|b$.
  Teorema fundamental de la aritmética: $n = p_1^{e_1}p_2^{e_2}p_r^{e_r}$.
- ✓ Definición "literal" de mcd y mcm.
  $\text{mcm}(a,b) = ab/\text{mcd}(a,b)$.
- ✓ Algoritmo de Euclides para calcular el mcd.
  Identidad de Bezout: $ax + by = \text{mcd}(a,b)$.
  Resolución en Z de $ax + by = c$.

BLOQUE A. CONCRECIÓN DE SABERES

A2. Aritmética modular.

- ✓ $a \equiv b \pmod{m}$ si y solo si $m \mid a - b$ o bien $a = b + km$.
  a y b son inversos módulo m si $ab \equiv 1 \pmod{m}$.
  a tiene inverso módulo m si y solo si $\mathrm{mcd}(a,m)=1$.
  Uso de la identidad de Bezout para calcular inversos.

- ✓ $ax \equiv b \pmod{m}$ tiene solución si y solo si $\mathrm{mcd}(a,m) \mid b$.
  $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ tiene solución si y solo si $\mathrm{mcd}(m,n) \mid a - b$.

BLOQUE A. CONCRECIÓN DE SABERES

A3. El conjunto Z/mZ.

- ✓ Aritmética en el conjunto $\{0, 1, \ldots, m\text{-}1\}$.
  Tablas de sumar y de multiplicar.
- ✓ a es una unidad en Z/mZ si y solo si tiene inverso.
  a no nulo es divisor de 0 en Z/mZ si y solo si existe b no nulo tal que $ab = 0$.
  $\phi(m)$ es el número de unidades de Z/mZ.
- ✓ Si a es una unidad, $a^e = 1$ para algún $e > 0$. El orden de a es el mínimo posible.
  Pequeño Teorema de Fermat: Si p es primo $a^p \equiv a \pmod{p}$.
  Teorema de Euler: Si $\text{mcd}(a,m) = 1$, $a^{\phi(m)} \equiv 1 \pmod{m}$.

BLOQUE A. CONCRECIÓN DE SABERES

A4. Criptografía.

- ✓ Origen, necesidad, usos de la esteganografía y de la criptografía.
- ✓ Cifrados de sustitución son aquellos que se basan en sustituir los símbolos que forman el mensaje por otros símbolos siguiendo algún tipo de regla fija.
- ✓ Un cifrado simétrico usa una misma clave para codificar y decodificar, que es conocida por ambos extremos (emisor y receptor).
- ✓ En un cifrado asimétrico se utilizan claves distintas y cada extremo solo conoce una de ellas.
- ✓ El algoritmo RSA.

BLOQUE A. CONCRECIÓN DE SABERES

Algoritmo RSA.

- Receptor:
  - Elige dos primos p y q y calcula $m = pq$, $\phi(m)=(p-1)(q-1)$.
  - Elige e, coprimo con $\phi(m)$ y calcula d, el inverso de e modulo $\phi(m)$. Es decir,
$$de \equiv 1 \pmod{\phi(m)}.$$
  - Hace público m y d. Se guarda e.

- Emisor:
  - Para enviar w, calcula $w^d \equiv c \pmod{m}$ y envía c en su lugar.

- Receptor:
  - Recibe c, calcula $c^e \equiv (w^d)^e \equiv w \pmod{m}$.

BLOQUE A. UNA POSIBLE TEMPORALIZACIÓN

	Aspectos a tratar	**Sesiones**
A1	Introducción y conceptos básicos.	3
	Ecuaciones diofánticas lineales con una y dos incógnitas.	3
A2	La relación de congruencia.	3
	Resolución de (sistemas de) congruencias lineales con una incógnita.	3
A3	El conjunto Z/mZ. Unidades y divisores de cero. La función phi.	3
	Orden de un elemento. Pequeño teorema de Fermat y teorema de Euler.	3
A4	Criptografía.	5

BLOQUE A. SOFTWARE

Algunos comandos de Maxima (software libre) para teoría de números:

primep(*a*)	→	Devuelve ‘true’ o ‘false’ según si *a* es primo o no.
next_prime(*a*)	→	Devuelve el primer primo mayor que *a*.
factor(*a*)	→	Devuelve la factorización de *a* en potencias de primos
gcd(*a*,*b*)	→	Devuelve el máximo común divisor de *a* y *b*.
lcm(*a*,*b*)	→	Devuelve el mínimo común múltiplo de *a* y *b*.
gcdex(*a*,*b*)	→	Devuelve [*x*,*y*,*d*] siendo *d* el mcd(*a*,*b*) y $ax + by = d$.
mod(*a*,*b*)	→	Calcula *a* módulo *b*.
inv_mod(*a*,*b*)	→	Devuelve el inverso de *a* módulo *b*.
totient(*a*)	→	Devuelve el valor de $\phi(m)$.
power_mod(*a*,*b*,*c*)	→	Devuelve a^b módulo *c*.

BLOQUE A. EJEMPLOS PARA POSIBLES SITUACIONES DE APRENDIZAJE

Vamos a trabajar sobre cuatro documentos.

- Contexto matemático.

  Un problema matemático concreto.
- Contexto histórico.

  Un fragmento en el que se describe un método (algoritmo) sin formalizar.
- Contexto lúdico.

  Una situación concreta.
- Contexto real.

  Una imagen.

BLOQUE A. EJEMPLOS PARA POSIBLES SITUACIONES DE APRENDIZAJE

Cada uno requiere una aproximación distinta debido a su naturaleza y a su grado de (in)concreción.

- Resolver y estudiar un problema matemático.
- Analizar y comprender un texto histórico.
- Explorar el potencial de una situación o de un contexto.
- Pensar cómo utilizar un objeto o problema real.

Tratar de dar los primeros pasos hacia el diseño de una situación de aprendizaje.

- Introducción y contextualización.
- Objetivos didácticos.
- Elementos curriculares.
- Conexiones.
- Descripción de la actividad.
- Metodología y estrategias didácticas.
- Atención a las diferencias individuales.
- Recomendaciones para la evaluación formativa.

BLOQUE A. EJEMPLO CONTEXTO MATEMÁTICO

$$x^2 - y^2 = n$$

Esta ecuación tiene solución si y solo si n es impar o múltiplo de 4.

Número de soluciones (positivas):

n	Cuadrado	No cuadrado
Impar	$\frac{\tau(n)+1}{2}$	$\frac{\tau(n)}{2}$
Múltiplo de 4	$\frac{\tau(n)+1}{2} - \iota(n)$	$\frac{\tau(n)}{2} - \iota(n)$

$\tau(n)$: número de divisores de n.
$\iota(n)$: número de divisores impares de n.

BLOQUE A. EJEMPLO CONTEXTO HISTÓRICO

Dado un entero N expresado en base 10:

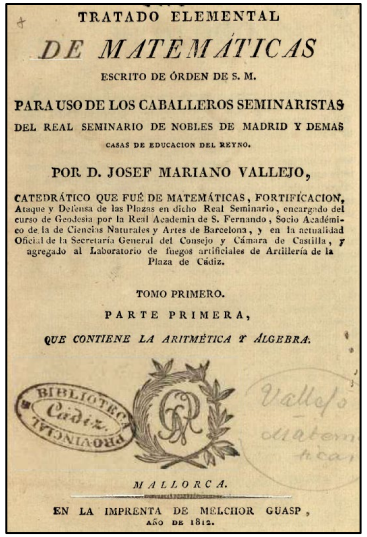
$$N = \sum_{i=0}^{k} c_i 10^i$$

Queremos saber si es divisible por un cierto entero m.

Para ello, tomamos $0 \leq e_i < m - 1$ tal que $e_i \equiv 10^i \pmod{m}$ y calculamos

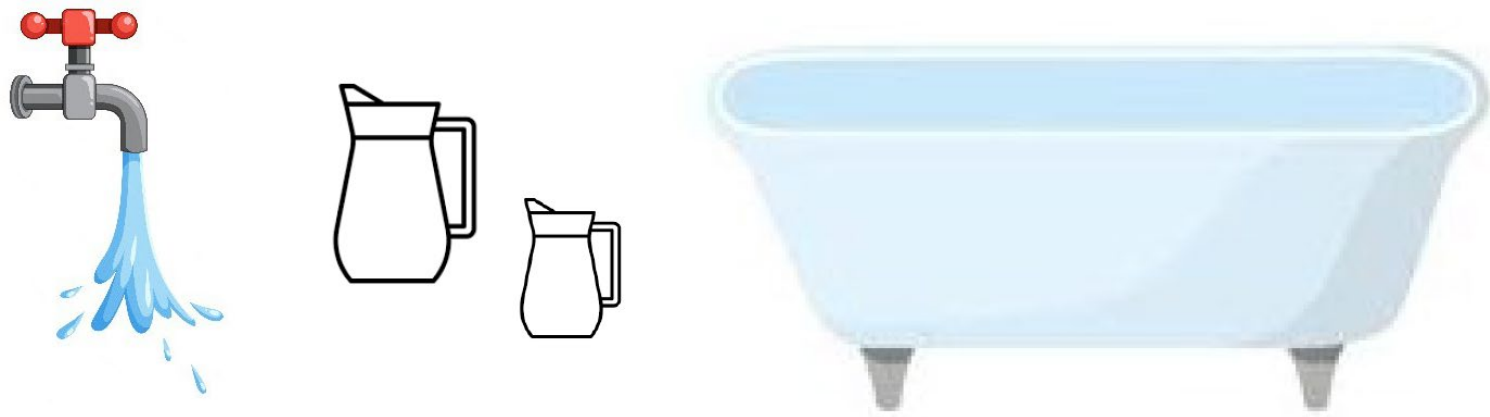
$$N' = \sum_{i=0}^{k} c_i e_i$$

Entonces, $m|N$ si y solo si $m|N'$.


TRATADO ELEMENTAL
DE MATEMÁTICAS
ESCRITO DE ÓRDEN DE S. M.
PARA USO DE LOS CABALLEROS SEMINARISTAS
DEL REAL SEMINARIO DE NOBLES DE MADRID Y DEMAS
CASAS DE EDUCACION DEL REYNO.
POR D. JOSEF MARIANO VALLEJO,
CATEDRÁTICO QUE FUÉ DE MATEMÁTICAS, FORTIFICACION, Ataque y Defensa de las Plazas en dicho Real Seminario, encargado del curso de Geodesia por la Real Academia de S. Fernando, Socio Académico de la de Ciencias Naturales y Artes de Barcelona, y en la actualidad Oficial de la Secretaría General del Consejo y Cámara de Castilla, y agregado al Laboratorio de fuegos artificiales de Artillería de la Plaza de Cádiz.
TOMO PRIMERO.
PARTE PRIMERA,
QUE CONTIENE LA ARITMÉTICA Y ÁLGEBRA.

MALLORCA.
EN LA IMPRENTA DE MELCHOR GUASP,
AÑO DE 1812.

BLOQUE A. EJEMPLO CONTEXTO LÚDICO



$$ax + by = L$$

a, b las capacidades de cada jarra.

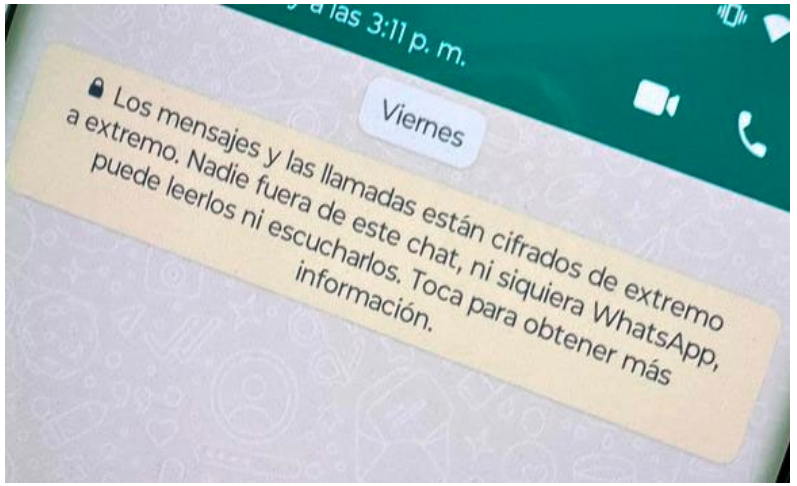
x, y las “veces” que se vierte cada jarra en la bañera.

L la cantidad de agua que se quiere tener en la bañera.

¿Cómo andamiar la actividad? Comenzar un 1 jarra, selección de a, b, L…

Una solución, todas las soluciones, soluciones positivas…

BLOQUE A. EJEMPLO CONTEXTO LÚDICO



¿Es un modo “interesante” o “útil” o “atractivo” para introducir la criptografía?

¿Qué preguntas puede suscitar?

Sobre el significado de términos: “cifrado”, “extremo a extremo”.
Sobre el procedimiento que se sigue para hacerlo.

Complementar con otros elementos:

https://youtu.be/Q8K311s7EiM