Curso de Iniciación Científica para Jóvenes Talentos
Nivel Pre-Avanzado
Teoría de números

1. Aritmética Modular

Supongamos que numeramos los días de la semana usando los números del 0 al 6, comenzando con el domingo. Si continuamos numerando, el día 7 es domingo nuevamente, el día 8 es lunes, y así sucesivamente. En cierto sentido, podemos pensar que $7 = 0$, $8 = 1$, etc., donde "=", obviamente, no tiene el mismo sentido usual. También podemos trabajar hacia atrás: el día -1 es sábado, el día -2 es viernes, etc. Así, $-1 = 6$, $-2 = 5$. No es difícil encontrar un patrón para los números correspondientes a cada día, dicho patrón se ilustra en la siguiente tabla:

Domingo	números de la forma $7n$
Lunes	números de la forma $7n + 1$
Martes	números de la forma $7n + 2$
Miércoles	números de la forma $7n + 3$
Jueves	números de la forma $7n + 4$
Viernes	números de la forma $7n + 5$
Sábado	números de la forma $7n + 6$

Notamos que los números de la forma $7n + 7$, son de la forma $7(n + 1)$ (y por tanto son de la forma $7n$). Entonces, el día que le corresponde a un número entero cualquiera está determinado por el residuo al dividir el número entre 7. Por ejemplo, el día que le corresponde al número 38 es el miércoles (ya que $38 = 7 \cdot 5 + 3$). Estos residuos son siempre $0, 1, 2, 3, 4, 5, 6$. Es posible definir una *aritmética de residuos*. Podemos acordar que $4 + 5 = 2$, esto signidica que el día 4 más 5 días es el día 2, lo cual es bastante natural. De esta forma podemos construir la tabla para la suma de los números del 0 al 6 de la siguiente forma:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

1.1. Congruencias

Sea n un número natural y $a, b \in \mathbb{Z}$. Decimos que a es congruente a b módulo n y escribimos:

$$a \equiv b \pmod{n}$$

si $n|a-b$. Por ejemplo, tenemos que $17 \equiv 3 \pmod 7$ y $10 \equiv -5 \pmod 3$. Es claro que si r es el resto de la división de a con n, entonces $a \equiv r \pmod n$ ($a = nq + r \Rightarrow n|a - r \Rightarrow a \equiv r \pmod n$).

Problema 1.1. *Encontrar dos enteros positivos y dos enteros negativos que sean congruentes con* 21 *módulo* 6*.*

La relación "$\equiv$" en el conjunto $\mathbb{Z}$ de los enteros es llamada **relación de congruencia**, veamos algunas de sus propiedades:

Proposición 1.1 (Reflexibidad)**.** *$a \equiv a \pmod n$.*

Se sigue de que $n|0 = a - a$.

Proposición 1.2 (Simetría)**.** *Si $a \equiv b \pmod n$, entonces $b \equiv a \pmod n$.*

Tenemos $n|a - b \Leftrightarrow n|b - a$.

Proposición 1.3 (Transitividad)**.** *Si $a \equiv b \pmod n$ y $b \equiv c \pmod n$, entonces $a \equiv c \pmod n$.*

Por deficinición esto equuivale a $n|a - b$ y $n|b - c$ implica $n|(a - b) + (b - c) = a - c$.

Obs: Estas tres primeras propiedades dicen que la relación de congruencia es una relación de equivalencia.

Proposición 1.4 (Compatibilidad con la suma y la diferencia)**.** *Si $a \equiv b \pmod n$ y $c \equiv d \pmod n$ entonces*

$$a + c \equiv b + d \pmod n$$
$$a - c \equiv b - d \pmod n.$$

Tenemos que $n|a - b$ y $n|c - d$ entonces $n|(a - b) + (c - d) = (a + c) - (b + d)$, que implica la primera congruencia, además $n|(a - b) - (c - d) = (a - c) - (b - d)$ que implica la segunda.

Obs: La propiedad anterior nos dice que podemos sumar y restar "miembro a miembro".

Proposición 1.5. *Si $a \equiv b \pmod n$, entonces para cualquier entero k, $ak \equiv bk \pmod n$.*

Esto equivale a $n|a - b$ entonces $n|k(a - b)$.

Proposición 1.6 (Compatibilidad con el producto)**.** *Si $a \equiv b \pmod n$ y $c \equiv d \pmod n$ entonces*

$$ac \equiv bd \pmod n.$$

Tenemos que $n|a - b$ y $n|c - d$ entonces $n|c(a - b) + b(c - d) = ac - bd$.

Obs: La propiedad anterior no dice que podemos multiplicar "miembro a miembro".

Proposición 1.7. *Si $a_i \equiv b_i \pmod n$, $i = 1, \ldots, k$ entonces $a_1 + a_2 + \cdots + a_k \equiv b_1 + b_2 + \cdots + b_k \pmod n$ y $a_1 a_2 \cdots a_k \equiv b_1 b_2 \cdots b_k \pmod n$. En particular, si $a \equiv b \pmod n$, luego para cualquier entero positivo k, $a^k \equiv b^k \pmod n$.*

Las propiedades mostradas anteriormente muestran que la relación de congruencia tiene un comportamiento muy similar a la relación de igualdad usual. Frecuentemente surgen confusiones con estas propiedades y las propiedades de igualdad, realice el siguiente ejercicio:

Problema 1.2. *En cada uno de los siguientes casos, encuentre otro ejemplo que muestre que la afirmación es FALSA:*

1. *Si $a \equiv b \pmod n$ y $b \equiv c \pmod m$ entonces $a \equiv c \pmod n$. Ej: $1 \equiv 5 \pmod 4$ y $5 \equiv 2 \pmod 3$ pero $1 \not\equiv 2 \pmod 3$.*
2. *Si $ca \equiv cb \pmod n$, entonces $a \equiv b \pmod n$. Ej: $3 \cdot 5 \equiv 3 \cdot 1 \pmod{12}$ pero $5 \not\equiv 1 \pmod{12}$.*
3. *Si $a^k \equiv b^k \pmod n$, entonces $a \equiv b \pmod n$. Ej: $2^4 \equiv 3^4 \pmod 5$ pero $2 \not\equiv 3 \pmod 5$.*

Apreder a manejar las congruencias facilita mucho a la hora de resolver problemas de divisibilidad. Para hacer opercaciones (sumar y multiplicar) en una congruencia, cualquier cantidad puede sustituirse por otra a la que ésta es congruente sin alterar la validez de la congruencia, por ejemplo si queremos el resto de la división de $49 \cdot 12 + 57^6$ con 5 tenemos que $49 \cdot 12 + 57^6 \equiv 4 \cdot 2 + 2^6 \pmod 5$, donde hemos sustituido $49 \equiv 4$, $12 \equiv 2$ y $57 \equiv 2$ todos en (mod 5) y a su vez $4 \cdot 2 + 2^6 \equiv 8 + 64 \equiv 72 \equiv 2 \pmod 5$. Note que no hemos sustituido el exponente 6, pues este es simplemente un símbolo que representa que 57 debe ser multiplicado 6 veces (si bien $6 \equiv 1 \pmod 5$, $2^6 \not\equiv 2^1 \pmod 5$).

Ejemplo 1.1. *Probar que módulo 3 todo número es congruente con la suma de las cifras que lo forman. Deducir el criterio de divisibilidad por 3: "Un entero a es divisible por 3 exactamente cuando la suma de las cifras de a lo es'.'*

Solución. Sean $a_m, a_{m-1}, \ldots, a_1, a_0$ las cifras de a en este orden (o sea $a = a_m a_{m-1} \ldots a_1 a_0$). Entonces $a = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$. Como $10 \equiv 1 \pmod 3$, de la propiedad 4.7 tenemos que $10^k \equiv 1^k \pmod 3$ y multiplicando por a_k (lo que nos permite la propiedad 4.5) tenemos $a_k 10^k \equiv a_k \pmod 3$ para $k = 0, 1, \ldots, m$. Luego

$$a \equiv a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0 \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod 3.$$

Para probar el criterio de divisibilidad por 3 basta observar que los números divisibles por 3 son precisamente aquellos que son congruentes con 0 módulo 3 y que por lo anterior, un número es congruente con 0 módulo 3, si y sólo si la suma de sus cifras lo es □

Ejemplo 1.2. *Demostrar que* $31 | 20^{15} - 1$.

Solución. Esto es equivalente a mostrar que $20^{15} \equiv 1 \pmod{31}$. Para eso observemos que:

$$20 \equiv -11 (mod 31) \tag{1}$$

Y así $20^2 \equiv (-11)^2 \pmod{31}$ $20^2 \equiv 121 \equiv -3 \pmod{31}$, tenemos

$$20^2 \equiv -3 (mod 31) \tag{2}$$

Multiplicando (1) y (2) miembro a miembro, obtenemos $20^3 \equiv 33 \pmod{31}$ y como $33 \equiv 2 \pmod{31}$,

$$20^3 \equiv 2 \pmod{31}$$

Elevando a la quinta potencia, tenemos $20^{15} \equiv 2^5 \equiv 32 \equiv 1 \pmod{31}$, concluimos que $20^{15} \equiv 1 \pmod{31}$ □

Problema 1.3. *Demostrar que:*

1. $41 | 2^{20} - 1$
2. $61 | 20^{15} - 1$
3. $13 | 2^{70} + 3^{70}$

Problema 1.4. *Halle el residuo que queda al dividir* $1! + 2! + 3! + \cdots + 99!$ *entre* 12.

Problema 1.5. *Pruebe el criterio de divisibilidad por* 11. *"Un número a es divisible por* 11 *si y sólo si la diferencia de la suma de las cifras pares de a con la suma de las cifras impares es divisible entre* 11*".*

Problema 1.6. *Muestre que si un entero a no es divisible por* 2 *y* 3*, entonces* $a^2 \equiv 1 \pmod{24}$.

Problema 1.7. *Si* $m | a - b$*, demostrar que* $m | a^k - b^k$ *para todo k natural.*

Problema 1.8. *Si k es un número impar, demostrar que* $a + b | a^k + b^k$.

Problema 1.9. *Calcule el resto de la división de* $2^{2^{2011}}$ *por* 97.

Problema 1.10. *Muestre que el dígito de las decenas de cualquier potencia de* 3 *es un número par (por ejemplo, el dígito de las decenas de* $3^6 = 729$ *es* 2*).*

1.2. Clases de residuos

Dado un número natural n cada conjunto de números congruentes entre sí se llama **clase módulo n** y cualquier elemento de ese conjunto es un representante de la clase. Si a es cualquier representante de la clase, entonces la clase a la cual pertenece el número a se denota por $\overline{a}$. Así podemos escribir:

$$\overline{a} = \{a + kn; k \in \mathbb{Z}\}$$

Llamamos $\mathbb{Z}_n$ al conjunto de todas las clases módulo n. Sabemos que si $a \in \mathbb{Z}$, podemos dividirlo por n obteniendo q y r enteros tales que:

$$a = nq + r, \text{ con } 0 \leq r \leq n - 1$$

Luego $a \equiv r \pmod{n}$. Resulta que un entero cualquiera es congruente en módulo n a algún entero en el intervalo 0 a $n-1$. En otras palabras, el cunjunto $\mathbb{Z}_n$ está formado por las clases $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$. Además todas estas clases son distintas entre sí, la única manera de que dos números entre 0 y $n-1$ sean congruentes módulo n es que sean iguales.

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

Así por ejemplo analicemos el conjunto $\mathbb{Z}_7$ de las clases en módulo 7, la cual consta de 7 elementos:

$$\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$$

Cada uno de estos elementos es un conjunto de enteros, $\overline{0}$ contiene todos los múltiplos de 7, $\overline{1}$ contiene todos los números de la forma $7k+1$, con $k \in \mathbb{Z}$, la clase $\overline{16}$ está representada por $\overline{2}$, pues todos los números de la forma $7k + 16$ son $7(k + 2) + 2$, o sea son de la forma $7k + 2$ y

$$\overline{5} = \{7k + 5; k \in \mathbb{Z}\} = \{\ \ldots, \text{-16,-9,-2,5,12,19,}\ldots\}$$

El número 144, al dividirlo con 7 obtenemos $144 = 7 \cdot 20 + 4$, o sea $144 \equiv 4 \pmod{7}$, por lo tanto 144 pertenece a la clase $\overline{4}$ módulo 7.

Problema 1.11. *Probar que en cualquier colección de 7 o más enteros siempre hay dos cuya suma o diferencia es divisible por 11.*

Problema 1.12. *Probar que la ecuación $5^n + 2 = 17^m$ no tiene soluciones con n y m naturales.*

Problema 1.13. *Encontrar todos los enteros positivos n tales que $n + 1 | n^3 - 1$.*

Problema 1.14. *Encontrar todos los enteros positivos n tales que $2n - 1 | n^3 + 1$.*

1.3. División Modular

Es hora de analizar la cuestión de calcular divisiones en $\mathbb{Z}_n$. Sean a y b dos números reales, el dividir a por b es equivalente a multiplicar a por $\frac{1}{b}$. El número real $\frac{1}{b}$ es conocido como el inverso de b. Lo que caracteriza a $\frac{1}{b}$ es la ecuación: $b \cdot \frac{1}{b} = 1$. Esto es asumiendo que $b \neq 0$. Traduzcamos todo esto para $\mathbb{Z}_n$.
Sea $\overline{a} \in \mathbb{Z}_n$. Diremos que $\overline{b} \in \mathbb{Z}_n$ es el **inverso** de $\overline{a}$ si se verifica la ecuación:

$$\overline{a} \times \overline{b} = \overline{1} \text{ en } \mathbb{Z}_n,$$

o equivalentemente si $a \cdot b \equiv 1 \pmod{n}$. Por ejemplo, $\overline{2}$ es el inverso de $\overline{3}$ en $\mathbb{Z}_5$, pues $3 \cdot 2 \equiv 1 \pmod{5}$ y $\overline{3}$ es el inverso de $\overline{9}$ en $\mathbb{Z}_{26}$. Resulta claro que si $\overline{a} = \overline{0}$ y $n > 1$, entonces $\overline{a}$ no tiene inverso (ya que para todo $\overline{b} \in \mathbb{Z}_n$ $\overline{0} \cdot \overline{b} = \overline{0}$). Sin embargo, la clase $\overline{0}$ no necesariamente es la única no invertible en $\mathbb{Z}_n$.
A los valores $\overline{a}, \overline{b} \in \mathbb{Z}_n$ distintos de cero que verifican la ecuación

$$\overline{a} \times \overline{b} = \overline{0} \text{ en } \mathbb{Z}_n,$$

los llamamos **divisores de cero**. Por ejemplo $\overline{8}$ y $\overline{3}$ son divisores de cero en $\mathbb{Z}_{12}$, pues $8 \cdot 3 \equiv 0 \pmod{12}$. El siguiente teorema nos dice qué valores en $\mathbb{Z}_n$ son invertibles.

Teorema 1.1. *Sea n un número natural. La clase $\overline{a}$ tiene inverso en $\mathbb{Z}_n$ si y sólo si, a y n son primos relativos.*

Demostración. Para la primera implicancia (esto es $(a,n)=1$ entonces a tiene inverso), tenemos que por el teorema de Bézout existen enteros s,t tales que $as+nt=1$, lo que implica $1 \equiv as+nt \equiv as \pmod{n}$. Luego $\overline{s}$ es inverso de $\overline{a}$ en $\mathbb{Z}_n$.
Recíprocamente, si $\overline{a}$ es invertible en $\mathbb{Z}_n$, con $\overline{b} \in \mathbb{Z}_n$ tal que $a \cdot b \equiv 1 \pmod{n}$, tenemos $n|ab-1$, luego exite $t \in \mathbb{Z}$ tal que $ab-1=nt$, de esta ecuación es claro que cualquier divisor común de a y n es también divisor de 1, luego $(a,n)=1$ □

El conjunto de los elementos de $\mathbb{Z}_n$ que tienen inverso es de vital importancia. Vamos a denotarlo por $(\mathbb{Z}_n)^*$ y definirlo por:

$$(\mathbb{Z}_n)^* = \{\overline{a} \in \mathbb{Z}_n; (a,n)=1\}$$

Por ejemplo $(\mathbb{Z}_{14})^* = \{\overline{1},\overline{3},\overline{5},\overline{9},\overline{11},\overline{13}\}$. Es fácil obtener $(\mathbb{Z}_p)^*$ cuando p es primo. En este caso $(a,p)=1$ siempre que a no sea múltiplo de p. Por tanto, cuando p es primo, todas las clases distintas de $\overline{0}$ tienen inverso en $\mathbb{Z}_p$. Por ejemplo $(\mathbb{Z}_7)^* = \{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6}\}$.

Problema 1.15. *Probar que ningún elemento de $\mathbb{Z}_n$ puede ser a la vez divisor de cero e invertible.*

Problema 1.16. *Probar que si a y n son primos relativos, entonces $ab \equiv ac \pmod{n}$ si y sólo si $b \equiv c \pmod{n}$.*

Problema 1.17. *Probar que si $(a,n)>1$, entonces es posible encontrar $k \not\equiv 0 \pmod{n}$ de tal manera que $ak \equiv 0 \pmod{n}$. Concluir que si $(a,n)>1$ con $a \neq 0$, entonces a es divisor de cero módulo n.*

Problema 1.18. *Probar que si $(a,n)>1$, entonces es posible encontrar k y l enteros no congruentes entre sí tales que $ak \equiv al \pmod{n}$. Ilustrar con $n=6$.*

Problema 1.19. *Probar que si $\overline{a},\overline{b} \in (\mathbb{Z}_n)^*$, entonces $\overline{a} \times \overline{b} \in (\mathbb{Z}_n)^*$.*

Problema 1.20. *Resolver la congruencia $7x \equiv 3 \pmod{15}$. Probar que la congruencia $3x \equiv 7 \pmod{15}$ no tiene solución.*

Problema 1.21. *Sea p un número primo. Demuestre que el entero positivo a, es su propio inverso módulo p, si y sólo si, $a \equiv 1 \pmod{p}$ o bien $a \equiv -1 \pmod{p}$.*

2. La Función Phi de Euler

La función $\phi : \mathbb{N} \to \mathbb{N}$ definida como:

$$\phi(n) = \#(\mathbb{Z}_n)^*$$

es llamada **función phi de Euler**. O sea, $\phi(n)$ es la cantidad de elementos del conjunto $(\mathbb{Z}_n)^*$, o lo que es equivalente a la cantidad de primos relativos con n en $\mathbb{Z}_n$.
Tenemos que $\phi(1)=\phi(2)=1$, $\phi(3)=2$ y para $n>2$, $1<\phi(n)<n$. Por ejemplo $\phi(14) = \#(\mathbb{Z}_{14})^* = \#\{\overline{1},\overline{3},\overline{5},\overline{9},\overline{11},\overline{13}\} = 6$. Habíamos analizado que si p es primo entonces el único elemento no invertible en $\mathbb{Z}_p$ era el cero. Por tanto $\phi(p)=p-1$.

Problema 2.1. *Halle:*

1. *$\phi(4)$, $\phi(8)$, $\phi(16)$ y en general $\phi(2^k)$.*
2. *$\phi(7)$, $\phi(49)$.*
3. *Si p es primo y k es un natural, $\phi(p^k)$.*

Problema 2.2. *Si p y q son primos, calcule $\phi(pq)$.*

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100	101	102	103	104	105
106	107	108	109	110	111	112	113	114	115	116	117	118	119	0

Problema 2.3. *La siguiente tabla muestra todas las clases módulo* 120*. ¿Qué forma tienen los elementos en cada columna? ¿Y en cada fila? Pinte de un color todos los números primos relativos con 15 y de otro color los primos relativos con 8. ¿Cuáles son las casillas de números invertibles en* $\mathbb{Z}_{120}$*, esto es, los elementos de* $(\mathbb{Z}_{120})^*$*?. ¿Cuántas columnas están pintadas? y ¿Cuántas filas?. Halle* $\phi(15)$*,* $\phi(8)$ *y finalmente* $\phi(120)$*. ¿Cómo es* $\phi(120)$ *en función a* $\phi(8)$ *y* $\phi(15)$*. ¿Es posible extender este resuldado para otros números?*

La siguiente proposición nos ayudará a calcular $\phi(n)$.

Proposición 2.1. *Si* m *y* n *son primos relativos, entonces* $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

Demostración. Como en el ejercicio anterior, podemos construir una tabla de $m \times n$, la primera columna es formada por los números de la forma $nk+1$, la segunda por los números de la forma $nk+2$ y así sucesivamente la i-esima columna constituyen los números de la forma $nk+i$. Notemos que $(nk+i, n) = (i, n)$, significa que si un número en esta tabla es primo relativo por n, entonces todos los números de esa columna son primos relativos con n. Luego existen $\phi(n)$ columnas en las cuales todos los números son primos relativos con n. Por otro lado, note que cada columna de la tabla contiene todos los residuos módulo m, siguiendo el mismo análisis vemos que cada columna contiene $\phi(m)$ primos relativos con m. Como m y n son primos relativos, tenemos que un número es primo relativo con mn si y sólo si lo es con m y con n a la vez $((c, mn) = 1 \Leftrightarrow (c, m) = (c, n) = 1)$. Si pintamos los primos relativos con n tenemos $\phi(n)$ columnas pintadas y pintando los primos relativos con m cada columna tiene $\phi(m)$ filas pintadas. Luego hay éxactamente $\phi(m) \cdot \phi(n)$ elementos en la inersección, luego $\phi(mn) = \phi(m) \cdot \phi(n)$

$$\begin{array}{lllll} 1 & 2 & 3 & \cdots & n-1 & n \\ n+1 & n+2 & n+3 & \cdots & 2n-1 & 2n \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ n(m-1)+1 & n(m-1)+2 & n(n-1)+3 & \cdots & nm-1 & 0 \end{array}$$

□

Ahora podemos calcular $\phi(n)$ para n grande, sin tener que hallar los elementos de $(\mathbb{Z}_n)^*$. Por ejemplo $\phi(308) = \phi(4 \cdot 77)$, como $(4, 77) = 1$ por la proposición anterior $\phi(308) = \phi(4) \cdot \phi(77)$, además $\phi(77) = \phi(7 \cdot 11) = \phi(7) \cdot \phi(11)$. Luego, $\phi(308) = \phi(2^2) \cdot \phi(7) \cdot \phi(11) = (2^2 - 2) \cdot 6 \cdot 10 = 120$. Si $n = {p_1}^{e_1} {p_2}^{e_2} \dots {p_r}^{e_r}$ es la descomposición canónica de n, como $({p_i}^{e_i}, {p_j}^{e_j}) = 1$ para $i \neq j$, aplicando varias veces la proposición tenemos

$$\begin{aligned} \phi(n) &= \phi({p_1}^{e_1} {p_2}^{e_2} \dots {p_r}^{e_r}) = \phi({p_1}^{e_1}) \phi({p_2}^{e_2}) \dots \phi({p_r}^{e_r}) \\ \phi(n) &= ({p_1}^{e_1} - {p_1}^{e_1 - 1})({p_2}^{e_2} - {p_2}^{e_2 - 1}) \dots ({p_r}^{e_r} - {p_r}^{e_r - 1}) \\ \phi(n) &= {p_1}^{e_1 - 1} {p_2}^{e_2 - 1} \dots {p_r}^{e_r - 1} (p_1 - 1)(p_2 - 1) \dots (p_r - 1) \end{aligned}$$

O bien, $\phi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1)$.

Problema 2.4. *Probar que para* $n \geq 3$*,* $\phi(n)$ *es siempre par.*

Problema 2.5. *Hallar, para* $n \in \mathbb{N}$*, la suma de todos los enteros positivos menores a* n *y coprimos con* n*.*

Problema 2.6. *Demostrar que si* $a|b$*, entonces* $\phi(a)|\phi(b)$*.*

Problema 2.7. *Encontrar todas las soluciones de* $\phi(n) = 4$*.*

Problema 2.8. *Probar que:* $\sum_{n|d} \phi(d) = n$ *para todo* $n \in \mathbb{N}$*.*

3. El teorema de Euler

Un **sistema completo de residuos** módulo n es un conjunto de enteros $\{r_1, r_2, \ldots, r_n\}$ tal que si $i \neq j$, se verifica que $r_i \not\equiv r_j$ y además, para todo entero m, existe un r_i tal que $m \equiv r_i \pmod{n}$. Esto significa que los r_i representan **todas las clases de congruencias módulo n.**

$$\{\overline{r_1}, \overline{r_2}, \ldots, \overline{r_n}\} = \mathbb{Z}/(n)$$

Problema 3.1. *Muestre que si $\{r_1, r_2, \ldots, r_n\}$ es un sistema completo de residuos módulo n y a, b son enteros con $(a, n) = 1$, entonces $\{ar_1 + b, ar_2 + b, \ldots, ar_n + b\}$ es un sistema completo de residuos módulo n.*

Un **sistema reducido de residuos** módulo n es un conjunto de $\varphi(n)$ enteros $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ tal que cada elemento es coprimo con n y además, para $i \neq j$, se verifica que $r_i \not\equiv r_j \pmod{n}$. Esto es, los r_i representan **todas las clases de congruencia invertibles módulo n.**

$$\{\overline{r_1}, \overline{r_2}, \ldots, \overline{r_{\varphi(n)}}\} = \mathbb{Z}/(n)^\times$$

Problema 3.2. *Muestre que si $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ es un sistema reducido de residuos módulo n y a es un entero tal que $(a, n) = 1$, entonces $\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$ es un sistema reducido de residuos módulo n.*

Teorema 3.1 (Teorema de Euler)**.** *Sean a, n enteros positivos coprimos, entonces*

$$a^{\varphi(n)} \equiv 1 \ (mod\ n).$$

Demostración. Sean $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ un sistema reducido de residuos módulo n, y a un entero coprimo con n, por el ejercicio 1.2. sabemos que $\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$ también es un sistema reducido de residuos módulo n, por lo que

$$\begin{aligned} ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi(n)} &\equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)} \pmod{n} \\ \Leftrightarrow a^{\varphi(n)} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} &\equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)} \pmod{n} \end{aligned}$$

Como $(r_i, n) = 1$ para $i = 1, 2, \ldots, \varphi(n)$, cada uno de las a_i posee inverso módulo n y multiplicando la congruencia por los inversos obtenemos $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Teorema 3.2 (Pequeño Teorema de Fermat)**.** *Sean p un primo y a un entero positivo, entonces*

$$a^p \equiv a \ (mod\ n).$$

Demostración. Si a es multiplo de p el teorema es evidente. Si no, entonces $(a, p) = 1$ y podemos aplicar el teorema de Euler, en este caso $\varphi(p) = p - 1$ o sea $a^{p-1} \equiv 1$ (mod p) y multiplicando por a en ambos lados de la congruencia obtenemos lo buscado. □

Obs: Otra versión de este teorema dice que si p es primo y a entero positivo coprimo con p, entonces $a^{p-1} \equiv 1 \pmod{p}$.

Los teoremas que acabamos de ver son muy útiles para resolver problemas de teoría de números, veremos aquí algunos ejemplos.

Ejemplo 3.1. *Muestre que existen infinitos números de la forma* $2000000\ldots00017$ *que son múltiplos de* 2017*.*

Solución. El problema equuivale a encontrar infinitos k tales que

$$\begin{aligned} 2 \cdot 10^k + 17 &\equiv 0 \pmod{2017} \\ \Leftrightarrow 2 \cdot 10^k + 17 &\equiv 2017 \pmod{2017} \\ \Leftrightarrow 2 \cdot 10^k &\equiv 2000 \pmod{2017} \\ \Leftrightarrow 10^{k-3} &\equiv 1 \pmod{2017} \end{aligned}$$

ya que 2000 es invertible módulo 2017, además por el pequeño teorema de Fermat $10^{2017-1} \equiv 1 \pmod{2017}$, luego basta con tomar $k = 2016t + 3$, con $t \in \mathbb{N}$. □

Ejemplo 3.2. *Muestre que no existe entero positivo x tal que* $103|x^3 - 2$

Solución. Note primeramente que 103 es primo. Ahora supongamos que $x^3 \equiv 2 \pmod{103}$, de modo que $103 \nmid x$. Ahora, elevando ambos lados de la congruencia a la $(103-1)/3 = 34$, obtenemos $x^{102} \equiv 2^{34} \pmod{103}$, haciendo las cuentas obtenemos $2^{34} \equiv 46 \pmod{103}$, luego $x^{102} \equiv 46$, pero por el pequeño teorema de Fermat debemos tener $x^{102} \equiv 1$, contradicción!. Por tanto no existe x tal que $103|x^3 - 2$. □

Ejemplo 3.3. *Encuentre un número $n \in \mathbb{N}$ tal que $2^n > 10^{2000}$ y 2^n tenga entre sus 2000 últimos dígitos por lo menos 1000 ceros consecutivos.*

Solución. Por el teorema de Fermat $2^{\varphi(5^{2000})} \equiv 1 \pmod{5^{2000}}$, por tanto existe $b \in \mathbb{N}$ tal que

$$2^{\varphi(5^{2000})} = 5^{2000}b + 1 \Rightarrow 2^{2000+\varphi(5^{2000})} = 10^{2000}b + 2^{2000}.$$

Luego, los 2000 últimos dígitos de $2^{2000+\varphi(5^{2000})}$ coinciden con la representación decimal de 2^{2000}, que tiene como máximo 667 dígitos, pues $2^{2000} < (2^3)^{667} < 10^{667}$. De esta forma hay al menos $2000 - 667 = 1333$ ceros consecutivos entre los 2000 últimos dígitos de $2^{2000+\varphi(5^{2000})}$, y así $n = 2000 + \varphi(5^{2000}) = 4 \cdot 5^{1999} + 2000$ satisface las condiciones del enunciado. □

Teorema 3.3 (Wilson)**.** *Para todo primo p, $(p-1)! \equiv -1$ (mod p).*

Demostración. El teorema se verifica para $p = 2, 3$. Consideremos $p \geq 5$.
Sea $S = \{2, 3, 4, \ldots, p-2\}$. Como p es primo, cada uno de estos enteros es coprimo con p, y por ende poseen un inverso en módulo p. Se pueden dar dos casos para cada elemento a:

1. que el inverso de a sea nuevamente a
2. que el inverso de a sea distinto a a

En el primer caso tendríamos $a \cdot a \equiv 1 \pmod{p}$, o sea $p|a^2 - 1$, esto es $p|(a+1)(a-1)$, y como p es primo se tiene que $p|a+1$ o $p|a-1$, o sea $a + 1 \equiv 0 \pmod{p}$ o $a + 1 \equiv 0 \pmod{p}$, de donde podemos deducir que 1 y $p-1$ son los únicos números inveros de sí mismos, $a = \overline{1}, \overline{p-1}$, luego $a \notin S$, absurdo. Solo se da el caso 2, o sea cada elemento de S posee un inverso distinto de sí mismo, además este inverso también pertenece a S puesto que son distintos de 1 y $p-1$. Esto nos permite agrupar a los elementos de S en parejas tales que cada uno quede con su inverso. Multiplicando el producto de todas estas parejas podemos deducir que $2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}$. Multiplicando por $p-1$ obtenemos $(p-1)! \equiv -1 \pmod{p}$. □

Ejemplo 3.4. *1. Si p es un primo, entonces para cualquier entero positivo $n < p$,*

$$(n-1)!(p-n)! \equiv (-1)^n \text{ (mod } p).$$

2. Si p es un primo, entonces $\binom{p-1}{k} \equiv (-1)^k$ (mod p) para todo $k = 0, 1, \ldots, p-1$.

Solución. 1. La propiedad es obvia para $p = 2$, asumamos ahora que p es impar. Del teorema de Wilson, $(p-1)! \equiv -1 \pmod{p}$, luego

$$(n-1)!n(n+1)\cdots(p-1) \equiv -1 \pmod{p},$$

lo cual es equivalente a

$$(n-1)!(p-(p-n))(p-(p-n-1))\cdots(p-1) \equiv -1 \pmod{p}$$

Además, $p - k \equiv -k$, $k = 1, 2, \ldots, p-n$, implica

$$(n-1)!(-1)^{p-n}(p-n)! \equiv -1 \pmod{p}$$

y como p es impar, se demuestra lo propuesto.

2. Tenemos

$$\binom{p-1}{k} = \frac{(p-1)!}{k!(p-k-1)!}$$

luego, $k!(p-k-1)!\binom{p-1}{k} \equiv (p-1)! \equiv -1 \pmod{p}$. Aplicando el resultado anterior para $n = k+1$, tenemos $k!(p-k-1)! \equiv (-1)^{k+1} \pmod{p}$ y obtenemos el resultado.

□

Problema 3.3. *Sea p un primo. Probar que p divide a $ab^p - a^p b$ para todo $a, b \in \mathbb{Z}$*

Problema 3.4. *Sea p un primo con $p > 5$. Probar que $p^8 \equiv 1 \pmod{240}$.*

Problema 3.5. *Probar que si a y b son enteros positivos coprimos, entonces existen enteros positivos m y n tales que $a^m + b^n \equiv 1 \pmod{ab}$.*

Problema 3.6. *Probar el recíproco del Teorema de Wilson: Si $(n-1)! \equiv -1 \pmod{n}$, para un entero $n \geq 2$, entonces n es primo.*

Problema 3.7. *Sean $a_1, a_2, \ldots, a_p$ y $b_1, b_2, \ldots, b_p$ sistemas completos de residuos módulo p, con p primo. ¿Puede $a_1b_1, a_2b_2, \ldots, a_pb_p$ ser un sistema completo de residuos módulo p?*

Problema 3.8. *Varios enteros son dados (algunos de ellos podrían ser iguales) tales que la suma de todos ellos es 1492. Decidir si la suma de sus potencias a la 7 puede ser igual a*

1. *1996;*
2. *1998.*

Problema 3.9. *Hallar la cantidad de enteros $n > 1$ para los cuales el número $a^{25} - a$ es divisible por n para cada entero a.*

Problema 3.10 (6th IMO). *a) Encontrar todos los enteros positivos n tales que 7 divide a $2^n - 1$.*

b) Probar que para cualquier entero positivo n, el número $2^n + 1$ no puede ser divisible por 7.

Problema 3.11. *Pruebe que para cada entero positivo s, existe un entero positivo n suya suma de sus dígitos es s y $s|n$.*

Problema 3.12. *Pruebe que si p es un primo impar, entonces el resto de dividir $(p-1)!$ con $p(p-1)$ es $(p-1)$.*

Problema 3.13 (46th IMO). *Considere la secuencia $a_1, a_2, \ldots$ definida como*

$$a_n = 2^n + 3^n + 6^n - 1 \ (n = 1, 2, \ldots)$$

Determine todos los enteros positivos que son primos relativos con cada uno de los terminos de la secuencia.

Problema 3.14 (13th IMO). *Pruebe que la secuencia $\{2^n - 3 | n = 2, 3, \ldots\}$ contiene una subsecuencia tal que todos sus miembros son primos relativos.*

Problema 3.15. *Sea $a > 1$ un entero positivo. Muestre que el conjunto*

$$\{a^2 + a - 1, a^3 + a^2 - 1, \ldots\}$$

contiene infinitos subconjuntos tales que cualesquiera dos miembros de estos son primos relativos.

4. Congruencias Lineales

Antes de empezar esta sección, resolvamos algunos ejercicios

Problema 4.1. *Encontrar todos los enteros x que satisfagan $4x + 20 \equiv 27x - 1 \pmod{5}$.*

Problema 4.2. *Sea $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ la descomposición de n en potencias de primos distintos. Pruebe que la congruencia*

$$a \equiv b \pmod{n}$$

es equivalente al sistema de congruencias

$$\begin{aligned} a &\equiv b \ (mod\ p_1^{e_1}) \\ a &\equiv b \ (mod\ p_2^{e_2}) \\ &\vdots \\ a &\equiv b \ (mod\ p_r^{e_r}) \end{aligned}$$

Ejemplo 4.1. *Resolver el sistema de congruencias*

$$\begin{array}{rcll} 2x & \equiv & 1 & (\text{mod } 7) \quad (*) \\ x & \equiv & 1 & (\text{mod } 5) \quad (**) \\ 2x-3 & \equiv & 29-2x & (\text{mod } 6) \quad (***) \\ x+3 & \equiv & 5x-3 & (\text{mod } 2) \quad (****) \end{array}$$

Solución. Resolvemos primero cada una por separado; después de hacer las cuentas obtendremos

$$\begin{array}{rcll} x & \equiv & 4 & (\text{mod } 7) \quad (*) \\ x & \equiv & 1 & (\text{mod } 5) \quad (**) \\ x & \equiv & 2 & (\text{mod } 3) \quad (***) \\ 0 & \equiv & 0 & (\text{mod } 2) \quad (****) \end{array}$$

Nótese que la última congruencia se satisface siempre (no importa qué valor se le dé a x). Esto quiere decir que la podemos eliminar sin alterar la solución del sistema. De la primera congruencia tenemos que $x = 4+7u$, para cualquier valor entero de u. Trataremos de encontrar para qué valores de u las otras congruencias también se satisfacen. Sustituyendo en (**) tenemos $4+7u \equiv 1 \pmod 5$. Ahora resolvamos con respecto a u:

$$\begin{array}{rcll} 2u & \equiv & \text{-3} & (\text{mod } 5) \\ u & \equiv & \text{-9} & (\text{mod } 5) \\ u & \equiv & 1 & (\text{mod } 5) \end{array}$$

Tenemos entonces que las soluciones comunes a las dos primeras congruencias son de la forma $x = 4+7u$, donde u es de la forma $1+5v$, esto es, $x = 4+7(1+5v) = 11+35v$. Ahora queremos ver para qué valores de v también se satisface la tercera. Sustituimos en (***) y resolvemos para v:

$$\begin{array}{rcll} 11+35v & \equiv & 2 & (\text{mod } 3) \\ 2v & \equiv & 0 & (\text{mod } 3) \\ v & \equiv & 0 & (\text{mod } 3) \end{array}$$

Hemos obtenido entonces que $v = 3w$, w entero. Sustituimos en x: $x = 11+35(3w) = 11+105w$ para cualquier entero w. Así el conjunto solución del sistema es la clase 11 módulo 105. □

Problema 4.3. *Resuelva el siguiente sistema de congruencias*

$$\begin{array}{rcll} 2x+3 & \equiv & 8 & (\text{mod } 5) \quad (1) \\ x-5 & \equiv & \text{3-x} & (\text{mod } 4) \quad (2) \\ 2x-1 & \equiv & 19-2x & (\text{mod } 12) \quad (3) \\ x-1 & \equiv & 1 & (\text{mod } 3) \quad (4) \end{array}$$

Es claro que habrá sistemas de congruencias que no tengan solución, aun cuando cada una de las congruencias de sistema sí sea soluble por separado, por ejemplo el sistema

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 4 \pmod 6 \end{aligned}$$

En algunas ocasiones es posible decidir que cierto sistema sí tiene solución sin resolverlo; esto es cuando al escribir todas las congruencias en la forma simplificada $x \equiv b \pmod{n}$ los módulos son primos relativos por parejas. Este es el contenido del teorema siguiente llamado **Teorema Chino del resto**. El teorema puede probarse por inducción sobre el número de congruencias siguiendo el método descrito en el ejemplo anterior, sin embargo daremos aquí otra prueba directa que exhibe explícitamente la solución del sistema.

Teorema 4.1 (Teorema Chino del Resto)**.** *Sean $m_1, m_2, \ldots, m_r$ enteros positivos tales que dos cualesquiera de ellos son coprimos y $a_1, a_2, \ldots, a_r$ enteros cualesquiera. Entonces, el sistema*

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1) \\ x &\equiv a_2 \ (mod\ m_2) \\ &\vdots \\ x &\equiv a_r \ (mod\ m_r) \end{aligned}$$

admite solución, además la solución es única en módulo $m = m_1 m_2 \ldots m_r$.

Demostración. Considerando a $m = m_1 m_2 \ldots m_r$, vemos que $\frac{m}{m_j}$ es entero y que $(\frac{m}{m_j}, m_j) = 1$. Entonces, existe un entero b_j tal que $\frac{m}{m_j} \cdot b_j \equiv 1 \pmod{m_j}$. Claramente, $\frac{m}{m_j} \cdot b_j \equiv 0 \pmod{m_i}$ para $i \neq j$. Definamos

$$x_0 = \textstyle\sum_{j=1}^{r} \frac{m}{m_j} \cdot b_j \cdot a_j$$

Tenemos que $x_0 \equiv \frac{m}{m_j} \cdot b_j \cdot a_j \equiv a_j \pmod{m_j}$. Entonces, x_0 es una solución de nuestro sistema de congruencias. Supongamos que x_1 también es una solución de nuestro sistema. Tendríamos que $x_0 \equiv x_1 \pmod{m_i}$ para cada i. Como $(m_i, m_j) = 1$ para $i \neq j$, entonces $x_0 \equiv x_1 \pmod{m}$. □

Ejemplo 4.2. *Hallar la solución del sistema*

$$\begin{aligned} x &\equiv 2 \ (mod\ 3) \\ x &\equiv 1 \ (mod\ 4) \\ x &\equiv 3 \ (mod\ 5) \end{aligned}$$

Solución. Procederemos como en la prueba del teorema. En este caso $m = 2 \cdot 4 \cdot 5 = 60$, ahora tenemos que encontrar los inversos b_i en cada una de las congruencias:

$$\tfrac{60}{3} b_1 \equiv 1 \pmod{3},\ \tfrac{60}{4} b_2 \equiv 1 \pmod{4},\ \tfrac{60}{5} b_3 \equiv 1 \pmod{5}$$

Obtenemos $b_1 = 2$, $b_2 = 3$, $b_3 = 3$. Luego

$$x_0 = 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 1 + 12 \cdot 3 \cdot 3 = 233$$

Teniendo en cuenta que todas las soluciones son congruentes módulo 60, es suficiente tomar $x_0 = 53$. Todas las soluciones son dadas por $x = 53 + 60k$, $k \in \mathbb{Z}$. □

Es importante notar que la utilidad del teorema no recae en calcular la solución al sistema, a veces puede ser más facil encontrar la solución del sistema utilizando el método del ejemplo 2.1.. La importancia recae en afirmar la existencia de la solución. Esto lo veremos en el siguiente ejemplo.

Ejemplo 4.3. *Probar que existen cadenas tan grandes como uno quiera de números naturales consecutivos en las que cada número es divisible por el cuadrado de un entero mayor que* 1*.*

Solución. Sea n un número natural cualquiera y sean $p_1, p_2, \ldots, p_n$ primos distintos. Consideremos el sistema de congruencias

$$\begin{aligned} x &\equiv -1 \pmod{p_1^2} \\ x &\equiv -2 \pmod{p_2^2} \\ &\vdots \\ x &\equiv -n \pmod{p_n^2} \end{aligned}$$

Por el Teorema Chino del resto el sistema tiene solución pues los módulos son primos relativos por parejas. Una solución cualquiera es tal que $p_i^2|x+i$, para $i=1,2,\ldots,n$, así que los n números consecutivos buscados son $x+1, x+2, \ldots, x+n$. □

Problema 4.4. *Determine un valor de s tal que $1024s \equiv 1 \pmod{2011}$ y calcule el resto de la división de 2^{2000} por 2011.*

Problema 4.5. *Un entero positivo n es llamado auto-replicante si los últimos dígitos de n^2 forman el número n. Por ejemplo 25 es auto-replicante, pues $25^2 = 625$. Determine todos los números auto-replicantes con exactamente 4 dígitos.*

Problema 4.6. *Probar que para n y r números naturales, existe una progresión aritmética de razón r, tal que cada uno de los primeros n elementos es divisible entre una k-ésima potencia de un número natural mayor que 1.*

Problema 4.7. *¿Existen 21 enteros positivos consecutivos tales que cada uno es divisible por al menos uno de los primos en el intervalo $2 \leq p \leq 13$?*

Problema 4.8. *Demostrar que para k y n números naturales, es posible encontrar k números consecutivos, cada uno de los cuales tiene al menos n divisores primos diferentes.*

Problema 4.9. *Demostrar que para todo entero positivo m y todo número par, este último puede ser escrito como la diferencia de dos enteros positivos, cada uno de los cuales es primo relativo con m.*

Problema 4.10 (Olimpiada de Mayo 2013)**.** *¿Es posible escribir 100 números impares en una fila de tal forma que la suma de cada 5 adyacentes sea un cuadrado perfecto y que la suma de cada 9 números adyacentes también sea un cuadrado perfecto?*

Problema 4.11. *Para cada conjunto de enteros positivos $\{a_1, a_2, \ldots, a_n\}$ existe un entero positivo b tal que el conjunto $\{ba_1, ba_2, \ldots, ba_n\}$ consiste en potencias perfectas.*

5. Residuos Cuadráticos y El símbolo de Legendre

Sean a y m enteros positivos tales que $m \neq 0$ y $(a,m) = 1$. Decimos que a es un **residuo cuadrático módulo** m si existe x entero tal que:

$$x^2 \equiv a \pmod{m}$$

Sea p un primo y a un entero positivo no divisible por p. El **símbolo de Legendre de a con respecto a p** se define de la siguiente forma:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es residuo cuadrático módulo } n \\ -1 & \text{si } a \text{ no es residuo cuadrático módulo } n \end{cases}$$

Es claro que todos los cuadrados perfectos son residuos cuadráticos. Probemos algunos resultados interesantes.

Ejemplo 5.1. *Sea p un primo. Entonces hay exactamente $(p+1)/2$ residuos cuadráticos módulo p.*

Demostración. Los números

$$0^2, 1^2, 2^2, \ldots, (\tfrac{p-1}{2})^2 \bmod p$$

son todos los residuos cuadráticos ya que todo entero x es congruente a $\pm i$ mod p para algún i tal que $o \leq i \leq \frac{p-1}{2}$ de modo que x^2 es congruente a uno de los números de arriba. Note además que módulo p estos números son todos distintos, pues si

$$\begin{aligned} i^2 \equiv j^2 \pmod{p} &\Rightarrow p|(i+j)(i-j) \\ &\Leftrightarrow p|i+j \text{ o } p|i-j \\ &\Leftrightarrow i \equiv \pm j \pmod{p} \end{aligned}$$

Pero como $o \leq i, j \leq \frac{p-1}{2} \Rightarrow 0 < i + j \leq p - 1$ o $i = j = 0$, tenemos que la única posibilidad es $i \equiv j \pmod{p}$.

Luego, $0^2, 1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ son todos distintos en módulo p. □

Veamos el siguiente resultado, el cual nos ayudará a determinar si un número es residuo cuadrático o no

Teorema 5.1 (Criterio de Euler)**.** *Si p es un primo impar y a un entero no divisible por él, entonces*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Demostración. Por el Pequeño Teorema de Fermat tenemos que $a^{p-1} \equiv 1 \pmod{p}$, de donde

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-12}{+}} 1) \equiv 0 \pmod{p} \Leftrightarrow p | a^{\frac{p-1}{2}} - 1 \text{ o } p | a^{\frac{p-1}{2}} - 1$$

esto es:

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

Supongamos que $\left(\frac{a}{p}\right)$=1, entonces a es residuo cuadrático y existe i tal que $i^2 \equiv a \pmod{p}$. Tenemos que $(i, p) = 1$, y por el Pequeño teorema de Fermat, $i^{p-1} \equiv 1 \pmod{p}$. Entonces,

$$a^{\frac{p-1}{2}} = (i^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

y el criterio de Euler se cumple.

Ahora, para , cada una de las congruencias $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ y $x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ se tienen $\frac{p-1}{2}$ soluciones distintas en el conjunto $\{1, 2, \ldots, p-1\}$. Los $\frac{p-1}{2}$ residuos cuadráticos corresponden a la primera de las congruencias y los demás a la segunda. Por lo tanto si a no es un residuo cuadrático, tenemos $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ y el Criterio de Euler también se cumple. □

Corolario 5.1. *El símbolo de Legendre posee las siguientes propiedades:*

1. *Si $a \equiv b \pmod{p}$ entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$*
2. $\left(\frac{a^2}{p}\right) = 1$
3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$*, o sea -1 es residuo cuadrático módulo p si y sólo si, $p \equiv 1 \pmod{4}$*
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

A continuacin veremos un resultado mucho más fuerte, la famosa Ley de Reciprocidad Cuadrática, gracias a la cual podemos determinar fcilmente si un nmero es o no un residuo cuadrtico. Una demostracin la podemos encontrar en [2].

Teorema 5.2 (Ley de Reciprocidad Cuadrática)**.** .

1. *Para todo primo impar p*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod{8} \\ -1 & \text{si } p \equiv \pm 3 \pmod{8} \end{cases}$$

2. *Si p y q son primos impares distintos, entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Ejemplo 5.2. *Determinar si -90 es residuo cuadrático módulo 1019 o no.*

Solución. Tenemos:

$$\left(\frac{-90}{1019}\right) = \left(\frac{-1}{1019}\right)\left(\frac{2}{1019}\right)\left(\frac{3^2}{1019}\right)\left(\frac{5}{1019}\right)$$

$\left(\frac{-1}{1019}\right) = (-1)^{(1019-1)/2} = (-1)^{509} = -1$;
$\left(\frac{2}{1019}\right) = (-1)^{\frac{1019^2-1}{8}} = -1$; (aquí usamos el resultado el problema anterior)
$\left(\frac{3^2}{1019}\right) = 1$;
$\left(\frac{5}{1019}\right)\left(\frac{1019}{5}\right) = (-1)^{\frac{1019-1}{2}\frac{5-1}{2}=1}$; implica $\left(\frac{5}{1019}\right) = \left(\frac{1019}{5}\right)$.
Luego,

$$\left(\frac{-90}{1019}\right) = (-1)\cdot(-1)\cdot 1\left(\frac{1019}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

O sea -90 es residuo cuadrático módulo 1019. □

Problema 5.1. *Calcular* $\left(\frac{44}{103}\right)$, $\left(\frac{-60}{1019}\right)$ *y* $\left(\frac{2010}{1019}\right)$.

Problema 5.2. *Determine todas las soluciones de* $x^{10} \equiv 1$ *(mod* 49*).*

Problema 5.3. *Muestre que si* p *es un primo de la forma* $4n+1$*, entonces* $p|n^n - 1$.

Problema 5.4. *Determinar si la congruencia* $x^2 \equiv 236$ *(mod* 257*) tiene solución.*

Problema 5.5. *Probar que existen infinitos primos de la forma* $3k+1$ *y* $3k-1$.

Problema 5.6. *Sea* p *un primo de la forma* $4k+1$*. Probar que* $p|n^n - 1$.

Problema 5.7. *Sea* $k = 2^{2^n}+1$ *para cierto entero positivo* n*. Mostrar que* k *es primo si y sólo si* k *es un factor de* $3^{\frac{k-1}{2}}+1$.

Problema 5.8. *Probar que* 2^n+1 *no tiene factores primos de la forma* $8k+7$.

Problema 5.9 (Ibero 2003)**.** *Se definen las sucesiones* $(a_n)_{n\geq 0}$, $(b_n)_{n\geq 0}$ *por*

$$a_0 = 1,\ b_0 = 4,\ a_{n+1} = a_n^{2001} + b_n,\ b_{n+1} = b_n^{2001} + a_n,\ n \geq 0.$$

Demuestre que 2003 *no divide ninguno de los terminos de estas sucesiones.*

Referencias

[1] Pérez Seguí, M. L., *Teoría de Números*, Cuadernos de Olimpiadas Matemáticas, Instituto de Matemáticas, UNAM, 3a edición (2006)

[2] Brochero, F; Moreira, C.; Saldanha, N; Tengan, E. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*, Projeto Euclides, Instituto Nacional de Matemática Pura y Aplicada, 4a edición (2015)

[3] Andreescu, T.; Andrica, D. *Number Theory: Structures, Examples, and Problems*, Birkhauser (2009)