Teorema Chino del Residuo

Alan Reyes-Figueroa

Teoría de Números (Aula 13) 23.agosto.2021

Teorema (Teorema Chino del Residuo)

Sean $b_1, b_2, \ldots, b_k \in \mathbb{Z}$ enteros cualesquiera y $n_1, n_2, \ldots, n_k \in \mathbb{Z}$, $n_i > 1$, primos relativos dos a dos. Entonces, el sistema de ecuaciones

$$\begin{aligned} x &\equiv b_1 \pmod{n_1}, \\ x &\equiv b_2 \pmod{n_2}, \\ &\ldots \\ x &\equiv b_k \pmod{n_k}. \end{aligned}$$

admite solución, y ésta es única módulo $N = n_1 n_2 \cdots n_k$.

Teorema (Teorema Chino del Residuo)

Sean $b_1, b_2, \ldots, b_k \in \mathbb{Z}$ enteros cualesquiera y $n_1, n_2, \ldots, n_k \in \mathbb{Z}$, $n_i > 1$, primos relativos dos a dos. Entonces, el sistema de ecuaciones

$$\begin{aligned} x &\equiv b_1 \pmod{n_1}, \\ x &\equiv b_2 \pmod{n_2}, \\ &\cdots \\ x &\equiv b_k \pmod{n_k}. \end{aligned}$$

admite solución, y ésta es única módulo $N = n_1 n_2 \cdots n_k$.

<u>Prueba</u>: Consideramos los números de la forma $N_i = \frac{N}{n_i} = \prod_{j \neq i} n_j$, para $i = 1, 2, \ldots, k$.

Teorema (Teorema Chino del Residuo)

Sean $b_1, b_2, \ldots, b_k \in \mathbb{Z}$ enteros cualesquiera y $n_1, n_2, \ldots, n_k \in \mathbb{Z}$, $n_i > 1$, primos relativos dos a dos. Entonces, el sistema de ecuaciones

$$\begin{aligned} x &\equiv b_1 \pmod{n_1}, \\ x &\equiv b_2 \pmod{n_2}, \\ &\ldots \\ x &\equiv b_k \pmod{n_k}. \end{aligned}$$

admite solución, y ésta es única módulo $N = n_1 n_2 \cdots n_k$.

<u>Prueba</u>: Consideramos los números de la forma $N_i = \frac{N}{n_i} = \prod_{j \neq i} n_j$, para $i = 1, 2, \ldots, k$. Observe que $(n_i, N_i) = 1$ (ya que los n_i son todos primos relativos). Luego, N_i es invertible módulo n_i, de modo que existe $c_i \in \mathbb{Z}$ tal que $c_i N_i \equiv 1 \pmod{n_i}$.

Teorema (Teorema Chino del Residuo)

Sean $b_1, b_2, \ldots, b_k \in \mathbb{Z}$ enteros cualesquiera y $n_1, n_2, \ldots, n_k \in \mathbb{Z}$, $n_i > 1$, primos relativos dos a dos. Entonces, el sistema de ecuaciones

$$\begin{aligned} x &\equiv b_1 \pmod{n_1}, \\ x &\equiv b_2 \pmod{n_2}, \\ &\cdots \\ x &\equiv b_k \pmod{n_k}. \end{aligned}$$

admite solución, y ésta es única módulo $N = n_1 n_2 \cdots n_k$.

Prueba: Consideramos los números de la forma $N_i = \frac{N}{n_i} = \prod_{j \neq i} n_j$, para $i = 1, 2, \ldots, k$.
Observe que $(n_i, N_i) = 1$ (ya que los n_i son todos primos relativos). Luego, N_i es invertible módulo n_i, de modo que existe $c_i \in \mathbb{Z}$ tal que $c_i N_i \equiv 1 \pmod{n_i}$.
Además, si $i \neq j$, como $n_j \mid \prod_{j \neq i} n_j = N_i$, se tiene que $c_j N_j \equiv 0 \pmod{n_i}$, para todo $i \neq j$.

Congruencias Lineales

Consideramos el entero

$$x_0 = c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \in \mathbb{Z}.$$

Congruencias Lineales

Consideramos el entero

$$x_0 = c_1 N_1 b_1 + c_2 N_2 b_2 + \ldots + c_k N_k b_k \in \mathbb{Z}.$$

Afirmamos que x_0 es solución del sistema de congruencias (1).

Congruencias Lineales

Consideramos el entero

$$x_0 = c_1 N_1 b_1 + c_2 N_2 b_2 + \ldots + c_k N_k b_k \in \mathbb{Z}.$$

Afirmamos que x_0 es solución del sistema de congruencias (1). De hecho, para cada $i = 1, 2, \ldots, k$ se tiene

$$x_0 \equiv c_1 N_1 b_1 + c_2 N_2 b_2 + \ldots + c_k N_k b_k \pmod{n_i}$$

Consideramos el entero

$$x_0 = c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \in \mathbb{Z}.$$

Afirmamos que x_0 es solución del sistema de congruencias (1). De hecho, para cada $i = 1, 2, \ldots, k$ se tiene

$$\begin{aligned} x_0 &\equiv c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \pmod{n_i} \\ &\equiv (0)b_1 + (0)b_2 + \ldots (1)b_i + \ldots + (0)b_k \pmod{n_i} \end{aligned}$$

Congruencias Lineales

Consideramos el entero

$$x_0 = c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \in \mathbb{Z}.$$

Afirmamos que x_0 es solución del sistema de congruencias (1). De hecho, para cada $i = 1, 2, \ldots, k$ se tiene

$$\begin{aligned} x_0 &\equiv c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \pmod{n_i} \\ &\equiv (0)b_1 + (0)b_2 + \ldots (1)b_i + \ldots + (0)b_k \pmod{n_i} \\ &\equiv b_i \pmod{n_i}. \end{aligned}$$

Congruencias Lineales

Consideramos el entero

$$x_0 = c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \in \mathbb{Z}.$$

Afirmamos que x_0 es solución del sistema de congruencias (1). De hecho, para cada $i = 1, 2, \ldots, k$ se tiene

$$\begin{aligned} x_0 &\equiv c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \pmod{n_i} \\ &\equiv (0)b_1 + (0)b_2 + \ldots (1)b_i + \ldots + (0)b_k \pmod{n_i} \\ &\equiv b_i \pmod{n_i}. \end{aligned}$$

Así, x_0 es solución del sistema.

Congruencias Lineales

Consideramos el entero

$$x_0 = c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \in \mathbb{Z}.$$

Afirmamos que x_0 es solución del sistema de congruencias (1). De hecho, para cada $i = 1, 2, \ldots, k$ se tiene

$$\begin{aligned} x_0 &\equiv c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \pmod{n_i} \\ &\equiv (0)b_1 + (0)b_2 + \ldots (1)b_i + \ldots + (0)b_k \pmod{n_i} \\ &\equiv b_i \pmod{n_i}. \end{aligned}$$

Así, x_0 es solución del sistema.

Por otro lado, si $x_1 \in \mathbb{Z}$ es otra solución, entonces

$$x_0 \equiv x_1 \pmod{n_i} \iff n_i \mid x_0 - x_1, \qquad \text{para todo } i = 1, 2, \ldots, k.$$

Congruencias Lineales

Consideramos el entero

$$x_0 = c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \in \mathbb{Z}.$$

Afirmamos que x_0 es solución del sistema de congruencias (1). De hecho, para cada $i = 1, 2, \ldots, k$ se tiene

$$\begin{aligned} x_0 &\equiv c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \pmod{n_i} \\ &\equiv (0)b_1 + (0)b_2 + \ldots (1)b_i + \ldots + (0)b_k \pmod{n_i} \\ &\equiv b_i \pmod{n_i}. \end{aligned}$$

Así, x_0 es solución del sistema.

Por otro lado, si $x_1 \in \mathbb{Z}$ es otra solución, entonces

$$x_0 \equiv x_1 \pmod{n_i} \iff n_i \mid x_0 - x_1, \qquad \text{para todo } i = 1, 2, \ldots, k.$$

Como los n_i son todos primos relativos, entonces los coroloarios al Lema de Euclides, más el uso de inducción matemática, implican que $N = n_1n_2 \cdots n_k \mid x_0 - x_1$.

Consideramos el entero

$$x_0 = c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \in \mathbb{Z}.$$

Afirmamos que x_0 es solución del sistema de congruencias (1). De hecho, para cada $i = 1, 2, \ldots, k$ se tiene

$$\begin{aligned} x_0 &\equiv c_1N_1b_1 + c_2N_2b_2 + \ldots + c_kN_kb_k \pmod{n_i} \\ &\equiv (0)b_1 + (0)b_2 + \ldots (1)b_i + \ldots + (0)b_k \pmod{n_i} \\ &\equiv b_i \pmod{n_i}. \end{aligned}$$

Así, x_0 es solución del sistema.

Por otro lado, si $x_1 \in \mathbb{Z}$ es otra solución, entonces

$$x_0 \equiv x_1 \pmod{n_i} \iff n_i \mid x_0 - x_1, \qquad \text{para todo } i = 1, 2, \ldots, k.$$

Como los n_i son todos primos relativos, entonces los coroloarios al Lema de Euclides, más el uso de inducción matemática, implican que $N = n_1n_2 \cdots n_k \mid x_0 - x_1$. Portanto $x_0 \equiv x_1 \pmod{N}$. $\square$

Congruencias Lineales

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica.

Congruencias Lineales

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica. Consideramos el mapa natural $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, dado por

$$f : b \pmod{N} \mapsto (b \pmod{n_1}, b \pmod{n_2}, \ldots, b \pmod{n_k}).$$

Congruencias Lineales

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica. Consideramos el mapa natural $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, dado por

$$f : b \pmod{N} \mapsto (b \pmod{n_1}, b \pmod{n_2}, \ldots, b \pmod{n_k}).$$

Este mapa está bien definido, pues si b' es otro representante en la misma clase de congruencia $b \pmod{N}$, entonces $N \mid b - b'$, y portanto $n_i \mid b - b'$, para todo $i = 1, 2, \ldots, k$, de modo que $b \equiv b' \pmod{n_i}$, $\forall i$, y se tiene que $f(b) = f(b')$.

Congruencias Lineales

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica. Consideramos el mapa natural $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, dado por

$$f : b \pmod N \mapsto (b \pmod{n_1}, b \pmod{n_2}, \ldots, b \pmod{n_k}).$$

Este mapa está bien definido, pues si b' es otro representante en la misma clase de congruencia $b \pmod N$, entonces $N \mid b - b'$, y portanto $n_i \mid b - b'$, para todo $i = 1, 2, \ldots, k$, de modo que $b \equiv b' \pmod{n_i}$, $\forall i$, y se tiene que $f(b) = f(b')$.

Observe que el Teorema Chino es equivalente a mostrar que el mapa f es una biyección:

Congruencias Lineales

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica. Consideramos el mapa natural $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, dado por

$$f : b \pmod{N} \mapsto (b \pmod{n_1}, b \pmod{n_2}, \dots, b \pmod{n_k}).$$

Este mapa está bien definido, pues si b' es otro representante en la misma clase de congruencia $b \pmod{N}$, entonces $N \mid b - b'$, y portanto $n_i \mid b - b'$, para todo $i = 1, 2, \dots, k$, de modo que $b \equiv b' \pmod{n_i}$, $\forall i$, y se tiene que $f(b) = f(b')$.

Observe que el Teorema Chino es equivalente a mostrar que el mapa f es una biyección: el hecho de f ser sobreyectiva corresponde a la existencia de la solución del sistema (1), mientras que la inyectividad corresponde a la unicidad módulo N.

Congruencias Lineales

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica. Consideramos el mapa natural $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, dado por

$$f : b \pmod{N} \mapsto (b \pmod{n_1}, b \pmod{n_2}, \ldots, b \pmod{n_k}).$$

Este mapa está bien definido, pues si b' es otro representante en la misma clase de congruencia $b \pmod{N}$, entonces $N \mid b - b'$, y portanto $n_i \mid b - b'$, para todo $i = 1, 2, \ldots, k$, de modo que $b \equiv b' \pmod{n_i}$, $\forall i$, y se tiene que $f(b) = f(b')$.

Observe que el Teorema Chino es equivalente a mostrar que el mapa f es una biyección: el hecho de f ser sobreyectiva corresponde a la existencia de la solución del sistema (1), mientras que la inyectividad corresponde a la unicidad módulo N.

Como $|\mathbb{Z}/N\mathbb{Z}| = N = n_1 n_2 \cdots n_k = |\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}|$, basta mostrar que f es inyectiva.

Congruencias Lineales

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica. Consideramos el mapa natural $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, dado por

$$f : b \pmod{N} \mapsto (b \pmod{n_1}, b \pmod{n_2}, \ldots, b \pmod{n_k}).$$

Este mapa está bien definido, pues si b' es otro representante en la misma clase de congruencia $b \pmod{N}$, entonces $N \mid b - b'$, y portanto $n_i \mid b - b'$, para todo $i = 1, 2, \ldots, k$, de modo que $b \equiv b' \pmod{n_i}$, $\forall i$, y se tiene que $f(b) = f(b')$.

Observe que el Teorema Chino es equivalente a mostrar que el mapa f es una biyección: el hecho de f ser sobreyectiva corresponde a la existencia de la solución del sistema (1), mientras que la inyectividad corresponde a la unicidad módulo N.

Como $|\mathbb{Z}/N\mathbb{Z}| = N = n_1 n_2 \cdots n_k = |\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}|$, basta mostrar que f es inyectiva. Primero note que f es un morfismo de anillos.

Congruencias Lineales

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica. Consideramos el mapa natural $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, dado por

$$f : b \pmod{N} \mapsto (b \pmod{n_1}, b \pmod{n_2}, \ldots, b \pmod{n_k}).$$

Este mapa está bien definido, pues si b' es otro representante en la misma clase de congruencia $b \pmod{N}$, entonces $N \mid b - b'$, y portanto $n_i \mid b - b'$, para todo $i = 1, 2, \ldots, k$, de modo que $b \equiv b' \pmod{n_i}$, $\forall i$, y se tiene que $f(b) = f(b')$.

Observe que el Teorema Chino es equivalente a mostrar que el mapa f es una biyección: el hecho de f ser sobreyectiva corresponde a la existencia de la solución del sistema (1), mientras que la inyectividad corresponde a la unicidad módulo N.

Como $|\mathbb{Z}/N\mathbb{Z}| = N = n_1 n_2 \cdots n_k = |\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}|$, basta mostrar que f es inyectiva. Primero note que f es un morfismo de anillos. Suponga que $f(x) = 0 = (0, 0, \ldots, 0)$. Entonces $x \equiv 0 \pmod{n}_i$, para todo $i = 1, 2, \ldots, k$.

Congruencias Lineales

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica. Consideramos el mapa natural $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, dado por

$$f : b \pmod{N} \mapsto (b \pmod{n_1}, b \pmod{n_2}, \ldots, b \pmod{n_k}).$$

Este mapa está bien definido, pues si b' es otro representante en la misma clase de congruencia $b \pmod{N}$, entonces $N \mid b - b'$, y portanto $n_i \mid b - b'$, para todo $i = 1, 2, \ldots, k$, de modo que $b \equiv b' \pmod{n_i}$, $\forall i$, y se tiene que $f(b) = f(b')$.

Observe que el Teorema Chino es equivalente a mostrar que el mapa f es una biyección: el hecho de f ser sobreyectiva corresponde a la existencia de la solución del sistema (1), mientras que la inyectividad corresponde a la unicidad módulo N.

Como $|\mathbb{Z}/N\mathbb{Z}| = N = n_1 n_2 \cdots n_k = |\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}|$, basta mostrar que f es inyectiva. Primero note que f es un morfismo de anillos. Suponga que $f(x) = 0 = (0, 0, \ldots, 0)$. Entonces $x \equiv 0 \pmod{n}_i$, para todo $i = 1, 2, \ldots, k$. Esto implica que $n_i \mid x$, $\forall i$, y de nuevo el lema de Euclides implica que $N \mid x$.

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica. Consideramos el mapa natural $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, dado por

$$f : b \pmod N \mapsto (b \pmod{n_1}, b \pmod{n_2}, \ldots, b \pmod{n_k}).$$

Este mapa está bien definido, pues si b' es otro representante en la misma clase de congruencia $b \pmod N$, entonces $N \mid b - b'$, y portanto $n_i \mid b - b'$, para todo $i = 1, 2, \ldots, k$, de modo que $b \equiv b' \pmod{n_i}$, $\forall i$, y se tiene que $f(b) = f(b')$.

Observe que el Teorema Chino es equivalente a mostrar que el mapa f es una biyección: el hecho de f ser sobreyectiva corresponde a la existencia de la solución del sistema (1), mientras que la inyectividad corresponde a la unicidad módulo N.

Como $|\mathbb{Z}/N\mathbb{Z}| = N = n_1 n_2 \cdots n_k = |\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}|$, basta mostrar que f es inyectiva. Primero note que f es un morfismo de anillos. Suponga que $f(x) = 0 = (0, 0, \ldots, 0)$. Entonces $x \equiv 0 \pmod n)_i$, para todo $i = 1, 2, \ldots, k$. Esto implica que $n_i \mid x$, $\forall i$, y de nuevo el lema de Euclides implica que $N \mid x$. Asi, $x \equiv 0 \pmod N$.

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica. Consideramos el mapa natural $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, dado por

$$f : b \pmod{N} \mapsto (b \pmod{n_1}, b \pmod{n_2}, \ldots, b \pmod{n_k}).$$

Este mapa está bien definido, pues si b' es otro representante en la misma clase de congruencia $b \pmod{N}$, entonces $N \mid b - b'$, y portanto $n_i \mid b - b'$, para todo $i = 1, 2, \ldots, k$, de modo que $b \equiv b' \pmod{n_i}$, $\forall i$, y se tiene que $f(b) = f(b')$.

Observe que el Teorema Chino es equivalente a mostrar que el mapa f es una biyección: el hecho de f ser sobreyectiva corresponde a la existencia de la solución del sistema (1), mientras que la inyectividad corresponde a la unicidad módulo N.

Como $|\mathbb{Z}/N\mathbb{Z}| = N = n_1 n_2 \cdots n_k = |\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}|$, basta mostrar que f es inyectiva. Primero note que f es un morfismo de anillos. Suponga que $f(x) = 0 = (0, 0, \ldots, 0)$. Entonces $x \equiv 0 \pmod{n}_i$, para todo $i = 1, 2, \ldots, k$. Esto implica que $n_i \mid x$, $\forall i$, y de nuevo el lema de Euclides implica que $N \mid x$. Asi, $x \equiv 0 \pmod{N}$. Esto muestra que $\operatorname{Ker} f = 0$, luego f es inyectiva, y portanto biyectiva. $\square$

Definición

Un entero $n \in \mathbb{Z}$ es ***libre de cuadrados*** *si n no es divisible por el cuadrado de ningún número mayor que 1.*

Definición

*Un entero $n \in \mathbb{Z}$ es **libre de cuadrados** si n no es divisible por el cuadrado de ningún número mayor que 1.*

Ejemplo: Vamos a mostrar que existen intervalos arbitráriamente grandes, de enteros consecutivos, ninguno de los cuales es libre de cuadrados.

Definición

*Un entero $n \in \mathbb{Z}$ es **libre de cuadrados** si n no es divisible por el cuadrado de ningún número mayor que 1.*

Ejemplo: Vamos a mostrar que existen intervalos arbitráriamente grandes, de enteros consecutivos, ninguno de los cuales es libre de cuadrados.

Solución: Sea $n \in \mathbb{N}$ un número natural cualquiera, y sean $p_1, p_2, \ldots, p_n$ primos distintos.

Definición

Un entero $n \in \mathbb{Z}$ es ***libre de cuadrados*** *si n no es divisible por el cuadrado de ningún número mayor que 1.*

Ejemplo: Vamos a mostrar que existen intervalos arbitráriamente grandes, de enteros consecutivos, ninguno de los cuales es libre de cuadrados.

Solución: Sea $n \in \mathbb{N}$ un número natural cualquiera, y sean $p_1, p_2, \ldots, p_n$ primos distintos. Por el Teorema Chino, existen soluciones al sistema

$$\begin{aligned} x &\equiv -1 \pmod{p_1^2}, \\ x &\equiv -2 \pmod{p_2^2}, \\ &\cdots, \\ x &\equiv -n \pmod{p_k^2}. \end{aligned}$$

Definición

Un entero $n \in \mathbb{Z}$ es ***libre de cuadrados*** *si n no es divisible por el cuadrado de ningún número mayor que 1.*

Ejemplo: Vamos a mostrar que existen intervalos arbitráriamente grandes, de enteros consecutivos, ninguno de los cuales es libre de cuadrados.

Solución: Sea $n \in \mathbb{N}$ un número natural cualquiera, y sean $p_1, p_2, \ldots, p_n$ primos distintos. Por el Teorema Chino, existen soluciones al sistema

$$\begin{aligned} x &\equiv -1 \pmod{p_1^2}, \\ x &\equiv -2 \pmod{p_2^2}, \\ &\cdots, \\ x &\equiv -n \pmod{p_k^2}. \end{aligned}$$

Si x_0 es una solución positiva, entonces cada uno de los números $x_0 + 1, x_0 + 2, \ldots, x_0 + n$ es divisible por el cuadrado de algún primo, y ninguno es libre de cuadrados.

Lema

Sea $P(x) \in \mathbb{Z}[x]$ *un polinomio no constante con coeficientes enteros. Para todo* $k, i \in \mathbb{Z}$*, se tiene que*

$$P(i) \mid P\big(kP(i) + i\big).$$

Lema

Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Para todo $k, i \in \mathbb{Z}$, se tiene que

$$P(i) \mid P\big(kP(i) + i\big).$$

<u>Prueba</u>: Observe que para todo $n \in \mathbb{N}$

$$\big(kP(i) + i\big)^n \equiv \sum_{j=0}^{n} \binom{n}{j} k^j P(i)^j i^{n-j} \equiv i^n \pmod{P(i)}.$$

Lema

Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Para todo $k, i \in \mathbb{Z}$, se tiene que

$$P(i) \mid P\big(kP(i) + i\big).$$

<u>Prueba</u>: Observe que para todo $n \in \mathbb{N}$

$$\big(kP(i) + i\big)^n \equiv \sum_{j=0}^{n} \binom{n}{j} k^j P(i)^j i^{n-j} \equiv i^n \pmod{P(i)}.$$

Como las congruencias se preservan mediante productos y sumas, entonces para cualquier polinomio $f(x) \in \mathbb{Z}[x]$, se tiene que $f\big(kP(i) + i\big) \equiv f(i) \pmod{P(i)}$.
En particular, $P\big(kP(i) + i\big) \equiv P(i) \equiv 0 \pmod{P(i)}$. $\square$

Aplicaciones

Ejemplo: Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros.

Aplicaciones

Ejemplo: Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Mostramos que para todo entero $n \in \mathbb{N}$, existe un entero i tal que los números son compuestos

$$P(i), P(i+1), P(i+2), \ldots, P(i+n),$$

Aplicaciones

Ejemplo: Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Mostramos que para todo entero $n \in \mathbb{N}$, existe un entero i tal que los números son compuestos

$$P(i), P(i+1), P(i+2), \ldots, P(i+n),$$

<u>Solución</u>: Supongamos que la secuencia $P(i), P(i+1), \ldots, P(i+n)$ contiene un primo para cada i.

Aplicaciones

Ejemplo: Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Mostramos que para todo entero $n \in \mathbb{N}$, existe un entero i tal que los números son compuestos

$$P(i), P(i+1), P(i+2), \ldots, P(i+n),$$

<u>Solución</u>: Supongamos que la secuencia $P(i), P(i+1), \ldots, P(i+n)$ contiene un primo para cada i. Entonces la secuencia $P(i)_{i \geq 1}$ contiene sólo números primos.

Aplicaciones

Ejemplo: Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Mostramos que para todo entero $n \in \mathbb{N}$, existe un entero i tal que los números son compuestos

$$P(i), P(i+1), P(i+2), \ldots, P(i+n),$$

Solución: Supongamos que la secuencia $P(i), P(i+1), \ldots, P(i+n)$ contiene un primo para cada i. Entonces la secuencia $P(i)_{i\geq 1}$ contiene sólo números primos. Consideramos los $n+1$ primeros números primos distintos $P(i_0), P(i_1), \ldots, P(i_n)$.

Aplicaciones

Ejemplo: Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Mostramos que para todo entero $n \in \mathbb{N}$, existe un entero i tal que los números son compuestos

$$P(i), P(i+1), P(i+2), \ldots, P(i+n),$$

<u>Solución</u>: Supongamos que la secuencia $P(i), P(i+1), \ldots, P(i+n)$ contiene un primo para cada i. Entonces la secuencia $P(i)_{i\geq 1}$ contiene sólo números primos.
Consideramos los $n+1$ primeros números primos distintos $P(i_0), P(i_1), \ldots, P(i_n)$. Por el Teorema Chino, existen infinitas soluciones al sistema

$$\begin{aligned} x &\equiv i_0 \pmod{P(i_0)}, \\ x &\equiv i_1 - 1 \pmod{P(i_1)}, \\ &\cdots, \\ x &\equiv i_n - n \pmod{P(i_n)}. \end{aligned}$$

UNIVERSIDAD DEL VALLE DE GUATEMALA

Ejemplo: Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Mostramos que para todo entero $n \in \mathbb{N}$, existe un entero i tal que los números son compuestos
$$P(i), P(i+1), P(i+2), \ldots, P(i+n),$$

Solución: Supongamos que la secuencia $P(i), P(i+1), \ldots, P(i+n)$ contiene un primo para cada i. Entonces la secuencia $P(i)_{i \geq 1}$ contiene sólo números primos.

Consideramos los $n+1$ primeros números primos distintos $P(i_0), P(i_1), \ldots, P(i_n)$. Por el Teorema Chino, existen infinitas soluciones al sistema
$$\begin{aligned} x &\equiv i_0 \pmod{P(i_0)}, \\ x &\equiv i_1 - 1 \pmod{P(i_1)}, \\ &\cdots, \\ x &\equiv i_n - n \pmod{P(i_n)}. \end{aligned}$$

Si x_0 es una solución de este sistema, entonces $x = x_0 + k\big(P(i_o)P(i_1)\cdots P(i_n)\big)$ es también solución, $\forall k \geq 0$.

Aplicaciones

Ejemplo: Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Mostramos que para todo entero $n \in \mathbb{N}$, existe un entero i tal que los números son compuestos

$$P(i), P(i+1), P(i+2), \ldots, P(i+n),$$

Solución: Supongamos que la secuencia $P(i), P(i+1), \ldots, P(i+n)$ contiene un primo para cada i. Entonces la secuencia $P(i)_{i \geq 1}$ contiene sólo números primos.
Consideramos los $n+1$ primeros números primos distintos $P(i_0), P(i_1), \ldots, P(i_n)$. Por el Teorema Chino, existen infinitas soluciones al sistema

$$\begin{aligned} x &\equiv i_0 \pmod{P(i_0)}, \\ x &\equiv i_1 - 1 \pmod{P(i_1)}, \\ \cdots &\;, \\ x &\equiv i_n - n \pmod{P(i_n)}. \end{aligned}$$

Si x_0 es una solución de este sistema, entonces $x = x_0 + k\big(P(i_0)P(i_1)\cdots P(i_n)\big)$ es también solución, $\forall k \geq 0$. Por el lema anterior, $P(x), P(x+1), \ldots, P(x+n)$ son compuestos, para k es suficientemente grande,

Ejemplo: Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Mostramos que para todo entero $n \in \mathbb{N}$, existe un entero i tal que los números son compuestos

$$P(i), P(i+1), P(i+2), \ldots, P(i+n),$$

<u>Solución</u>: Supongamos que la secuencia $P(i), P(i+1), \ldots, P(i+n)$ contiene un primo para cada i. Entonces la secuencia $P(i)_{i \geq 1}$ contiene sólo números primos.

Consideramos los $n+1$ primeros números primos distintos $P(i_0), P(i_1), \ldots, P(i_n)$. Por el Teorema Chino, existen infinitas soluciones al sistema

$$\begin{aligned} x &\equiv i_0 \pmod{P(i_0)}, \\ x &\equiv i_1 - 1 \pmod{P(i_1)}, \\ &\cdots, \\ x &\equiv i_n - n \pmod{P(i_n)}. \end{aligned}$$

Si x_0 es una solución de este sistema, entonces $x = x_0 + k\big(P(i_o)P(i_1)\cdots P(i_n)\big)$ es también solución, $\forall k \geq 0$. Por el lema anterior, $P(x), P(x+1), \ldots, P(x+n)$ son compuestos, para k es suficientemente grande, múltiplos respectivamente de $P(i_0)$, $P(i_1), \ldots, P(x_n)$. $\square$

Congruencias de grado 2

Sea $p > 2$ un primo impar, y sean $a, b, c \in \mathbb{Z}$, con $p \nmid a$.

Congruencias de grado 2

Sea $p > 2$ un primo impar, y sean $a, b, c \in \mathbb{Z}$, con $p \nmid a$. Estamos interesados en resolver la ecuación cuadrática

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{1}$$

Congruencias de grado 2

Sea $p > 2$ un primo impar, y sean $a, b, c \in \mathbb{Z}$, con $p \nmid a$. Estamos interesados en resolver la ecuación cuadrática

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{1}$$

Completando al cuadrado (esto es, multiplicando por $4a$, y luego sumando b^2), la ecuación anterior es equivalente a

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}. \tag{2}$$

(Observe que 2 y a no son divisíbles por p).

Congruencias de grado 2

Sea $p > 2$ un primo impar, y sean $a, b, c \in \mathbb{Z}$, con $p \nmid a$. Estamos interesados en resolver la ecuación cuadrática

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{1}$$

Completando al cuadrado (esto es, multiplicando por $4a$, y luego sumando b^2), la ecuación anterior es equivalente a

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}. \tag{2}$$

(Observe que 2 y a no son divisíbles por p).

Así, estamos interesados en encontrar criterios para la existencia de soluciones de la ecuación

$$x^2 \equiv d \pmod{p}. \tag{3}$$

UNIVERSIDAD DEL VALLE DE GUATEMALA

Congruencias de grado 2

Sea $p > 2$ un primo impar, y sean $a, b, c \in \mathbb{Z}$, con $p \nmid a$. Estamos interesados en resolver la ecuación cuadrática

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{1}$$

Completando al cuadrado (esto es, multiplicando por $4a$, y luego sumando b^2), la ecuación anterior es equivalente a

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}. \tag{2}$$

(Observe que 2 y a no son divisíbles por p).

Así, estamos interesados en encontrar criterios para la existencia de soluciones de la ecuación

$$x^2 \equiv d \pmod{p}. \tag{3}$$

Definición

*Si la ecuación (3) tiene solución, esto es, $\bar{d}$ es un cuadrado perfecto en $\mathbb{Z}/p\mathbb{Z}$, diremos que d es un **residuo cuadrático** módulo p.*

Congruencias de grado 2

Hay exactamente $\frac{p+1}{2}$ residuos cuadráticos módulo p, $p > 2$. A saber:

$$0^2, (\pm 1)^2, (\pm 2)^2, (\pm 3)^2, \ldots, \Big(\pm \frac{p-1}{2}\Big)^2 \pmod{p},$$

Congruencias de grado 2

Hay exactamente $\frac{p+1}{2}$ residuos cuadráticos módulo p, $p > 2$. A saber:

$$0^2, (\pm 1)^2, (\pm 2)^2, (\pm 3)^2, \ldots, \Big(\pm \frac{p-1}{2}\Big)^2 \pmod{p},$$

ya que $i^2 \equiv (-i)^2 \pmod{p}$.

Congruencias de grado 2

Hay exactamente $\frac{p+1}{2}$ residuos cuadráticos módulo p, $p > 2$. A saber:

$$0^2, (\pm 1)^2, (\pm 2)^2, (\pm 3)^2, \ldots, \Big(\pm \frac{p-1}{2}\Big)^2 \pmod{p},$$

ya que $i^2 \equiv (-i)^2 \pmod{p}$. Observe que todos estos números son incongruentes módulo p, de manera que conforman un sistema completo de residuos cuadráticos módulo p, pues

Congruencias de grado 2

Hay exactamente $\frac{p+1}{2}$ residuos cuadráticos módulo p, $p > 2$. A saber:

$$0^2, (\pm 1)^2, (\pm 2)^2, (\pm 3)^2, \ldots, \Big(\pm \frac{p-1}{2}\Big)^2 \pmod{p},$$

ya que $i^2 \equiv (-i)^2 \pmod{p}$. Observe que todos estos números son incongruentes módulo p, de manera que conforman un sistema completo de residuos cuadráticos módulo p, pues

$$\begin{aligned} i^2 \equiv j^2 \pmod{p} &\iff p \mid i^2 - j^2 = (i-j)(i+j) \\ &\iff p \mid i-j \text{ ó } p \mid i+j \\ &\iff i \equiv \pm j \pmod{p}. \end{aligned}$$

Congruencias de grado 2

Hay exactamente $\frac{p+1}{2}$ residuos cuadráticos módulo p, $p > 2$. A saber:

$$0^2, (\pm 1)^2, (\pm 2)^2, (\pm 3)^2, \ldots, \Big(\pm\frac{p-1}{2}\Big)^2 \pmod{p},$$

ya que $i^2 \equiv (-i)^2 \pmod{p}$. Observe que todos estos números son incongruentes módulo p, de manera que conforman un sistema completo de residuos cuadráticos módulo p, pues

$$\begin{aligned} i^2 \equiv j^2 \pmod{p} &\iff p \mid i^2 - j^2 = (i-j)(i+j) \\ &\iff p \mid i - j \text{ ó } p \mid i + j \\ &\iff i \equiv \pm j \pmod{p}. \end{aligned}$$

Así, si x es residuo cuadrático módulo p, debe ser congruente a alguno de estos números.

Congruencias de grado 2

Hay exactamente $\frac{p+1}{2}$ residuos cuadráticos módulo p, $p > 2$. A saber:

$$0^2, (\pm 1)^2, (\pm 2)^2, (\pm 3)^2, \ldots, \left(\pm \frac{p-1}{2}\right)^2 \pmod{p},$$

ya que $i^2 \equiv (-i)^2 \pmod{p}$. Observe que todos estos números son incongruentes módulo p, de manera que conforman un sistema completo de residuos cuadráticos módulo p, pues

$$\begin{aligned} i^2 \equiv j^2 \pmod{p} &\iff p \mid i^2 - j^2 = (i-j)(i+j) \\ &\iff p \mid i-j \text{ ó } p \mid i+j \\ &\iff i \equiv \pm j \pmod{p}. \end{aligned}$$

Así, si x es residuo cuadrático módulo p, debe ser congruente a alguno de estos números.

Ahora, aunque conozcamos la lista completa de residuos cuadráticos módulo p, en la práctica es difícil reconocer si un número d es o no residuo cuadrático módulo p.

Congruencias de grado 2

Ejemplo: Módulo 23 tenemos

- $0^2 \equiv 0 \pmod{23}$,
- $1^2 \equiv 1 \pmod{23}$,
- $2^2 \equiv 4 \pmod{23}$,
- $3^2 \equiv 9 \pmod{23}$,
- $4^2 \equiv 16 \pmod{23}$,
- $5^2 \equiv 2 \pmod{23}$,
- $6^2 \equiv 13 \pmod{23}$,
- $7^2 \equiv 3 \pmod{23}$,
- $8^2 \equiv 18 \pmod{23}$,
- $9^2 \equiv 12 \pmod{23}$,
- $10^2 \equiv 8 \pmod{23}$,
- $11^2 \equiv 6 \pmod{23}$,

Congruencias de grado 2

Ejemplo: Módulo 23 tenemos

- $0^2 \equiv 0 \pmod{23}$,
- $1^2 \equiv 1 \pmod{23}$,
- $2^2 \equiv 4 \pmod{23}$,
- $3^2 \equiv 9 \pmod{23}$,
- $4^2 \equiv 16 \pmod{23}$,
- $5^2 \equiv 2 \pmod{23}$,
- $6^2 \equiv 13 \pmod{23}$,
- $7^2 \equiv 3 \pmod{23}$,
- $8^2 \equiv 18 \pmod{23}$,
- $9^2 \equiv 12 \pmod{23}$,
- $10^2 \equiv 8 \pmod{23}$,
- $11^2 \equiv 6 \pmod{23}$,

Así, los resíduos cuadráticos módulo 23 son:

$$0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.$$

Congruencias de grado 2

Ejemplo: Módulo 23 tenemos

- $0^2 \equiv 0 \pmod{23}$,
- $1^2 \equiv 1 \pmod{23}$,
- $2^2 \equiv 4 \pmod{23}$,
- $3^2 \equiv 9 \pmod{23}$,
- $4^2 \equiv 16 \pmod{23}$,
- $5^2 \equiv 2 \pmod{23}$,
- $6^2 \equiv 13 \pmod{23}$,
- $7^2 \equiv 3 \pmod{23}$,
- $8^2 \equiv 18 \pmod{23}$,
- $9^2 \equiv 12 \pmod{23}$,
- $10^2 \equiv 8 \pmod{23}$,
- $11^2 \equiv 6 \pmod{23}$,

Así, los resíduos cuadráticos módulo 23 son:

$$0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.$$

Ejemplo: ¿Es 53 resíduo cuadrático módulo 101?

Congruencias de grado 2

Ejemplo: Módulo 23 tenemos

- $0^2 \equiv 0 \pmod{23}$,
- $1^2 \equiv 1 \pmod{23}$,
- $2^2 \equiv 4 \pmod{23}$,
- $3^2 \equiv 9 \pmod{23}$,
- $4^2 \equiv 16 \pmod{23}$,
- $5^2 \equiv 2 \pmod{23}$,
- $6^2 \equiv 13 \pmod{23}$,
- $7^2 \equiv 3 \pmod{23}$,
- $8^2 \equiv 18 \pmod{23}$,
- $9^2 \equiv 12 \pmod{23}$,
- $10^2 \equiv 8 \pmod{23}$,
- $11^2 \equiv 6 \pmod{23}$,

Así, los resíduos cuadráticos módulo 23 son:

$$0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.$$

Ejemplo: ¿Es 53 resíduo cuadrático módulo 101?
No.

Congruencias de grado 2

Ejemplo: Módulo 23 tenemos

- $0^2 \equiv 0 \pmod{23}$,
- $1^2 \equiv 1 \pmod{23}$,
- $2^2 \equiv 4 \pmod{23}$,
- $3^2 \equiv 9 \pmod{23}$,
- $4^2 \equiv 16 \pmod{23}$,
- $5^2 \equiv 2 \pmod{23}$,
- $6^2 \equiv 13 \pmod{23}$,
- $7^2 \equiv 3 \pmod{23}$,
- $8^2 \equiv 18 \pmod{23}$,
- $9^2 \equiv 12 \pmod{23}$,
- $10^2 \equiv 8 \pmod{23}$,
- $11^2 \equiv 6 \pmod{23}$,

Así, los resíduos cuadráticos módulo 23 son:

$$0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.$$

Ejemplo: ¿Es 53 resíduo cuadrático módulo 101?
No.

Precisamos de una forma eficiente para determinar si un entero a cualquiera es residuo cuadrático módulo p.