Electiva II: Criptografía. Zaldívar, Felipe. Introducción a la teoría de números.

Electiva II: Criptografía. Zaldívar, Felipe. Introducción a la teoría de números.

- **Preliminares** ¿Cómo resolver problemas aritmético-algebraicos usando cálculo simbólico?

Electiva II: Criptografía. Zaldívar, Felipe. Introducción a la teoría de números.

- **Preliminares** ¿Cómo resolver problemas aritmético-algebraicos usando cálculo simbólico?
  - Cuadernos de Google Colab.
  - Funciones y clases. Módulo sympy.ntheory.

Electiva II: Criptografía. Zaldívar, Felipe. Introducción a la teoría de números.

- **Preliminares** ¿Cómo resolver problemas aritmético-algebraicos usando cálculo simbólico?
  - Cuadernos de Google Colab.
  - Funciones y clases. Módulo sympy.ntheory.
- **Cifrados de sustitución** ¿Por qué el algoritmo de la división es clave para crear cifrados por sustitución?

Electiva II: Criptografía. Zaldívar, Felipe. Introducción a la teoría de números.

- **Preliminares** ¿Cómo resolver problemas aritmético-algebraicos usando cálculo simbólico?
  - Cuadernos de Google Colab.
  - Funciones y clases. Módulo sympy.ntheory.
- **Cifrados de sustitución** ¿Por qué el algoritmo de la división es clave para crear cifrados por sustitución?
  - Números primos, congruencias y aritmética de residuos.
  - Teoremas de Fermat y Euler. Criptosistemas Cesar y Hill.

Electiva II: Criptografía. Zaldívar, Felipe. Introducción a la teoría de números.

- **Preliminares** ¿Cómo resolver problemas aritmético-algebraicos usando cálculo simbólico?
  - Cuadernos de Google Colab.
  - Funciones y clases. Módulo sympy.ntheory.
- **Cifrados de sustitución** ¿Por qué el algoritmo de la división es clave para crear cifrados por sustitución?
  - Números primos, congruencias y aritmética de residuos.
  - Teoremas de Fermat y Euler. Criptosistemas Cesar y Hill.
- **Primer cifrado de clave pública** ¿Favorece al desarrollo del pensamiento computacional el uso de atajos en los cálculos, usando nuevas representaciones de los números enteros?

Electiva II: Criptografía. Zaldívar, Felipe. Introducción a la teoría de números.

- **Preliminares** ¿Cómo resolver problemas aritmético-algebraicos usando cálculo simbólico?
  - Cuadernos de Google Colab.
  - Funciones y clases. Módulo sympy.ntheory.
- **Cifrados de sustitución** ¿Por qué el algoritmo de la división es clave para crear cifrados por sustitución?
  - Números primos, congruencias y aritmética de residuos.
  - Teoremas de Fermat y Euler. Criptosistemas Cesar y Hill.
- **Primer cifrado de clave pública** ¿Favorece al desarrollo del pensamiento computacional el uso de atajos en los cálculos, usando nuevas representaciones de los números enteros?
  - Algoritmos para potencias y raíces.
  - Firmas digitales. Criptosistema RSA.

Electiva II: Criptografía. Zaldívar, Felipe. Introducción a la teoría de números.

- **Preliminares** ¿Cómo resolver problemas aritmético-algebraicos usando cálculo simbólico?
  - Cuadernos de Google Colab.
  - Funciones y clases. Módulo sympy.ntheory.
- **Cifrados de sustitución** ¿Por qué el algoritmo de la división es clave para crear cifrados por sustitución?
  - Números primos, congruencias y aritmética de residuos.
  - Teoremas de Fermat y Euler. Criptosistemas Cesar y Hill.
- **Primer cifrado de clave pública** ¿Favorece al desarrollo del pensamiento computacional el uso de atajos en los cálculos, usando nuevas representaciones de los números enteros?
  - Algoritmos para potencias y raíces.
  - Firmas digitales. Criptosistema RSA.

- **Ecuaciones módulo un número entero** ¿Puede el ordenamiento en tablas de cálculos aritméticos fomentar el reconocimiento de patrones antes de la formalización con teoremas?

- **Ecuaciones módulo un número entero** ¿Puede el ordenamiento en tablas de cálculos aritméticos fomentar el reconocimiento de patrones antes de la formalización con teoremas?
  - Funciones de Euler y Möebius. Raíces. Logaritmos discretos.
  - Intercambio de claves Diffie-Hellman y Criptosistema ElGamal.

- **Ecuaciones módulo un número entero** ¿Puede el ordenamiento en tablas de cálculos aritméticos fomentar el reconocimiento de patrones antes de la formalización con teoremas?
  - Funciones de Euler y Möebius. Raíces. Logaritmos discretos.
  - Intercambio de claves Diffie-Hellman y Criptosistema ElGamal.
- **Residuos cuadráticos y símbolos de Jacobi** ¿Practicar criptografía revela la pertinencia de la enseñanza y el aprendizaje de estructuras algebraicas?

- **Ecuaciones módulo un número entero** ¿Puede el ordenamiento en tablas de cálculos aritméticos fomentar el reconocimiento de patrones antes de la formalización con teoremas?
  - Funciones de Euler y Möebius. Raíces. Logaritmos discretos.
  - Intercambio de claves Diffie-Hellman y Criptosistema ElGamal.
- **Residuos cuadráticos y símbolos de Jacobi** ¿Practicar criptografía revela la pertinencia de la enseñanza y el aprendizaje de estructuras algebraicas?
  - Ley de reciprocidad cuadrática.
  - Criptosistema Rabin.

- **Ecuaciones módulo un número entero** ¿Puede el ordenamiento en tablas de cálculos aritméticos fomentar el reconocimiento de patrones antes de la formalización con teoremas?
  - Funciones de Euler y Möebius. Raíces. Logaritmos discretos.
  - Intercambio de claves Diffie-Hellman y Criptosistema ElGamal.
- **Residuos cuadráticos y símbolos de Jacobi** ¿Practicar criptografía revela la pertinencia de la enseñanza y el aprendizaje de estructuras algebraicas?
  - Ley de reciprocidad cuadrática.
  - Criptosistema Rabin.
- **Historia reciente de criptografía** ¿Es el impacto ambiental la única preocupación ante la inminente creación de monedas digitales?

- **Ecuaciones módulo un número entero** ¿Puede el ordenamiento en tablas de cálculos aritméticos fomentar el reconocimiento de patrones antes de la formalización con teoremas?
  - Funciones de Euler y Möebius. Raíces. Logaritmos discretos.
  - Intercambio de claves Diffie-Hellman y Criptosistema ElGamal.
- **Residuos cuadráticos y símbolos de Jacobi** ¿Practicar criptografía revela la pertinencia de la enseñanza y el aprendizaje de estructuras algebraicas?
  - Ley de reciprocidad cuadrática.
  - Criptosistema Rabin.
- **Historia reciente de criptografía** ¿Es el impacto ambiental la única preocupación ante la inminente creación de monedas digitales?
  - Satoshi Nakamoto: Bitcoin P2P e-cash.
  - Activistas digitales Cyberpunk (protección de la privacidad).
  - Criptomonedas VS Otros servicios en internet. Alto impacto ambiental.

- **Ecuaciones módulo un número entero** ¿Puede el ordenamiento en tablas de cálculos aritméticos fomentar el reconocimiento de patrones antes de la formalización con teoremas?
  - Funciones de Euler y Möebius. Raíces. Logaritmos discretos.
  - Intercambio de claves Diffie-Hellman y Criptosistema ElGamal.
- **Residuos cuadráticos y símbolos de Jacobi** ¿Practicar criptografía revela la pertinencia de la enseñanza y el aprendizaje de estructuras algebraicas?
  - Ley de reciprocidad cuadrática.
  - Criptosistema Rabin.
- **Historia reciente de criptografía** ¿Es el impacto ambiental la única preocupación ante la inminente creación de monedas digitales?
  - Satoshi Nakamoto: Bitcoin P2P e-cash.
  - Activistas digitales Cyberpunk (protección de la privacidad).
  - Criptomonedas VS Otros servicios en internet. Alto impacto ambiental.