Aritmética modular y ecuaciones diofánticas con aplicaciones a las comunicaciones

Rafael Crespo García, Ramón Esteban Romero[1]

[1]Universitat de València
Estalmat Comunitat Valenciana

Encuentro Estalmat, Castro Urdiales, abril de 2025

Agradecimientos


REAL ACADEMIA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES DE ESPAÑA

ESTALMAT
COMUNITAT VALENCIANA


GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

FECYT
INNOVACIÓN


Purposeful Ventures


CIEM
Centro Internacional de Encuentros Matemáticos


EXCMO. AYUNTAMIENTO DE CASTRO URDIALES


Financiado por la Unión Europea
NextGenerationEU


GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

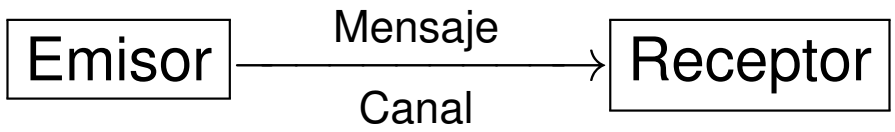

Plan de Recuperación, Transformación y Resiliencia


INSTITUTO NACIONAL DE CIBERSEGURIDAD


Universidad de Cantabria

Introducción

Motivación: el proceso de comunicación

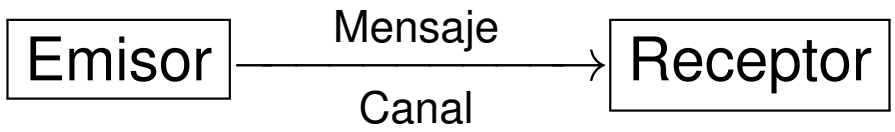


Dos problemas:

- El canal puede tener ruido y el mensaje puede llegar con errores. ¿Qué podemos hacer para minimizar el efecto de este ruido?
- El mensaje puede ser interceptado en el canal. ¿Cómo podemos ocultar el significado del mensaje para que quien lo intercepte no sea capaz de entenderlo?

Introducción

Motivación: el proceso de comunicación

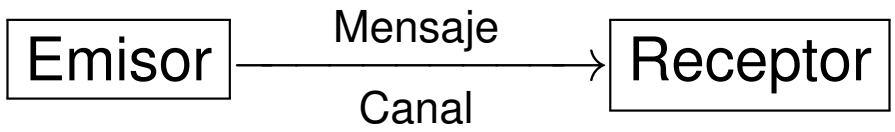


Dos problemas:

- El canal puede tener ruido y el mensaje puede llegar con errores. ¿Qué podemos hacer para minimizar el efecto de este ruido?
- El mensaje puede ser interceptado en el canal. ¿Cómo podemos ocultar el significado del mensaje para que quien lo intercepte no sea capaz de entenderlo?

Introducción

Motivación: el proceso de comunicación

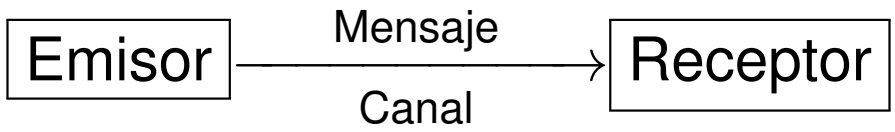


Dos problemas:

- El canal puede tener ruido y el mensaje puede llegar con errores. ¿Qué podemos hacer para minimizar el efecto de este ruido?
- El mensaje puede ser interceptado en el canal. ¿Cómo podemos ocultar el significado del mensaje para que quien lo intercepte no sea capaz de entenderlo?

Introducción

Motivación: el proceso de comunicación

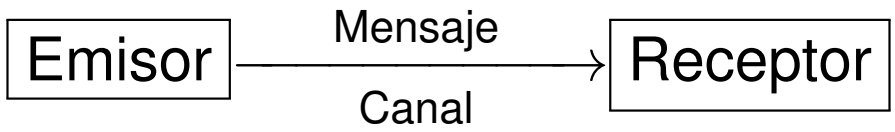


Dos problemas:

- El canal puede tener ruido y el mensaje puede llegar con errores. ¿Qué podemos hacer para minimizar el efecto de este ruido? Teoría de códigos
- El mensaje puede ser interceptado en el canal. ¿Cómo podemos ocultar el significado del mensaje para que quien lo intercepte no sea capaz de entenderlo?

Introducción

Motivación: el proceso de comunicación



Dos problemas:

- El canal puede tener ruido y el mensaje puede llegar con errores. ¿Qué podemos hacer para minimizar el efecto de este ruido? Teoría de códigos
- El mensaje puede ser interceptado en el canal. ¿Cómo podemos ocultar el significado del mensaje para que quien lo intercepte no sea capaz de entenderlo? Criptografía

Introducción

Sesiones

1. Aritmética modular: descifrando códigos secretos (segundo, Alejandro Miralles)
2. Criptografía: descubriendo mensajes ocultos (segundo, Ramón Esteban)
3. Ecuaciones diofánticas y aplicaciones (veteranos, Ramón Esteban)

Introducción

Aritmética modular y códigos

- Introducimos la aritmética modular o del reloj con ejemplos relacionados con horas, ángulos, días de la semana.
- Utilizamos códigos de repetición para introducir la noción de detección y corrección de errores.
- Analizamos códigos basados en aritmética modular, como:
  - código de paridad,
  - letra del DNI,
  - caracteres de los códigos de lectura óptica del DNI,
  - códigos GTIN-13 (códigos de barras),
  - códigos de cuentas bancarias (CCC, IBAN),

  prestando especial atención a la capacidad para detectar errores y tratando de justificar por qué los detectan.

Introducción

Criptografía

- Presentamos codificaciones por trasposición, como la escítala espartana.
- Presentamos el cifrado de César, que tratamos como un problema de aritmética modular, con ayuda de discos giratorios que ayudan a cifrar y descifrar.
- Introducimos el cifrado afín como manera de introducir más claves.
- Presentamos los cifrados de sustitución y vemos cómo el análisis de frecuencias permite descifrarlos. El alumnado tiene que interpretar unos criptokaraokes.

Introducción

Criptografía

- Presentamos los cifrados de Vigenère como manera de igualar las frecuencias de los símbolos del mensaje. Mostramos cómo las libretas de uso único son criptosistemas perfectos.
- Vemos también que un problema importante de estos sistemas clásicos es la transmisión de la clave, lo que motiva el uso de criptosistemas de clave pública.

Ecuaciones diofánticas y aplicaciones

Ecuaciones diofánticas lineales

- Problema de la tumba de Diofanto
- Ver si las ecuaciones diofánticas siguientes tienen solución:

$$\begin{aligned} 4x + \quad 3y &= 5 \\ 1234x - 5678y &= 1 \\ 13x + \quad 21y &= 2. \end{aligned}$$

  Si tienen soluciones, ¿cómo hallar más?
- Generalización: ¿qué condiciones deben cumplir los enteros a, b, c para que $ax + by = c$ tenga soluciones enteras? ¿Cómo hallarlas todas?
- Algún problema en el que pedimos soluciones enteras no negativas

Ecuaciones diofánticas y aplicaciones

Algoritmo de Euclides e identidad de Bézout

- Para encontrar las soluciones de estas ecuaciones diofánticas, tienen un papel fundamental el algoritmo de Euclides y la identidad de Bézout.
- Hacemos notar que algoritmos como RSA dependen fuertemente del hecho de que la factorización de un número como producto de primos es un problema difícil y no es práctico utilizarlo para calcular el mcd, mientras que el algoritmo de Euclides lo determina muy rápidamente.

Ecuaciones diofánticas y aplicaciones

Algoritmo de Euclides e identidad de Bézout

Diofanto

Euclides (323–383 a.C.)

Étienne Bézout (1730–1783)

Ecuaciones diofánticas y aplicaciones

Algoritmo de Euclides e identidad de Bézout

- Podríamos pensar que agencias poderosas podrían haber encontrado un método rápido para factorizar enteros y, así, romper RSA, pero si fuera así, parecería extraño que agencias como
  - `https://www.cni.es/` (España)
  - `https://www.nsa.gov/` (Estados Unidos de América)
  - `https://cyber.gouv.fr/` (Francia)
  - `https://www.mi5.gov.uk/` (Reino Unido)
  - `https://www.12339.gov.cn/` (República Popular China)

  basaran la seguridad de sus redes en RSA.

Ecuaciones diofánticas y aplicaciones

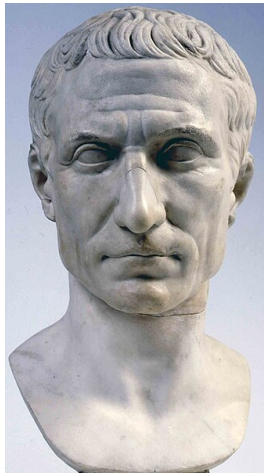
Ecuaciones en congruencias

- Los problemas de ecuaciones en congruencias lineales se pueden reducir a problemas de resolución de ecuaciones diofánticas lineales: $ax \equiv c \pmod{m}$ equivale a $ax - my = c$ para un $y \in \mathbb{Z}$.
- Se pretende que el alumnado obtenga las soluciones de una ecuación de la forma $ax \equiv b \pmod{m}$, salvo congruencia módulo m, en función de $d = \mathrm{mcd}(a, m)$ y de si $d \mid b$.
- Estos problemas permiten descifrar los cifrados afines de la forma $x \mapsto ax + b \mod m$ para $\mathrm{mcd}(a, m) = 1$, que generalizan los criptosistemas de tipo César.

Ecuaciones diofánticas y aplicaciones

Ecuaciones en congruencias

Karl Friedrich Gauß (1777–1855)



Gaius Iulius Cæsar (100–44 a.C)

Ecuaciones diofánticas y aplicaciones

El teorema chino de los restos

Problema

- *Cuando todos los miembros de una comisión fallera participan en un pasacalles y lo hacen en filas de dos, queda una persona suelta.*
- *Cuando van en filas de tres, también sobra una persona.*
- *Cuando van en filas de cinco, sobran dos personas, y*
- *cuando van en filas de siete, sobran tres personas.*

¿Qué podemos decir sobre el número de miembros de la comisión fallera?

Ecuaciones diofánticas y aplicaciones

El teorema chino de los restos

Guerreros de Xi'an

Qin Jiushao
秦九韶
(1202–1261)

Ecuaciones diofánticas y aplicaciones

El teorema chino de los restos

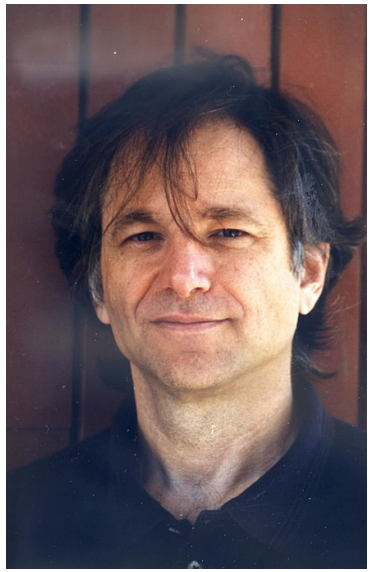
- Se usa la identidad de Bézout para resolver estos problemas de ecuaciones en congruencias cuando los módulos son primos entre sí dos a dos.
- Se analizan algunos ejemplos en los que se ve qué sucede cuando algunos módulos no son primos dos a dos: en unos casos hay soluciones; en otros, no.

Aplicaciones

Criptosistema RSA (1977)

Ronald L. Rivest
(1947–)

Adi Shamir
(1952–)



Leonard Max
Adleman
(1945–)

Aplicaciones

Criptosistema RSA (1977)

- Se introduce la criptografía de clave pública.
- El cálculo de la clave privada en RSA depende de la resolución de una ecuación en congruencias.