Congruencias

Si a y b son enteros y $\mathbf{n}$ es un número natural, decimos que a y b son **congruentes modulo $\mathbf{n}$** si $a-b$ es divisible entre $\mathbf{n}$, y escribimos $a \equiv b \pmod{\mathbf{n}}$.
Observar que $a \equiv b \pmod{\mathbf{n}}$ si y solo si a y b dejan el mismo residuo al ser divididos entre $\mathbf{n}$.

Ejemplos.

$3 \equiv 7 \pmod 4$ $\quad -5 \equiv 9 \pmod 7$ $\quad 66 \equiv 0 \pmod{11}$ $\quad -1 \equiv 1 \pmod 2$

Lema 1. Las congruencias modulo $\mathbf{n}$ definen una relación de equivalencia en $\mathbf{Z}$.

Demostración. Hay que ver que ser congruentes modulo n es una relación reflexiva, simétrica y transitiva:

- $a \equiv a \pmod n$ ya que $a-a=0$ es divisible entre n para todo n.
- Si $a \equiv b \pmod n$ entonces $b \equiv a \pmod n$, ya que si $a-b$ es divisible entre n entonces $b-a$ también es divisible entre n.
- Si $a \equiv b \pmod n$ y $b \equiv c \pmod n$ entonces $a \equiv c \pmod n$, ya que si $a-b$ y $b-c$ son divisibles entre n entonces $a-c=(a-b)+(b-c)$ también es divisible entre n. □

Ejemplos.

- Dos números son congruentes modulo 2 si y solo si tienen la misma paridad. Las dos clases de equivalencia modulo 2 están formadas por los números pares y los números impares.
- Hay 4 clases de equivalencia de enteros modulo 4, representadas por los residuos 0, 1, 2 y 3.
  Las 4 clases de equivalencia son
  $\overline{0}$ = {...,-12,-8, -4,0,4,8,12,...} $\quad \overline{1}$ = {...,-11,-8,-3,1,5,9,13,...}
  $\overline{2}$ = {...,-10,-6,-2,2,6,10,14,...} $\quad \overline{3}$ = {...,-9,-5,-1,3,7,11,15,...}

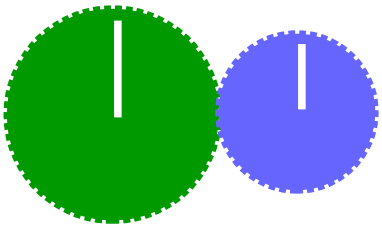
Lema 2. La relación de congruencia modulo $\mathbf{n}$ es compatible con la suma y el producto en $\mathbf{Z}$:
si $a \equiv b \pmod n$ y $c \equiv d \pmod n$ entonces $a+c \equiv b+d \pmod n$ y $a \cdot c \equiv b \cdot d \pmod n$.

Demostración. Si $a \equiv b \pmod n$ y $c \equiv d \pmod n$ entonces $a-b$ y $c-d$ son divisibles entre n, por lo tanto $(a+c)-(b+d) = (a-b)+(c-d)$ es divisible entre n, así que $a+c \equiv b+d \pmod n$.
Ademas $(a-b)\cdot c$ es divisible entre n y $b\cdot(c-d)$ es divisible entre n, por lo tanto $a\cdot c-b\cdot d = (a-b)\cdot c- b\cdot(c-d)$ es divisible entre n, así que $a\cdot c \equiv b\cdot d \pmod n$. □

Ejemplos.

- Como $2 \equiv 7 \pmod 5$ y $4 \equiv -6 \pmod 5$ entonces $2+4 \equiv 7-6 \pmod 5$ y $2 \cdot 4 \equiv 7 \cdot (-6) \pmod 5$.
- Si ahorita son las 9 entonces en 7 horas serán las 4, ya que $9+7 \equiv 4 \pmod{12}$
- Si hoy es martes entonces en 30 días será jueves, ya que $30 \equiv 2 \pmod 7$

Problemas.



1. Dos engranes E y F con m y n dientes respectivamente giran juntos ¿Después de cuantas vueltas de E y cuantas de F los dos engranes vuelven a la posición original, si...

a. m=20, n=30 ? b. m=21, n=30 ? c. m=20, n=31 ?

2. Si son las 3pm entonces dentro de 100 horas serán las __ y en 1000 horas serán las __

3. Si hoy es martes dentro de 100 días será ___ y dentro de 4321 días será ___
Si este año mi cumpleaños es el jueves, el próximo año será el ___

4. Demuestra que si $ac \equiv bc \pmod n$ con c y n primos relativos entonces $a \equiv b \pmod n$.
Muestra que esto puede fallar si m y n no son primos relativos.

5. Demuestra que si p es un numero primo entonces $ab \equiv 0 \pmod p$ si y solo si $a \equiv 0 \pmod p$ o $b \equiv 0 \pmod p$. Muestra que esto no es cierto si p no es primo.

Ecuaciones con congruencias.

Podemos preguntarmos cuales números enteros satisfacen alguna relación de congruencia.

Ejemplo. ¿Cuales números enteros satisfacen...

- $\mathbf{x} \equiv 3 \pmod 5$? los números que al dividirse entre 5 dejan residuo 3: ...-7,-2,3,8,13,...
- $2\mathbf{x} \equiv 0 \pmod 6$? los números que multiplicados por 2 son divisibles entre 6: ...-6,-3,0,3,6,...
- $4\mathbf{x} \equiv 1 \pmod 2$? ninguno, porque 4x-1 nunca es divisible entre 2
- $2\mathbf{x} = 3 \pmod 5$? los que multip. por 2 y divididos entre 5 dejan residuo 3: ...-6,-1,4,9,14,...
- $3\mathbf{x} = 2 \pmod 6$? ninguno porque 3x-2 nunca es divisible entre 6

En los ejemplos anteriores la ecuación $ax \equiv b \pmod n$ a veces tiene una infinidad de soluciones y otras veces no tiene ninguna. Podemos preguntarnos si esto siempre ocurre, y si habrá una manera de hallar las soluciones a estas ecuaciones que no sea adivinando.

Lema 4. Si **a** y **n** son primos relativos la congruencia $a\mathbf{x} \equiv b \pmod{\mathbf{n}}$ siempre tiene soluciones, y todas las soluciones son congruentes modulo n.

Demostración. $ax \equiv b \pmod n$ si y solo si existe y en **Z** tal que $ax+ny=b$. Esta ecuación tiene soluciones enteras si y solo si el mcd de a y n divide a b. Si a y n son primos relativos su mcd es 1 así que la ecuación tiene soluciones.

Si $ax_1 \equiv b \pmod n$ y $ax_2 \equiv b \pmod n$ son soluciones de la ecuación entonces $a(x_1-x_2) \equiv 0 \pmod n$. Esto dice que n divide a $a(x_1-x_2)$ y como a y n son primos relativos n debe dividir a (x_1-x_2) así que $x_1 \equiv x_2 \pmod n$.

Ejemplos

- ¿La ecuación $3\mathbf{x}\equiv 2 \pmod 5$ tiene soluciones? ¿Si las tiene, cuales son?

  Si tiene, ya que 3 y 5 son primos relativos.

  Una solución es x=-1. Las otras soluciones son suma de esa solución con soluciones de la ecuación homogénea $3x\equiv 0 \pmod 5$ que son ...,-10,-5,0,5,10,15,...)

  Así que las soluciones de la ecuación son x=...,-11,-6,-1,4,9,14,...

- ¿La ecuación $9\mathbf{x}\equiv 4 \pmod{11}$ tiene soluciones? ¿Si sí, cuales son?

  Si, como 9 y 11 son primos relativos, existe una combinación lineal entera de 9 y 11 que da 1

  $5\cdot 9-4\cdot 11=1$. Multiplicando por 4 obtenemos $20\cdot 9-16\cdot 11=4$,

  por lo tanto $4\equiv 20\cdot 9 \pmod{11}$ y una solución es x=20.

  Las otras soluciones se obtienen sumándole las soluciones de la ecuación homogénea $9x\equiv 0 \pmod{11}$ que son los múltiplos de 11. Así que las soluciones de la ecuación son x=...,-13,-2,9,20,31,42,...

Si a y n no son primos relativos, la congruencia $ax=b \pmod n$ puede tener o no tener solución, dependiendo de b, y las soluciones pueden ser o no ser congruentes modulo n.

Ejemplos.

- ¿La ecuación $2\mathbf{x}\equiv 3 \pmod 6$ tiene soluciones?

  No, $2\mathbf{x}-3$ nunca es divisible entre 6.

- ¿La ecuación $2\mathbf{x}\equiv 4 \pmod 6$ tiene soluciones ? Si: $\mathbf{x}=-1$ es solución.

  Las otras soluciones son la suma de esa con las soluciones de la homogéneas $2x\equiv 0 \pmod 6$, que son los múltiplos de 3. Así que las soluciones son ,...,-7-4,-1,2,5,8,...

  Observar que estas son las mismas soluciones de la ecuación $\mathbf{x}\equiv 2 \pmod 3$

Problemas.

6. ¿Existirá algún entero **x** tal que ...

   a. $4\mathbf{x}\equiv 3 \pmod 5$? b. $4\mathbf{x}\equiv 3 \pmod 6$?

   c. $3\mathbf{x}\equiv 4 \pmod 5$? d. $3\mathbf{x}\equiv 4 \pmod 6$?

   (basta dar uno o mostrar que no existe, se trata es hacerlo a pie, sin usar el lema 4)

7. Demuestra que la ecuación $ax\equiv b \pmod n$ tiene solución si y solo si b es divisible entre el mcd de a y n.

8. Encuentra todas las soluciones de las siguientes ecuaciones:

   a. $7\mathbf{x}\equiv 1 \pmod 3$ b. $3\mathbf{x}\equiv 0 \pmod 7$.

   c. $4\mathbf{x}\equiv 6 \pmod 7$ d. $5\mathbf{x}\equiv 4 \pmod 9$

   e. $9\mathbf{x}\equiv 7 \pmod{15}$ f. $18\mathbf{x}\equiv 11 \pmod{41}$

   (aquí si se vale usar el lema 4)

9. Muestra que si la ecuación $ax\equiv b \pmod n$ tiene soluciones, entonces tiene una menor que n.

10. Muestra lo siguiente*, sin hallar todas las soluciones:*

a. Las ecuaciones $3x \equiv 1 \pmod 7$ y $6x \equiv 2 \pmod 7$ tienen las mismas soluciones.

b. Las ecuaciones $2x \equiv 1 \pmod 6$ y $4x \equiv 2 \pmod 6$ no tienen las mismas soluciones.

c. Las ecuaciones $3x \equiv 2 \pmod 7$ y $5x \equiv 1 \pmod 7$ tienen las mismas soluciones.

Hint: para c, muestra que cada ecuación se puede multiplicar por un número para obtener la otra.

Sistemas de congruencias.

En el siglo III el matemático chino Sunzi propuso el siguiente problema:

> *Hay algunas cosas cuya cantidad desconocemos. Si las contamos de 3 en 3 sobran 2, si las contamos de 5 en 5 sobran 3 y si las contamos de 7 en 7 sobran 2 ¿Cuantas cosas son?*

Que en lenguaje moderno diría:

> *Hallar un numero entero que al dividirse entre 3 deje residuo 2, al dividirse entre 5 deje residuo 3 y al dividirse entre 7 deje residuo 2.*

En el siglo VI el hindú Aryabhata dio un algoritmo para resolver problemas de este tipo, y en el siglo XIII el chino Qin Jiushao dio la solución general.

En el siglo XVIII Gauss definió las congruencias, con las que el problema puede escribirse:

> *Hallar las soluciones del sistema*

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Podemos intentar atacar el problema con fuerza bruta, hallando las soluciones de cada ecuación y viendo que números están en su intersección:

$x \equiv 2 \pmod 3$ ...-7,-4,-1,2,5,8,11,14,17,20,23,...

$x \equiv 3 \pmod 5$ ...-12,-7,-2,3,8,13,18,23,28,33,...

$x \equiv 2 \pmod 7$ ...-19,-12,-5,2,9,16,23,30,37,44,...

Aquí 23 es la única solución común visible, podría haber muchas otras en las listas completas

¿Y que pasa si cambiamos la tercera ecuación y consideramos el siguiente sistema?

$x \equiv 2 \pmod 3$ ...-7,-4,-1,2,5,8,11,14,17,20,23,26,29,32,35,38,41,44...

$x \equiv 3 \pmod 5$ ...-12,-7,-2,3,8,13,18,23,28,33,38,43...

$x \equiv 4 \pmod 7$ ...-17,-10,-3,4,11,18,25,32,39,46,...

Aquí no se ve ninguna solución común, pero podría estar antes o después en las listas...

No es nada obvio cuando un sistema de ecuaciones en congruencias tiene soluciones.
La respuesta la da el siguiente resultado:

Teorema Chino de los Residuos. Si $n_1, n_2, n_3, \ldots, n_k$ son primos relativos, entonces el sistema de congruencias

- $$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \ldots\ldots \quad \ldots\ldots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

siempre tiene soluciones, y las soluciones son congruentes modulo $n_1n_2n_3\ldots n_k$.
En particular, existe exactamente una solución entre 0 y $n_1n_2n_3\ldots n_k$.

Demostración.

Veremos primero que si el sistema tiene soluciones, estas difieren por múltiplos de $n_1n_2n_3\ldots n_k$.

Si x_1 es una solución del sistema y $x_2 \equiv x_1 \pmod{n_1n_2n_3\ldots n_k}$ entonces x_2 también es solución del sistema ya que $x_2 \equiv x_1 \pmod{n_i}$ para cada i.

Y si x_1 y x_2 son soluciones del sistema, entonces $x_1-x_2 \equiv 0 \pmod{n_i}$ para cada i, así que x_1-x_2 es divisible entre cada n_i. Como los n_i son primos relativos, esto implica que x_1-x_2 es divisible entre el producto de todos los n_i, así que $x_1 \equiv x_2 \pmod{n_1n_2n_3\ldots n_k}$.

Para ver que estos sistemas siempre tienen soluciones consideremos primero un sistema de 2 ecuaciones:

$x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2}$

Sabemos que la primera ecuación tiene soluciones, que son de la forma $x = a_1+n_1y$ para y en **Z**.

Sustituyendo este valor de x en la segunda ecuación obtenemos

$a_1+n_1y \equiv a_2 \pmod{n_2}$ así que $n_1y \equiv a_2-a_1 \pmod{n_2}$

Como n_1 y n_2 son primos relativos, entonces esta ecuación tiene soluciones.

Si y_1 es una solución entonces $x = a_1+n_1y_1$ es solución de la primera ecuación y también

$x = a_1+n_1y_1 \equiv a_1+(a_2-a_1) \equiv a_2 \pmod{n_2}$ así que x también es solución de la segunda ecuación

Ahora podemos proceder por inducción en el numero de ecuaciones.

Supongamos que todo sistema de k ecuaciones tiene soluciones, que difieren por múltiplos de los k módulos, y consideremos un sistema de k+1 ecuaciones.

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \ldots\ldots \quad \ldots\ldots \\ x \equiv a_k \pmod{n_k} \\ x \equiv a_{k+1} \pmod{n_{k+1}} \end{cases}$$

Por hipótesis de inducción, el sistema formado por la primeras k ecuaciones tiene soluciones, que son de la forma $x = a+n_1n_2\ldots n_ky$ para y en **Z**.

Sustituyendo en la ultima ecuación obtenemos

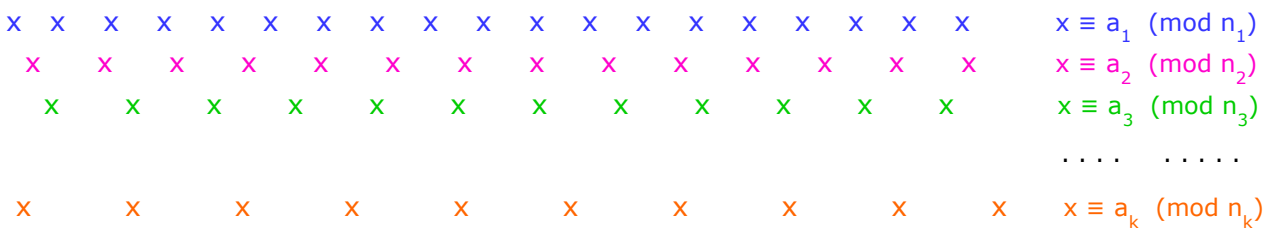
$a+n_1n_2...n_ky \equiv a_{k+1} \pmod{n_{k+1}}$ así que $n_1n_2...n_ky \equiv a_{k+1} - a \pmod{n_{k+1}}$

Como $n_1n_2...n_k$ y n_{k+1} son primos relativos, entonces esta ecuación tiene soluciones.

Si y es una solución entonces $x= a+n_1n_2...n_ky$ es una solución de las primeras k ecuaciones y también $x = a+n_1n_2...n_ky \equiv a+(a_{k+1}-a) \equiv a_{k+1} \pmod{n_{k+1}}$ así que x también es solución de la ultima ecuación. □

Una manera de visualizar el teorema chino de los residuos.

Si tenemos un sistema de ecuaciones $x \equiv a_i \pmod{n_i}$ $i=1,2,...,k$ entonces cada ecuación tiene una infinidad de soluciones, que son de la forma a_i+mn_i para m en $\mathbf{Z}$, asi que están distribuidas periódicamente en $\mathbf{Z}$ como las x en cada renglón de este dibujo:



Las x en el renglón i están a distancia n_1 y desplazadas a_1. Las soluciones del sistema están donde las x en todos los renglones están alineadas verticalmente (en el dibujo no se ven). El teorema dice que si las distancias en los renglones son primos relativos, entonces siempre hay alineaciones verticales, sin importar como sean los desplazamientos y que las alineaciones verticales ocurren periódicamente a distancia $n=n_1 n_2...n_k$.

Ejemplo. Hallar las soluciones del sistema

$$\begin{cases} x \equiv 5 \pmod{9} \\ x \equiv 2 \pmod{13} \end{cases}$$

Las soluciones de la primera ecuación son de la forma $x = 5+9y$ para y en $\mathbf{Z}$.

Sustituyendo esto en la segunda ecuación obtenemos

$5+9y \equiv 2 \pmod{13}$ que equivale a $9y \equiv -3 \pmod{13}$. Una solución es $y = -9$

Por lo tanto una solución del sistema original es $x = 5+9y = 5-81 = -76$.

Y todas las soluciones son $x = -76+107n$ para y en $\mathbf{Z}$.

Ejemplo. Encuentra las soluciones del sistema

$$\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 7 \pmod{12} \\ x \equiv 5 \pmod{13} \end{cases}$$

El sistema debe tener una solución entre 0 y $11\cdot12\cdot13=1716$. Podemos hallarla como sigue:

Las soluciones de la primera ecuación son $x=11y+1$ para y en $\mathbf{Z}$.

Sustituyendo este valor de x en la segunda ecuación queda

$11y+1 \equiv 7 \pmod{12}$ que equivale a $11y \equiv 6 \pmod{12}$ que equivale a $-y \equiv 6 \pmod{12}$

las soluciones de esta ecuación son $y=-6+12z$ para z en $\mathbf{Z}$, sustituyendo en x queda

$x = 11y+1 = 11(-6+12z)+1 = 132z-65$

Sustituyendo este valor de x en la tercera ecuación queda

$132z-65 \equiv 5 \pmod{13}$ simplificando queda
$2z \equiv 5 \pmod{13}$ multiplicando por 7 da
$14z \equiv 35 \pmod{13}$ y simplificando queda
$z \equiv 9 \pmod{13}$

cuyas soluciones son $z=9+13m$. Sustituyendo este valor de z en x queda
$x = 132z-65 = 132(9+13m)-65 = 1123+1716m$, con m en $\mathbf{Z}$.
La solución positiva mas pequeña (el único valor de x entre 0 y 1716) es 1188, lo que puede comprobarse dividiendo 1188 entre 11, 12 y 13.

Problemas.

11. Encontrar todas las soluciones de los sistemas de congruencias

a. $\begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 6 \pmod{11} \end{cases}$

b. $\begin{cases} x \equiv 1 \pmod{9} \\ x \equiv 4 \pmod{11} \\ x \equiv 2 \pmod{20} \end{cases}$

12. Hallar el número natural mas pequeño que dividido entre 17 deja residuo 5 y dividido entre 19 deja residuo 8. (usando el teorema chino, no la fuerza bruta)

13. ¿Cual es el número mas cercano a 1000 que al dividirse entre 7 deja residuo 2, al dividirse entre 9 deja residuo 3 y al dividirse entre 11 deja residuo 4?

14. Hallar todas las soluciones (ojo con los módulos)

a. $\begin{cases} x \equiv 3 \pmod{6} \\ x \equiv 7 \pmod{10} \end{cases}$

b. $\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 7 \pmod{9} \end{cases}$

15. Hallar todas las soluciones del sistema de congruencias

$$\begin{cases} 4x \equiv 2 \pmod{11} \\ 5x \equiv 6 \pmod{17} \end{cases}$$

hint: cambiar las congruencias por otras equivalentes donde los coeficientes de x sean 1

Los enteros modulo n.

Para cada $n>1$ hay n clases de congruencia de enteros módulo n, correspondientes a los residuos $0,1,2,3,...,n-1$, y que denotaremos por $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, ..., $\overline{n-1}$.

Al conjunto de clases de congruencia modulo **n** se le denota por $\mathbf{Z}_n$.
Observar que $\overline{a}=\overline{b}$ en $\mathbf{Z}_n \Leftrightarrow a\equiv b \pmod{\mathbf{n}} \Leftrightarrow n|a-b$.

Los elementos de $\mathbf{Z}_n$ pueden sumarse y multiplicarse: la suma y producto modulo n están bien definidas porque si $a\equiv b \pmod{\mathbf{n}}$ y $c\equiv d \pmod{\mathbf{n}}$ entonces $a+c\equiv b+d \pmod{\mathbf{n}}$ y $ac\equiv bd \pmod{\mathbf{n}}$.

Ejemplo. $\mathbf{Z}_5$ tiene 5 elementos: $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$. Las tablas de la suma y multiplicación en $\mathbf{Z}_5$ son:

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

En la tabla de la suma en cada renglón aparecen los mismos números pero recorridos.

En la multiplicación en cada renglón aparecen todos los números, pero en distintos ordenes.

Ejemplo. $\mathbf{Z}_6$ tiene 6 elementos: $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$. Las tablas de la suma y multiplicación en $\mathbf{Z}_6$:

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

La tabla de la suma en $\mathbf{Z}_6$ se parece a la de $\mathbf{Z}_5$: en cada renglón están todos los números pero recorridos.

La tabla de la multiplicación es muy distinta: en algunos renglones solo aparecen algunos números, estos están repetidos y el 0 aparece como producto de números distintos de 0.

Teorema. Para cada $\mathbf{n}>1$, $\mathbf{Z}_n$ es un anillo conmutativo con unidad.

Demostración. Hay que ver que la suma y el producto que definimos en $\mathbf{Z}_n$ cumplen las propiedades de las operaciones en un anillo. La suma y el producto modulo **n** son asociativas y conmutativas ya que la suma y el producto de números en **Z** lo son. El producto modulo **n** se distribuye con la suma modulo **n** ya que el producto en **Z** se distribuye con la suma en **Z**.

En $\mathbf{Z}_n$ el neutro aditivo es $\overline{0}$, el neutro multiplicativo es $\overline{1}$ y el inverso aditivo de $\overline{a}$ es $\overline{n-a}$. □

Decimos que un elemento $a\neq 0$ de un anillo **A** es un **divisor de 0** si existe un elemento $b\neq 0$ en **A** tal que $ab=0$.

Ejemplos:

- **Z** no tiene divisores de 0.
- $\mathbf{Z}_5$ no tiene divisores de 0.
- $\mathbf{Z}_6$ si tiene divisores de 0: son $\overline{2}$, $\overline{3}$ y $\overline{4}$.

Lema. En $\mathbf{Z}_n$, $\overline{m}$ es un divisor de 0 si y solo si el mcd de m y n es mayor que 1.

Demostración. Tomemos $\overline{m}\neq\overline{0}$ en $\mathbf{Z}_n$.

Si $\overline{m}\cdot\overline{r}=\overline{0}$ en $\mathbf{Z}_n$ entonces $n|mr$. Así que si m y n son primos relativos $n|r$ y esto dice que $\overline{r}=0$ en $\mathbf{Z}_n$, por lo tanto $\overline{m}$ no es un divisor de 0.

Si el mcd de m y n es $d>1$, entonces $m=ad$ y $n=bd$ para algunos a y b menores que n. Entonces $\overline{b}\neq 0$ en $\mathbf{Z}_n$ pero $\overline{m}\cdot\overline{b} = \overline{ad}\cdot\overline{b} = \overline{a}\cdot\overline{db} = \overline{a}\cdot\overline{bd} = \overline{a}\cdot\overline{n} = \overline{0}$ en $\mathbf{Z}_n$ lo que dice que $\overline{m}$ es un divisor de 0. □

Ejemplo. En $\mathbf{Z}_{20}$ los son divisores de 0 son $\overline{2}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{8}$, $\overline{10}$, $\overline{12}$, $\overline{14}$, $\overline{15}$, $\overline{16}$ y $\overline{18}$.

Un **dominio entero** es un anillo conmutativo donde el producto de dos elementos distintos de 0 es distinto de 0, es decir, donde no hay divisores de 0.

Lema. En un dominio entero vale la cancelación: si $ab=ac$ y $a\neq 0$, entonces $b=c$.

Demostración. Si $ab=ac$ entonces $a(b-c)=0$. En un dominio entero el producto solo puede ser 0 si uno de los factores es 0. Si $a\neq 0$ entonces $b-c=0$ por lo tanto $b=c$. □

Lema. $\mathbf{Z}_n$ es un dominio entero si y solo si **n** es un número primo.

Demostración. Si **n** es primo y $\overline{a}\cdot\overline{b}=\overline{0}$ en $\mathbf{Z}_n$ entonces $n|ab$ y como **n** es primo entonces $n|a$ o $n|b$, lo que dice que $\overline{a}=\overline{0}$ o $\overline{b}=\overline{0}$ en $\mathbf{Z}_n$.

Si **n** no es primo, $n=ab$ para un par de enteros positivos $a,b<n$. Entonces $\overline{a}\neq\overline{0}$ y $\overline{b}\neq\overline{0}$ en $\mathbf{Z}_n$ pero $\overline{a}\cdot\overline{b}=\overline{0}$ en $\mathbf{Z}_n$ así que $\overline{a}$ y $\overline{b}$ son divisores de $\overline{0}$. □

Problemas.

16. Calcula la tabla de multiplicar de $\mathbf{Z}_7$ y la de $\mathbf{Z}_8$.

17. Encuentra los divisores de 0 en $\mathbf{Z}_{21}$ y di por cuanto hay que multiplicarlos para obtener 0.

18. ¿$\mathbf{Z}_{129}$ es un dominio entero? ¿y $\mathbf{Z}_{131}$? Explica.

19. ¿Es cierto que en un anillo conmutativo el producto de divisores de 0 es divisor de 0?
¿Y que la suma de divisores de 0 es un divisor de 0?

20. Demuestra que si en un anillo conmutativo A vale la cancelación para el producto entonces A es un dominio entero.

La multiplicación en $\mathbf{Z}_n$.

Si m es primo relativo con $\mathbf{n}$, entonces al multiplicar a $\overline{m}$ por todos los elementos de $\mathbf{Z}_n$ quedan elementos *distintos* de $\mathbf{Z}_n$ ya que si $\overline{m}\cdot\overline{a} = \overline{m}\cdot\overline{b}$ en $\mathbf{Z}_n$ entonces $\overline{m}\cdot(\overline{a}-\overline{b})= \overline{0}$ en $\mathbf{Z}_n$ así que $n|m(a-b)$ y como m y n son primos relativos entonces $n|a-b$ así que $\overline{a} = \overline{b}$ en $\mathbf{Z}_n$.

Esto dice que en la tabla de multiplicar de $\mathbf{Z}_n$ el renglón correspondiente a m tiene n números *distintos*, por lo que deben aparecer todos: $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, ..., $\overline{n-1}$.

Si m y n *no* son primos relativos, y su mcd es d, entonces todos los múltiplos de m son múltiplos de d, por lo que al multiplicar por $\overline{m}$ solo aparecen múltiplos de $\overline{d}$. Debe aparecer $\overline{d}$ (ya que existen enteros a y b tales que $am+bn=d$ por lo que $\overline{a}\cdot\overline{m}=\overline{d}$ y por lo tanto aparecen todos los múltiplos de $\overline{d}$ y cada uno aparece repetido d veces.

Recordar que si $\mathbf{A}$ es un anillo conmutativo entonces un *inverso multiplicativo* de un elemento a es un elemento b tal que $ab=1$. Los inversos multiplicativos en un anillo conmutativo son únicos, ya que si $ab=1$ y $ac=1$ entonces $b=1b=(ac)b=a(cb)=a(bc)=(ab)c=1c=c$ así que $b=c$.

Lema. En $\mathbf{Z}_n$ la clase $\overline{a}$ tiene inverso si y solo si a y n son primos relativos.

Demostración.

$\Rightarrow$ Si existe $\overline{b}$ en $\mathbf{Z}_n$ tal que $\overline{a}\cdot\overline{b}=\overline{1}$ entonces $n|ab-1$, así que existe m tal que $ab-1=mn$, por lo que 1 es una combinación lineal entera de a y n, así que a y n son primos relativos. □

$\Leftarrow$ Si a y n son primos relativos entonces existe una combinación lineal entera $ab+mn=1$ así que $\overline{a}\cdot\overline{b}=\overline{1}$ en $\mathbf{Z}_n$ y esto dice que $\overline{b}$ es inverso de $\overline{a}$.

Ejemplos:

- En $\mathbf{Z}_7$ todos los elementos distintos de 0 tienen inversos. Podemos hallar el inverso de cada $\overline{m}$ hallando la combinación lineal de 7 y m da 1: para $\overline{m}=\overline{5}$, $(3)5-2(7)=1$ así que $3\cdot5\equiv1 \pmod 7$ y esto dice que el inverso de $\overline{5}$ es $\overline{3}$.

- En $\mathbf{Z}_{12}$ los elementos $\overline{1},\overline{5},\overline{7},\overline{11}$ tienen inversos, los elementos $\overline{2},\overline{3},\overline{4},\overline{6},\overline{8},\overline{9},\overline{10}$ son divisores de 0, por lo que no pueden tener inversos.

- ¿En $\mathbf{Z}_{37}$ cual es el inverso multiplicativo de $\overline{16}$?

  Por el algoritmo de Euclides
  $37 = 16\cdot 2+5$
  $16 = 5\cdot 3+1$
  $1 = 16-5\cdot 2 = 16-(37-16\cdot 2)\cdot 3 = 16\cdot 7-37\cdot 3$
  así que $16\cdot 7 \equiv 1 \pmod{37}$ y el inverso de $\overline{16}$ es $\overline{7}$.

Un **campo** es un anillo conmutativo donde cada elemento distinto de 0 tiene un inverso multiplicativo. Los números reales forman un campo, los racionales forman otro, los enteros no.

Todos los campos son dominios enteros, ya que si $ab=0$ y $a\neq 0$, entonces podemos multiplicar la igualdad por el inverso multiplicativo de a y obtener $b=(a^{-1}a)b=a^{-1}(ab)=a^{-1}0=0$ así que $b=0$.
Pero hay muchos dominios enteros que no son campos, como $\mathbf{Z}$.

Corolario. Si $\mathbf{p}$ es un número primo entonces $\mathbf{Z}_p$ es un campo.

Demostración. Ya sabemos que cada $\mathbf{Z}_n$ es un anillo conmutativo con unidad. Falta ver que si $\mathbf{p}$ es primo entonces cada $\overline{a}\neq 0$ en $\mathbf{Z}_p$ tiene un inverso multiplicativo. Esto se sigue del lema anterior porque si $\mathbf{p}$ es primo todos los números entre 1 y $p-1$ son primos relativos con $\mathbf{p}$. □

Observar que en los campos existe la división, que se define para $b\neq 0$ como $a\div b=a\cdot b^{-1}$.

Ejemplo: $\mathbf{Z}_2$ es un campo con solo 2 elementos.

Ejemplo: $\mathbf{Z}_5$ es un campo, así que en $\mathbf{Z}_5$ podemos dividir entre números distintos de 0:

$\overline{1}\div\overline{2} = \overline{3}$ ya que $\overline{2}\times\overline{3} = \overline{1}$ en $\mathbf{Z}_5$
$\overline{1}\div\overline{4} = \overline{4}$ ya que $\overline{4}\times\overline{4} = \overline{1}$ en $\mathbf{Z}_5$
$\overline{2}\div\overline{3} = \overline{4}$ ya que $\overline{3}\times\overline{4} = \overline{2}$ en $\mathbf{Z}_5$
$\overline{3}\div\overline{4} = \overline{2}$ ya que $\overline{4}\times\overline{2} = \overline{3}$ en $\mathbf{Z}_5$

Ecuaciones lineales.

Si $\mathbf{A}$ es un anillo conmutativo, una **ecuación lineal** en $\mathbf{A}$ es una ecuación de la forma $ax+b=0$ donde a y b son elementos de $\mathbf{A}$, $a\neq 0$ y la incógnita x es un elemento desconocido en $\mathbf{A}$.

La existencia de soluciones para las ecuaciones lineales depende del anillo:

- En un campo cada ecuación lineal $ax+b=0$ tiene exactamente una solución: $x=-b\div a$.
- En otros anillos la ecuación lineal $ax+b=0$ puede tener una solución o tener varias o no tener ninguna, dependiendo de los coeficientes.

Ejemplos. Considerar la ecuación $4x+6 = 0$ en distintos anillos

- En $\mathbf{Q}$ tiene una solución $x=-6/4$.
- En $\mathbf{Z}$ no tiene solución, porque 6 no es divisible entre 4.
- En $\mathbf{Z}_7$ tiene una solución $x = \overline{4}^{-1}\cdot(-\overline{6}) = \overline{2}\cdot\overline{1} = \overline{2}$
- En $\mathbf{Z}_8$ no tiene soluciones porque el mcd de 4 y 8 no divide a 6
- En $\mathbf{Z}_9$ tiene una solución: $x=3$
- En $\mathbf{Z}_{10}$ tiene 2 soluciones: $x=1$ y $x=6$

Problemas.

21. Encuentra los inversos multiplicativos de $\overline{3}$, $\overline{5}$ y $\overline{9}$ en $\mathbf{Z}_{16}$.

22. Has las siguientes operaciones en el campo $\mathbf{Z}_{11}$

a. $\overline{1}\div\overline{4}$ b. $\overline{1}\div\overline{9}$ c. $\overline{2}\div\overline{5}$ d. $\overline{3}\div\overline{7}$ e. $\overline{8}\div\overline{6}$

23. Encuentra todos los números en $\mathbf{Z}_{12}$ tales que

a. multiplicados por $\overline{7}$ dan $\overline{5}$ b. multiplicados por $\overline{3}$ dan $\overline{5}$ c. multiplicados por $\overline{10}$ dan $\overline{4}$

24. Encuentra las soluciones de las ecuaciones a. $4x+11\equiv 0$ y b. $8x-10=0$ en $\mathbf{Z}_{13}$. (las respuestas al tanteo no cuentan)

25. Encuentra un $\mathbf{Z}_n$ donde la ecuación lineal $6x+4=0$ tenga

a. una solución b. ninguna solución c. mas de una solución

Aritmética modular.

La aritmética de los enteros modulo n es algunos aspectos mas sencilla que la aritmética de los enteros, pero tiene sus sorpresas.

Si $a\equiv b \pmod n$ entonces $ac\equiv bc \pmod n$ para toda c en $\mathbf{Z}$ por lo tanto $a^r\equiv b^r \pmod n$ para toda r.

¿Será cierto que si $a\equiv b \pmod n$ entonces $r^a\equiv r^b \pmod n$?

Ejemplo: $1\equiv 5 \pmod 4$

$3^1\equiv 3$, $3^5\equiv 243$ y $3\equiv 243 \pmod 4$ así que $3^1\equiv 3^5 \pmod 4$.

$2^1\equiv 2$, $2^5\equiv 32$ y $2\not\equiv 32 \pmod 4$ así que $2^1\not\equiv 2^5 \pmod 4$.

Las potencias de un número módulo n deben repetirse periódicamente porque solo hay n residuos distintos, pero no tienen que repetirse con el periodo del módulo.

Calcular las potencias en $\mathbf{Z}_n$ es mas fácil que calcular las potencias en $\mathbf{Z}$ porque solo tenemos que multiplicar los residuos modulo n.

Ejemplos:

Las potencias de 7 en $\mathbf{Z}_9$:

$\overline{7}^0=\overline{1}$

$\overline{7}^1=\overline{7}$

$\overline{7}^2=\overline{4}$

$\overline{7}^3=\overline{1}$

$\overline{7}^4=\overline{7}$

$\overline{7}^5=\overline{4}$

$\overline{7}^6=\overline{1}$

Las potencias de 7

se repiten con periodo 3.

.

Las potencias de 7 en $\mathbf{Z}_{10}$:

$\overline{7}^0=\overline{1}$

$\overline{7}^1=\overline{7}$

$\overline{7}^2=\overline{9}$

$\overline{7}^3=\overline{3}$

$\overline{7}^4=\overline{1}$

$\overline{7}^5=\overline{7}$

$\overline{7}^6=\overline{9}$

$\overline{7}^7=\overline{3}$

$\overline{7}^8=\overline{1}$

$\overline{7}^9=\overline{7}$

las potencias de 7

se repiten con periodo 4

Las potencias de 7 en $\mathbf{Z}_{11}$:

$\overline{7}^0=\overline{1}$

$\overline{7}^1=\overline{7}$

$\overline{7}^2=\overline{9}$

$\overline{7}^3=\overline{3}$

$\overline{7}^4=\overline{1}$

$\overline{7}^5=\overline{7}$

$\overline{7}^6=\overline{9}$

$\overline{7}^7=\overline{3}$

$\overline{7}^8=\overline{1}$

$\overline{7}^9=\overline{7}$

$\overline{7}^{10}=\overline{7}$

$\overline{7}^{11}=\overline{7}$

las potencias de 7

se repiten con periodo 10

¿Como se pueden explicar los periodos de las potencias mod n? ¿Tienen alguna relación con el módulo?

Teorema pequeño de Fermat. Si p es un numero primo entonces $a^p \equiv a \pmod p$ para todo a.

Corolarios:

- Si p es primo y p no divide a a entonces $a^{p-1} \equiv 1 \pmod p$.

  Esto es cierto porque entonces a y p son primos relativos, asi que a tiene un inverso mod p, y multiplicando $a^{p-1} \equiv 1 \pmod p$ por el inverso de a obtenemos el resultado.
- Si p es primo, el periodo de repetición de las potencias de a en $\mathbf{Z}_p$ divide a $p-1$.

  Como $a^0 \equiv 1$ y $a^{p-1} \equiv 1$ las potencias de a se repiten después de $p-1$ pasos. Y el periodo de repetición mínimo debe dividir a cualquier periodo de repetición, porque si no se repetirían después del residuo.

Observación. Si n no es primo $a^n \equiv a \pmod n$ puede ser cierta o no dependiendo de a y n.

Ejemplos:

- $2^5 \equiv 2 \pmod 5$
- $3^7 \equiv 3 \pmod 7$
- $4^6 \equiv 4 \pmod 6$
- $5^6 \not\equiv 5 \pmod 6$

Hay muchas demostraciones del teorema pequeño de Fermat, una sencilla usa el siguiente lema:

Lema. Si p es un número primo entonces $(a+b)^p \equiv a^p+b^p \pmod p$ para todos a,b en $\mathbf{Z}$.

Demostración. Por el Teorema del binomio*

$$(a+b)^n \equiv a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 +\ldots+ \binom{n}{k} a^{n-k}b^k +\ldots+ \binom{n}{n-1} ab^{n-1} + b^n$$

donde $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$

Basta ver que todos los coeficientes de los términos donde aparecen a y b son divisibles entre n.

El número n aparece en el numerador de $\frac{n!}{k!\,(n-k)!}$ y todos los números en el denominador son menores a n. El cociente es un entero, que se obtiene cancelando los factores primos comunes en el numerador y el denominador. Si n es primo entonces n aparece entre los factores primos del numerador pero no aparece entre los factores primos del denominador, por lo tanto sobrevive a la cancelación y el resultado es divisible entre n. □

* Quienes no recuerden el teorema del binomio pueden ver: https://www.matem.unam.mx/~max/AS1/N5.pdf pagina 9

Demostración del teorema pequeño de Fermat. Por inducción sobre a.

Base de inducción. $1^p=1 \pmod p$.

Paso de inducción. Supongamos que el teorema vale para a y probemos que vale para $a+1$:

Si $a^p \equiv a \pmod p$ entonces por el lema anterior $(a+1)^p \equiv a^p +1^p \pmod p$.

Y por hipótesis de inducción $a^p +1^p \equiv a+1 \pmod p$ asi que ya acabamos. □

El test de primalidad de Fermat es un procedimiento para tratar de adivinar si un número n es primo, usando el teorema pequeño de Fermat:

Elegir al azar un número a menor que n, calcular $a^{n-1} \pmod n$.

- Si el resultado *no* es 1 el numero n *no* es primo.
- Si el resultado es 1 el numero n *puede ser* primo.

Observar que si $a^{n-1} \equiv 1 \pmod n$ entonces a y n son primos relativos. Así que si n no es primo siempre hay valores de a para los que $a^{n-1} \not\equiv 1 \pmod n$. Y muchas veces $a^{n-1} \not\equiv 1 \pmod n$ aunque a y n sean primos relativos. Así que si repetimos el test muchas veces eligiendo a al azar y el resultado es siempre 1 entonces es *muy probable* que n sea primo.

Problemas.

26. a. Calcula las potencias de 4 modulo 13. ¿Con que periodo se repiten?
    b. Calcula las potencias de 7 modulo 13. ¿Con que periodo se repiten?

27. Calcula: a. $100^{100} \pmod 3$ b. $3^{99} \pmod 7$ c. $7^{91} \pmod 8$ *no trabajen de mas!*

28. ¿Para cuales valores de a se tiene que $a^8 \not\equiv a \pmod 8$? ¿Y que $a^{12} \not\equiv a \pmod{12}$?

29. Muestra que si n no es primo entonces la congruencia $(a+b)^n \equiv a^n+b^n \pmod n$ puede fallar.

Cuadrados y raíces cuadradas.

Para saber cuales números tienen raíces cuadradas en $\mathbf{Z}_n$ necesitamos saber como son los cuadrados de todos los números en $\mathbf{Z}_n$.

Ejemplos.

En $\mathbf{Z}_{11}$	En $\mathbf{Z}_{12}$	En $\mathbf{Z}_{13}$
$0^2 = 0$	$0^2 = 0$	$0^2 = 0$
$1^2 = 1$	$1^2 = 1$	$1^2 = 1$
$2^2 = 4$	$2^2 = 4$	$2^2 = 4$
$3^2 = 9$	$3^2 = 9$	$3^2 = 3$
$4^2 = 5$	$4^2 = 4$	$4^2 = 3$
$5^2 = 3$	$5^2 = 1$	$5^2 = 12$
$6^2 = 3$	$6^2 = 0$	$6^2 = 10$
$7^2 = 5$	$7^2 = 1$	$7^2 = 10$
$8^2 = 9$	$8^2 = 4$	$8^2 = 12$
$9^2 = 4$	$9^2 = 9$	$9^2 = 3$
$10^2 = 1$	$10^2 = 4$	$10^2 = 9$
	$11^2 = 1$	$11^2 = 4$
		$12^2 = 1$

Los cuadrados en $\mathbf{Z_{11}}$ son 0, 1, 3, 4, 5 y 9. 0 tiene una raíz, 1, 3, 4, 5 y 9 tienen dos raíces cada uno.

Los cuadrados en $\mathbf{Z_{12}}$ son 0, 1, 4 y 9. 0 y 9 tienen dos raíces, 1 y 4 tienen cuatro raíces.

Los cuadrados en $\mathbf{Z_{13}}$ son 0, 1, 3, 4, 9, 10 y 12. 0 tiene una raíz, 1, 3, 4, 9, 10 y 12 tienen dos raíces.

Lema. En $\mathbf{Z}_p$ con p primo cada número a tiene a lo mas 2 raíces cuadradas.

Demostración. Si b y c son soluciones de la ecuación $x^2 \equiv a \pmod p$ entonces $b^2 \equiv c^2 \pmod p$ así que $b^2 - c^2 \equiv 0 \pmod p$. Por lo tanto $p|c^2-b^2=(c+b)(c-b)$ y como p es primo entonces $p|c+b$ o $p|c-b$.

Entonces $c+b \equiv 0 \pmod p$ o $c-b \equiv 0 \pmod p$ por lo tanto $c \equiv -b \pmod p$ o $c \equiv b \pmod p$. □

Corolario. En $\mathbf{Z}_p$ con un p primo impar, la mitad de los números distintos de 0 tienen raíces cuadradas.

Demostración. Si b es raíz de un número a en $\mathbf{Z}_p$ entonces -b también es raíz de a, y por el lema anterior a no puede tener otras raíces. Así que a tiene 2 raíces, excepto si $b \equiv -b$. Pero en este caso $2b \equiv 0$ asi que $p|2b$ y como p es un primo distinto de 2 entonces $p|b$, por lo tanto $b \equiv 0$, lo que dice que 0 es el único cuadrado con una sola raíz.

Así que la función $c : \mathbf{Z}_p - \{0\} \to \mathbf{Z}_p - \{0\}$ que envía cada número a su cuadrado es 2 a 1 y su imagen debe tener la mitad de elementos que el dominio. □

Factoriales en $\mathbf{Z}_n$.

Son mas fáciles de calcular que en $\mathbf{Z}$ porque solo hay que multiplicar los residuos modulo n.

Observar que $m! \equiv 0 \pmod{n}$ si $m \geq n$.

Ejemplos.

Factoriales en $\mathbf{Z}_6$:

$1! = 1$
$2! = 2$
$3! = 0$
$4! = 0$
$5! = 0$

Factoriales en $\mathbf{Z}_7$:

$1! = 1$
$2! = 2$
$3! = 6$
$4! = 3$
$5! = 1$
$6! = -1$
$7! = 0$

Factoriales en $\mathbf{Z}_9$:

$1! = 1$
$2! = 2$
$3! = 6$
$4! = 6$
$5! = 3$
$6! = 0$

Si n no es primo, podemos escribir $n=ab$ con $1<a,b<n$ así que a y b son factores de $(n-1)!$, por lo que $n=ab$ divide a $(n-1)!$ y por lo tanto $(n-1)! \equiv 0 \pmod{n}$.

Si n es primo entonces todos los números entre 1 y n son primos relativos con n así que $(n-1)!$ es primo relativo con n y por lo tanto $(n-1)! \not\equiv 0 \pmod{n}$.

Así que n es primo $\Leftrightarrow$ $(n-1)! \not\equiv 0 \pmod{n}$

Teorema de Wilson. Si p es primo entonces $(p-1)! = -1$ en $\mathbf{Z}_p$.

Demostración. Si p es primo, cada número a entre 1 y p es primo relativo con p y por lo tanto a tiene un inverso en $\mathbf{Z}_p$. El inverso de -1 es -1, pero el inverso de cualquier número a distinto de 1 y -1 es un número distinto de a (ya que si el inverso de a es a entonces a es una raíz cuadrada de 1, pero las únicas raíces cuadradas de 1 en $\mathbf{Z}_p$ con p primo son 1 y -1). Así que en el producto $1\cdot2\cdot3\cdot\ldots\cdot(p-1)$ aparece cada número y su inverso y se cancelan, y solo queda -1 (que solo aparece una vez en el producto). Por lo tanto $1\cdot2\cdot3\cdot\ldots\cdot(p-1) \equiv -1 \pmod{p}$. □

Problemas.

30. ¿-1 tiene raíces cuadradas en $\mathbf{Z}_{11}$? ¿-1 tiene raíces cuadradas en $\mathbf{Z}_{13}$? ¿Si si, cuales son?

31. a. Muestra que si p primo, los únicos números en $\mathbf{Z}_p$ cuyo cuadrado es 1 son 1 y -1.
    b. Muestra que esto puede fallar si p no es primo.

32. ¿Cuales números en $\mathbf{Z}_{11}$ tienen raíces cubicas?

33. Calcula a. 99! en $\mathbf{Z}_{101}$ b. 100! en $\mathbf{Z}_{1001}$

34. ¿Si n es primo, cuanto vale (n-2)! (mod n)? ¿Y si n no es primo?