Congruencias y polinomios

Mario Pineda Ruelas
Departamento de Matemáticas,
Universidad Autónoma Metropolitana-Iztapalapa
correo electrónico: mpr@xanum.uam.mx

Gabriel D. Villa Salvador
Departamento de Control Automático,
Centro de Investigación y de Estudios Avanzados, IPN
correo electrónico gvilla@ctrl.cinvestav.mx

1 $\mathbb{Z}_m$

Uno de los conceptos fundamentales en teoría de números es el de *congruencia*. Históricamente las congruencias fueron estudiadas primeramente por Fermat, Euler, Lagrange y Legendre. Gauss, en su famosa obra *Disquisitiones Arithmeticæ*, es el primer matemático que hace un estudio coherente y sistemático del tema.

Muchos problemas teórico-práctico pueden simplificarse estudiando el residuo que deja cada entero al ser dividido por un entero fijo. De esta forma, podemos pensar que la teoría de las congruencias es una herramienta poderosa que nos ayuda a resolver problemas por medio del estudio de residuos. Por ejemplo, sabemos que el cuadrado de cualquier entero deja residuo 0 ó 1 al ser dividido entre 4. Si queremos averiguar si el número 505395 es un cuadrado, entonces un buen indicio es conocer su residuo al ser dividido entre 4. Puesto que $505395 = 4(126348) + 3$, entonces 505395 no es un cuadrado. Si el residuo hubiera sido 0 ó 1, entonces no necesariamente se trata de un cuadrado, simplemente el número es un sospechoso de ser un cuadrado.

Sea n cualquier entero diferente de 0. Definimos en $\mathbb{Z}$ la siguiente relación: $a \equiv b$ si y sólo si $n \mid a - b$. Si los enteros a, b están relacionados diremos que a es *congruente* con b módulo n y escribiremos $a \equiv b \pmod{n}$. Es fácil verificar que $\equiv$ satisface:

1. $a \equiv a \pmod{n}$.
2. Si $a \equiv b \pmod{n}$, entonces $b \equiv a \pmod{n}$.
3. Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, entonces $a \equiv c \pmod{n}$.

De lo anterior se sigue que $\equiv$ es una relación de equivalencia. Fue Gauss[1] el primero en introducir este concepto así como la notación.

De la definición de congruencia se sigue fácilmente el siguiente resultado:

Teorema 1.1. *Sean $a, b, c, d, m, n \in \mathbb{Z}$ con $n \neq 0$.*

1. *Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces $a + c \equiv b + d \pmod{n}$.*
2. *Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces $ax + cy \equiv bx + dy \pmod{n}$, para todo $x, y \in \mathbb{Z}$.*
3. *Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces $ac \equiv bd \pmod{n}$. En particular $a^m \equiv b^m \pmod{n}$ para todo $m \in \mathbb{N}$.*
4. *Si $d \mid n$ y $a \equiv b \pmod{n}$, entonces $a \equiv b \pmod{d}$.*
5. *Si $f(x) \in \mathbb{Z}[x]$ y $a \equiv b \pmod{n}$, entonces $f(a) \equiv f(b) \pmod{n}$.*

Demostración: Es un ejercicio fácil para el lector.

□

Notemos que por el algoritmo de la división el entero a tiene la forma $a = nq + r$ donde $0 \leq r < |n|$, así que $a \equiv r \pmod{n}$. En general, dos enteros son congruentes módulo n si y sólo si dejan el mismo residuo al ser divididos por n. El Teorema 1.1 nos dice que las congruencias se gobiernan *casi* con las mismas leyes que una igualdad. En este sentido, el símbolo $\equiv$ es como el símbolo $=$; los dos se gobiernan *casi* bajo las mismas leyes aritméticas. El siguiente resultado, es un criterio de cancelación para el producto bajo el símbolo $\equiv$.

Teorema 1.2. *$ax \equiv ay \pmod{m}$ si y sólo si $x \equiv y \pmod{\dfrac{m}{\mathrm{mcd}(a, m)}}$.*

Demostración: Si $ax \equiv ay \pmod{m}$, entonces $m \mid a(x - y)$ y $a(x - y) = mt$, para algún $t \in \mathbb{Z}$. Si $g = \mathrm{mcd}(a, m)$ tenemos

$$\frac{a}{g}(x - y) = \frac{m}{g}t,$$

y por tanto

[1] Karl-Friedrich Gauss nace en Gotinga, Alemania el 30 de abril de 1777. Hijo de padres humildes, ingresa a la Universidad de Gotinga en 1795 recibiendo el apoyo económico del duque Carlos Guillermo. El 30 de marzo de 1796 obtiene, a partir de ecuaciones ciclotómicas, la construcción del polígono regular de 17 lados usando sólo regla y compás. Es en este momento cuando se decide a ser matemático. En 1798 recibe su doctorado en la Universidad de Helmsted bajo la dirección del profesor Johann Friedrich Pfaff. En 1801 publica su gran tratado *Disquisitiones Aritmeticæ*, en el que presenta un resumen de trabajos de sus predecesores, formula conceptos y cuestiones que indicarán, durante más de un siglo, las líneas maestras de la investigación en teoría de números. Entre sus alumnos más notables destacan Dedekind y Riemann. Muere durante el sueño el 23 de febrero de 1855. Este espacio es muy breve para describir la grandeza científica de Gauss.

$$\frac{m}{g} \mid \frac{a}{g}(x-y).$$

Por otro lado

$$\operatorname{mcd}\left(\frac{m}{g}, \frac{a}{g}\right) = 1,$$

así $\frac{m}{g} \mid x-y$ y $x \equiv y \pmod{\frac{m}{g}}$. Inversamente, si $x-y = \frac{m}{g}t$, tenemos $a(x-y) = m\frac{a}{g}t$ y así $ax \equiv ay \pmod{m}$.

□

Teorema 1.3. *Sean $m_1, \ldots, m_r$ enteros diferentes de 0. Entonces para $1 \leq i \leq r$ se tiene*

$$x \equiv y \pmod{m_i} \text{ si y sólo si } x \equiv y \pmod{\operatorname{mcm}(m_1, ..., m_r)}.$$

Demostración: Como $m_i \mid x-y$, entonces $x-y$ es un múltiplo común de los m_i's. Usando el Teorema **??** tenemos $\operatorname{mcm}(m_1, ..., m_r) \mid x-y$. La otra parte es consecuencia del Teorema 1.1 parte (4).

□

Teorema 1.4. *Si $x \equiv y \pmod{m}$, entonces $\operatorname{mcd}(x, m) = \operatorname{mcd}(y, m)$.*

Demostración: Si $x \equiv y \pmod{m}$, entonces para alguna $t \in \mathbb{Z}$ se tiene $x = mt + y$. Aplicando el Lema **??** se sigue que $\operatorname{mcd}(x, m) = \operatorname{mcd}(y, m)$.

□

El inverso del teorema anterior no es válido, por ejemplo $x = 2$, $y = 4$, $m = 7$.

Definición 1.5. *Sea $m \in \mathbb{Z} \setminus \{0\}$. El conjunto de enteros $\{x_1, \ldots, x_s\}$ es un sistema completo de residuos módulo m, el cual escribiremos como $SCR(m)$, si dado $y \in \mathbb{Z}$, existe un único $x_i \in SCR(m)$ tal que $y \equiv x_i \pmod{m}$.*

Notemos que si $x_i, x_j \in SCR(m)$ con $i \neq j$, entonces $x_i \not\equiv x_j \pmod{m}$ y por tanto en un $SCR(m)$, cualesquiera dos elementos son incongruentes módulo m. El conjunto $\{0, 1, \ldots, |m|-1\}$ es un $SCR(m)$.

Teorema 1.6. *Si $\{x_1, \ldots, x_s\}$ y $\{y_1, \ldots, y_t\}$ son $SCR(m)$, enonces $s = t$.*

Demostración: Supongamos que $s < t$. Para cada $x_i \in \{x_1, \ldots, x_s\}$ existe un único $y_j \in \{y_1, \ldots, y_t\}$ tal que $x_i \equiv y_j \pmod{m}$. Reacomodando los elementos de $\{y_1, \ldots, y_t\}$, podemos suponer que $x_i \equiv y_i \pmod{m}$. Sea y_j con $s+1 \leq j \leq t$. Puesto que $\{x_1, \ldots, x_s\}$ es un $SCR(m)$, entonces existe un único $x_r \in$

$\{x_1, \ldots, x_s\}$ tal que $y_j \equiv x_r \pmod{m}$. De lo anterior se sigue que $y_j \equiv x_r \equiv y_r \pmod{m}$ y $j \neq r$, lo cual es absurdo. De la misma forma $t < s$ nos lleva a un absurdo. Por tanto $t = s$.

□

Corolario 1.7. *Cualquier $SCR(m)$ tiene cardinalidad $|m|$.*

Demostración: $\{0, 1, \ldots, |m| - 1\}$ es un $SCR(m)$.

□

El siguiente resultado es útil para identificar sistemas completos de residuos.

Teorema 1.8. *Si el conjunto $\{x_1, ..., x_{|m|}\}$ satisface $x_i \not\equiv x_j \pmod{m}$ para $i \neq j$, entonces $\{x_1, ..., x_{|m|}\}$ es un $SCR(m)$.*

Demostración: Como $x_i \not\equiv x_j \pmod{m}$ para $i \neq j$, entonces x_i y x_j dejan diferente residuo al ser divididos por m. Reordenando los x_i de tal manera que $x_i = mq_i + i$, obtenemos que $x_i \equiv i \pmod{m}$. Sea $y \in \mathbb{Z}$. Entonces $y = mq + j$ con $0 \leq j < |m|$. De lo anterior se sigue que $y \equiv x_j \pmod{m}$.

□

Observemos que si $\{x_1, ..., x_s\}$ es un $SCR(m)$, entonces $s = |m|$ y para $i \neq j$ necesariamente $x_i \not\equiv x_j \pmod{m}$.

Corolario 1.9. *Sean $a, m \in \mathbb{Z}$ primos relativos y $\{x_1, ..., x_{|m|}\}$ un $SCR(m)$. Entonces $\{ax_1, ..., ax_{|m|}\}$ es un $SCR(m)$.*

Demostración: Supongamos que para algún par de índices i, j se cumple $ax_i \equiv ax_j \pmod{m}$. Usando el Teorema 1.2 obtenemos $x_i \equiv x_j \pmod{m}$ y esto último sólo es posible cuando $i = j$.

□

Definición 1.10. *Si $m > 0$ escribiremos $\mathbb{Z}_m$ en lugar de $SCR(m)$. Por comodidad convenimos en que $\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1\}$. El conjunto $\mathbb{Z}_m$ se conoce con el nombre de anillo de residuos módulo m.*

El anillo $\mathbb{Z}_m$ es una de las estructuras algebraicas más importantes en teoría de números. La manera conveniente de construir esta estructura es por medio de la definición de congruencia. La relación $\equiv$ que definimos al principio de este capítulo es de equivalencia y por lo tanto en cada clase de equivalencia podemos considerar como representante al residuo que deja un entero al ser dividido por el entero fijo m. Es por esto que $\mathbb{Z}_m = \{[0], [1], \ldots [m - 1]\}$ y por abuso de notación, simplemente escribimos $\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1\}$.

En el anillo de residuos módulo m introducimos una suma y un producto:

$$[i] + [j] = [i + j] \quad \text{y} \quad [i][j] = [ij].$$

Lema 1.11. *La suma y producto definidas en $\mathbb{Z}_m$ no dependen del representante.*

Demostración: Si $a \in [i]$ y $b \in [j]$, entonces por la parte (1) y (3) del Teorema 1.1 se sigue que $i + j \equiv a + b \pmod{m}$ y $ij \equiv ab \pmod{m}$.

□

Con la suma de enteros módulo m tenemos propiedades aritméticas muy buenas. Por ejemplo, la suma es asociativa, conmutativa, la clase [0] funciona perfectamente como neutro aditivo. Adicionalmente, si $i \in \mathbb{Z}_m$, entonces $n-i$ es el inverso aditivo de i. Sin embargo, con el producto no somos muy afortunados. Por ejemplo, si $m = dq$ es compuesto y $1 < d, q < m$, en $\mathbb{Z}_m$ tenemos que $d, q \neq 0$ y $d \cdot q = 0$. En la Sección 2.2 regresaremos nuevamente a discutir la multiplicación de los enteros módulo m.

Definición 1.12. *Sea $m \neq 0$. Un conjunto de enteros $\{x_1, \ldots, x_s\}$ es un sistema reducido de residuos módulo m, el cual escribiremos $SRR(m)$, si dado $y \in \mathbb{Z}$ con $\mathrm{mcd}(y, m) = 1$, existe un único $x_i \in SRR(m)$ tal que $y \equiv x_i \pmod{m}$.*

Es claro que en la definición anterior queda implícito que para $i \neq j, x_i \not\equiv x_j \pmod{m}$. Según el Teorema 1.4 tenemos que los elementos de un $SRR(m)$ deben satisfacer $\mathrm{mcd}(x_i, m) = 1$.

Teorema 1.13. *Si $\{x_1, \ldots, x_s\}$ y $\{y_1, \ldots, y_t\}$ son $SRR(m)$, entonces $s = t$.*

Demostración: Supongamos $s < t$. Como $(y_j, m) = 1$, entonces existe un único $x_i \in \{x_1, \ldots, x_s\}$ tal que $y_j \equiv x_i \pmod{m}$. Reacomodando los índices si es necesario, podemos suponer que $x_j \equiv y_j \pmod{m}$. Para $s + 1 \leq i \leq t$ se tiene $y_i \equiv x_r \equiv y_r \pmod{m}$ para algún $x_r \in \{x_1, \ldots, x_s\}$.

□

Definición 1.14. *La función φ de Euler en el entero positivo m está dado por*

$$\varphi(m) = |SRR(m)|.$$

Según el teorema anterior, cualesquiera dos $SRR(m)$ tienen la misma cardinalidad. Así, la definición de la función φ es consistente. Es fácil ver que el conjunto

$$\{x : 1 \leq x \leq m, \mathrm{mcd}(x, m) = 1\}$$

es un $SRR(m)$. De esta forma $\varphi(1) = 1$, $\varphi(4) = 2$, $\varphi(13) = 12$ y si p es un número primo, entonces $\varphi(p) = p - 1$.

El siguiente resultado lo podemos usar para identificar sistemas reducidos de residuos.

Teorema 1.15. *Si $m > 1$, entonces el conjunto $\{x_1, \ldots, x_{\varphi(m)}\}$ es un SRR(m) si $x_i \not\equiv x_j \pmod m$ para $i \neq j$ y $\mathrm{mcd}(x_i, m) = 1$ para $i = 1, \ldots, \varphi(m)$.*

Demostración: Primero observemos que $x_i = mq_i + r_i$ con $0 < r_i < m$ y $\mathrm{mcd}(r_i, m) = \mathrm{mcd}(x_1, m) = 1$. Por otro lado, puesto que $x_i \not\equiv x_j \pmod m$ para $i \neq j$, los siguientes conjuntos coinciden:

$$\{r_1, r_2, ..., r_{\varphi(m)}\} = \{1 \leq x < m : \ \mathrm{mcd}(x, m) = 1\}.$$

Sea $y \in \mathbb{Z}$ con $\mathrm{mcd}(y, m) = 1$. Entonces existe un único $i \in \{1 \leq x < m : \mathrm{mcd}(x, m) = 1\}$ tal que $y \equiv i \pmod m$. Pero i es congruente con algún $r_i \in \{r_1, r_2, ..., r_{\varphi(m)}\}$. Por transitividad obtenemos el resultado. □

Corolario 1.16. *Si $\mathrm{mcd}(a, m) = 1$ y $\{x_1, \ldots, x_{\varphi(m)}\}$ es un SRR(m), entonces el conjunto $\{ax_1, ..., ax_{\varphi(m)}\}$ también es un SRR(m).*

Demostración: Es evidente que $\mathrm{mcd}(ax_i, m) = 1$ y $ax_i \not\equiv ax_j \pmod m$ para $i \neq j$. □

En la sección 2.3 regresaremos al estudio de los sistemas reducidos de residuos.

Teorema 1.17. [Euler[2]] *Si $\mathrm{mcd}(a, m) = 1$, entonces $a^{\varphi(m)} \equiv 1 \pmod m$.*

Demostración: Si $\{x_1, \ldots, x_{\varphi(m)}\} = \mathrm{SRR}(m)$, entonces $\{ax_1, \ldots, ax_{\varphi(m)}\}$ es un SRR(m). Puesto que cada x_i es congruente a algún ax_j módulo m, tenemos

$$\prod_{i=1}^{\varphi(m)} x_i \equiv \prod_{i=1}^{\varphi(m)} ax_i \equiv a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} x_i \pmod m.$$

Puesto que

$$\mathrm{mcd}\Big(\prod_{i=1}^{\varphi(m)} x_i \ , m\Big) = 1,$$

entonces haciendo uso del Teorema 1.2 obtenemos $a^{\varphi(m)} \equiv 1 \pmod m$.

□

[2]Leonhard Euler nació el 15 de abril de 1707 en Basilea, Suiza. Ingresa a la Universidad de Basilea para estudiar teología y hebreo, pero sus conocimientos y aptitudes en matemáticas atraen la atención de Johan Bernoulli quien le dedica una sesión semanal para responder a sus preguntas. Euler publicó su primera memoria a los dieciocho años y en sus escritos nunca dejó de considerar la potencia deductiva de la inteligencia como la supremacía indiscutible, y aún cuando los resultados del cálculo contradijeran el sentido común, no dudaba en adoptarlos. En todas las ramas de las matemáticas puede encontrarse su nombre. Sus contribuciones principales están en: el cálculo, las ecuaciones diferenciales, la geometría analítica de curvas y superficies, la teoría de números y el cálculo de variaciones. El 7 de septiembre de 1783, después de haber hablado sobre temas populares de la época, como el descubrimiento de Urano, dejó de calcular y vivir.

Los sistemas reducidos de residuos juegan un papel muy importante en teoría de números. Ellos tienen una estructura aritmética muy interesante. Por ejemplo, son cerrados bajo la multiplicación módulo m y cada elemento tiene un inverso multiplicativo. Esto último lo garantiza el Teorema de Euler pues la congruencia $a^{\varphi(m)} \equiv 1 \pmod{m}$ la podemos reescribir como $a \cdot a^{\varphi(m)-1} \equiv 1 \pmod{m}$. De esta forma tenemos que $a^{\varphi(m)-1}$ es el inverso multiplicativo de a si $\varphi(m) \geq 1$. En esencia, estamos describiendo las propiedades algebraicas que definen lo que se conoce como grupo.

Definición 1.18. *Un conjunto $G \neq \emptyset$ es un grupo si existe una función $* : G \times G \to G$ tales que:*

1. *Para $x, y, z \in G$ se tiene $*(x, *(y, z)) = *(*(x, y), z)$.*
2. *Existe un elemento distinguido $e \in G$ tal que $*(e, x) = *(x, e) = x$, para cualquier $x \in G$.*
3. *Si $x \in G$, existe $y \in G$ tal que $*(x, y) = *(y, x) = e$.*

Si escribimos $*(x, y) = x * y$, entonces la definición de grupo queda como:

1. Para $x, y, z \in G$ se tiene $x * (y * z) = (x * y) * z$.
2. Existe un elemento distinguido $e \in G$ tal que $e * x = x * e = x$, para cualquier $x \in G$.
3. Si $x \in G$, existe $y \in G$ tal que $x * y = y * x = e$.

Con esta nueva escritura es fácil identificar la propiedad asociativa, la existencia de un neutro y la existencia de inversos. Adicionalmente, si la función $*$ satisface $x * y = y * x$, entonces diremos que G es un grupo abeliano. El objetivo de haber dado la definición anterior es llamar a las cosas por su nombre. Así tenemos los siguientes ejemplos de grupo abeliano:

1. $\mathbb{Z}$ con $*$ la suma usual de enteros.
2. $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ con $*$ la suma usual de enteros.
2. $\mathbb{Z}_m$ con $*$ la suma módulo m.
3. $SRR(m)$ con $*$ el producto módulo m.

Corolario 1.19. [Pequeño Teorema de Fermat[3]] *Si p es primo y $\text{mcd}(p, a) = 1$, entonces $a^{p-1} \equiv 1 \pmod{p}$.*

[3]En 1640, Fermat comunicó a Bernhard Frénicle este resultado sin demostración. Fue Euler en 1736 el que publicó la primera demostración. Por cierto que se le conoce como *Pequeño Teorema de Fermat* simplemente para distinguirlo del *Último Teorema de Fermat*: Si $n \geq 3$, entonces la ecuación $x^n + y^n = z^n$ no es soluble en enteros x, y, z tales que $xyz \neq 0$. Esta conjetura fue resuelta en 1995 por Andrew Wiles y su estudiante Richard Taylor.

Demostración: Si p es primo, $\varphi(p) = p - 1$.

□

En el Teorema 3.9 de este capítulo presentaremos una generalización del Teorema de Euler.

1.1 Pseudoprimos

En el Pequeño Teorema de Fermat, si $a = 2$ tenemos como caso particular que

$$p \mid 2^p - 2.$$

Hace 25 siglos, los matemáticos chinos creían que el inverso de esta afirmación era cierta. Es decir, si

$$n \mid 2^n - 2,$$

entonces n es primo. Sólo tenían evidencias numéricas para $n \leq 300$. De hecho, esta afirmación es falsa. Por ejemplo,

$$341 \mid 2^{341} - 2$$

y $341 = 11 \cdot 31$. En honor a esta creencia errónea, se dice que un entero compuesto n es *pseudoprimo* si

$$n \mid 2^n - 2.$$

Estos primos *falsos* aparecen con menos frecuencia que los primos *normales*. Por ejemplo, los pseudoprimos ≤ 2000 son $341, 561, 645, 1105, 1387, 1729, 1905$ y la cantidad de primos ≤ 2000 es 307.

PROBLEMAS

1. Demostrar que:
   a) Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces $a + c \equiv b + d \pmod{n}$.
   b) Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces $ac \equiv bd \pmod{n}$.
   c) Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces $ax + cy \equiv bx + dy \pmod{n}$.
   d) Si $d \mid n$ y $a \equiv b \pmod{n}$, entonces $a \equiv b \pmod{d}$.

e) Si $f(x) \in \mathbb{Z}[x]$ y $a \equiv b \pmod{n}$, entonces $f(a) \equiv f(b) \pmod{n}$.

2. Usar el inciso e) del problema anterior para demostrar que:

   a) No existe un polinomio $f(x) \in \mathbb{Z}[x]$ de grado positivo tal que $f(x)$ es un número primo para todo $x \in \mathbb{Z}$.

   b) Cualquier entero es congruente con la suma de sus dígitos módulo 9.

3. ¿Qué día fue el 2 de octubre de 1968? Supongamos que el día de hoy es domingo. Dentro de 1091 días ¿qué día será?

4. Considerar $n = a_0 + a_1 10 + ... + a_k 10^k$ la representación decimal del entero n y $f(x) = a_0 + a_1 x + ... + a_k x^k$. Mostrar que $n = f(10) \equiv f(-1) \pmod{11}$.

5. Sea n un entero de tres dígitos. Si $n = a_0 + a_1 10 + a_2 10^2$ es la representación decimal de n, entonces $n \equiv a_0 + 3a_1 + 2a_2 \pmod{7}$. A partir de lo anterior dar un criterio de divisibilidad por 7 de un entero de tres dígitos. Encontrar un criterio de divisibilidad entre 7 para un número de $4, 5$ ó 6 dígitos . ¿Se puede generalizar para un número de k cifras?

6. Usar el problema 4 para dar un criterio de divisibilidad por 11.

7. Usar el problema 4 para demostrar que $(356)^2 \neq 126732$.

8. Usar el Pequeño Teorema de Fermat para:

   a) Encontrar el residuo que se obtiene al dividir 3^{457} entre 17.

   b) Resolver la congruencia $x^{132} \equiv 5 \pmod{31}$.

   c) Resolver la congruencia $x^{221} \equiv 8 \pmod{13}$.

   d) Resolver la congruencia $x^4 \equiv 7 \pmod{29}$.

9. Usar el Pequeño Teorema de Fermat para justificar que el número 6663 no es primo. Sugerencia: encontrar $a \in \mathbb{Z}$ tal que $a^{6663} \not\equiv a \pmod{6663}$.

10. Encontrar algunos dígitos de 9^{9^9}.

11. Si contamos con los dedos de una mano comenzando por el dedo índice y terminamos con el pulgar ¿en qué dedo terminará $3^{3^{3^3}}$ ó $11^{11^{11}}$?

12. Mostrar que $\varphi(n) = n - 1$ si y sólo si n es primo.

13. Encontrar un entero positivo n tal que $\varphi(n)$ es impar.

14. ¿Qué se puede decir de n si $\varphi(n)$ es el cuadrado de un primo?

15. Encontrar todos los valores de n para los cuales $\varphi(n) = n/2$.

16. Observe por medio de ejemplos que $\varphi(n)$ casi siempre es divisible por 4. Describir todos los enteros n para los cuales $\varphi(n)$ no es divisible por 4.

17. Un número compuesto m se llama *número de Carmichael* si la congruencia $a^m \equiv a \pmod{m}$ es soluble para todo entero a. En particular, esta clase de números son pseudoprimos y son muy difíciles de calcular. En 1912, Robert D. Carmichael conjeturó que hay una infinidad de ellos y fue hasta 1994 que se demostró que esta conjetura es cierta [**?**].

    a) Verificar que el entero $m = 561 = 3 \cdot 11 \cdot 17$ es un número de Carmichael. Sugerencia: si $\text{mcd}(a, p) = 1$ para $p = 3, 7, 11$, mostrar que $a^{560} \equiv 1 \pmod{p}$ usando el Pequeño Teorema de Fermat.

    b) Encontrar algunos números de Carmichael usando el siguiente criterio: si $n = (6m+1)(12m+1)(18m+1)$ y $6m+1,\ 12m+1,\ 18m+1$ son números primos, entonces n es un número de Carmichael. Por ejemplo, $1729 = 7 \cdot 13 \cdot 19$.

18. Mostrar usando sólo congruencias que 341, 561 y 161038 son pseudoprimos. El último número fue descubierto por D.H. Lehmer en 1950 y es el primer número pseudoprimo par.

19. Sea n un pseudoprimo impar. Mostrar que $2^n - 1$ también es pseudoprimo. Concluir que existe una infinidad de pseudoprimos. Sugerencia: mostrar que $2^n = nk + 2$ para algún entero $k \geq 1$ y luego observar que $2^n - 1 \mid (2^n)^k - 1$.

20. Mostrar que la ecuación $5^n + 2 = 17^m$ no tiene solución en los enteros positivos n, m.

21. Encontrar $x \in \mathbb{Z}$ tal que $1^4 + 2^4 + 3^4 + \ldots + 50^4 \equiv x \pmod{5}$.

22. Encontrar el residuo que resulta al dividir $1 + 2! + 3! + \cdots + 147!$ entre 21.

23. Mostrar que un $SRR(n)$ es cerrado bajo la multiplicación módulo n.

24. Encontrar un $SCR(19)$ que contenga sólo múltiplos de 4.

25. Usando la definición de $SRR(m)$ mostrar que $\{1, 2, 4, 5, 7, 8\}$ es un sistema reducido de residuos módulo 9.

26. Sea $n > 1$. Mostrar que $SRR(n) = \{1, 2, \ldots, n-1\}$ si y sólo si n es un número primo.

27. Si $\text{mcd}(a, n) = 1$, entonces para $x \in \mathbb{Z}$ se tiene que

$$SCR(n) = \{x, x + a, x + 2a, \ldots x + (n-1)a\}.$$

28. Mostrar que cualquier conjunto de n enteros consecutivos es un $SCR(n)$.

29. Sea $A = \{x_1, ..., x_{\varphi(n)}\}$ un conjunto de $\varphi(n)$ enteros tal que $x_i \not\equiv x_j \pmod{n}$ si $i \neq j$. Mostrar que A no necesariamente es un $SRR(n)$, es decir, la hipótesis $\text{mcd}(x_i, n) = 1$ en el Teorema 1.15 es indispensable.

30. Mostrar con un ejemplo que si

$$\{x_1, ..., x_{\varphi(m)}\} = SRR(m), \quad \{y_1, ..., y_{\varphi(n)}\} = SRR(n),$$

entonces no necesariamente el conjunto

$$\{x_i y_j : 1 \leq i \leq \varphi(m),\ 1 \leq j \leq \varphi(n)\}$$

es un $SRR(mn)$.

31. Sea $SRR(n) = \{r_1, r_2, ..., r_{\varphi(n)}\}$. Mostrar que $\displaystyle\sum_{i=1}^{\varphi(n)} r_i = \frac{n\varphi(n)}{2}$.

32. Mostrar que si $\text{mcd}(n, 7) = 1$, entonces $7 \mid n^6 - 1$.

33. Mostrar que si $\text{mcd}(n, 7) = 1$, entonces $7 \mid n^{12} - 1$.

34. Mostrar que $5 \mid n^{13} - n$ para todo $n \in \mathbb{N}$.

35. Sea $U_n = \{a \in \mathbb{Z}_n : ax \equiv 1 \pmod{n} \text{ es soluble}\}$. Mostrar que:

    a) Si $a, b \in U_n$, entonces $ab \in U_n$.
    b) Si $a \in U_n$ y b es solución de $ax \equiv 1 \pmod{n}$, entonces $b \in U_n$.
    c) $|U_n| = \varphi(n)$.
    d) Si p es primo, entonces $U_p = \{1, 2, ..., p-1\}$.
    e) Mostrar que si $U_n = \{1, 2, \ldots, n-1\}$, entonces n es primo.
    f) Encontrar alguna relación entre U_n y $SRR(n)$.

36. Si $a \in U_n$, entonces decimos que a es una unidad de $\mathbb{Z}_n$. Encontrar todas las unidades en:

    a) $\mathbb{Z}_5$,
    b) $\mathbb{Z}_{11}$,
    c) $\mathbb{Z}_{14}$,
    d) $\mathbb{Z}_{2999}$.

37. Si p es primo, entonces $x^p \equiv x \pmod{p}$ para toda $x \in \mathbb{Z}$. En particular, si $a, b \in \mathbb{Z}$, entonces $(a+b)^p \equiv a + b \pmod{p}$.

38. Sea p un número primo y $f(x) = x^{2p} - x^p + 1$. Mostrar que $13 \mid f(10)$.

39. Sea p un primo impar. Mostrar que:

    a) $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \pmod{p}$.
    b) $1^p + 2^p + 3^p + \ldots + (p-1)^p \equiv 0 \pmod{p}$.

40. Si p, q son primos diferentes, entonces $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

41. Sea $x \in \mathbb{Z}$. Demostrar que $x^2 \equiv 0 \pmod 4$ ó $x^2 \equiv 1 \pmod 4$. ¿Es cierto que si $x \equiv 0, 1 \pmod 4$, entonces x es un cuadrado? Verificar que el número 7313559 no es un cuadrado.

42. Un entero a tiene la expresión decimal $a = 5x72$. Encontrar x de tal forma que $a \equiv 1 \pmod 9$.

2 La congruencia $ax + b \equiv 0 \pmod m$

En esta sección principia nuestro estudio de la congruencia $f(x) \equiv 0 \pmod m$, donde $f(x)$ es un polinomio con coeficientes en $\mathbb{Z}$. Sea m un entero diferente de 0. Si $f(x) = a_0 + a_1x + ... + a_nx^n$ y $a_i \in \mathbb{Z}$, entonces escribiremos $f(x) \in \mathbb{Z}[x]$.

Definición 2.1. *Sea $f(x) \in \mathbb{Z}[x]$. Si $a \in \mathbb{Z}$ satisface que $f(a) \equiv 0 \pmod m$, entonces diremos que a es una raíz de $f(x)$ módulo m.*

Convenimos en que dos raíces a, b son la "misma" raíz, si éstas satisfacen $a \equiv b \pmod m$. En este sentido, la congruencia $f(x) \equiv 0 \pmod m$ tiene solución única, si cualesquiera dos raíces son congruentes módulo m. Esta idea de aglutinar aquellas raíces que son congruentes es consecuencia de la parte 5 del Teorema 1.1.

Definición 2.2. *Si $f(x) = a_0 + a_1x + \ldots + a_nx^n$ y n es el mayor entero positivo tal que $a_n \not\equiv 0 \pmod m$, entonces diremos que el grado de $f(x)$ módulo m es n.*

Como caso particular, si $n = 1$ entonces $f(x) = a_0 + a_1x$ es un polinomio lineal módulo m si $a_1 \not\equiv 0 \pmod m$. Una aplicación del Teorema de Euler nos da las soluciones de una congruencia lineal.

Proposición 2.3. *Sea $f(x) = ax + b \in \mathbb{Z}[x]$ y $\text{mcd}(m, a) = 1$ con $m \neq 0$. La congruencia $f(x) \equiv 0 \pmod m$ tiene solución única módulo m.*

Demostración: Según el Teorema de Euler 1.17, $a^{\varphi(m)} \equiv 1 \pmod m$. Entonces

$$-a^{\varphi(m)}b \equiv -b \pmod m.$$

Ponemos $x = -a^{\varphi(m)-1}b$ y por tanto $ax + b \equiv 0 \pmod m$.

Si x_1 es otra solución, entonces $ax_1 + b \equiv ax + b \pmod m$. Cancelando obtenemos $x_1 \equiv x \pmod m$.

□

Corolario 2.4. *Sean* $a, b, c, m \in \mathbb{N}$ *tal que* $\text{mcd}(a, m) = \text{mcd}(b, \varphi(m)) = 1$. *Si* $d \in \mathbb{N}$ *es tal que* $bd \equiv 1 \pmod{\varphi(m)}$ *y* $a^b \equiv c \pmod{m}$, *entonces* $a \equiv c^d \pmod{m}$.

Demostración: En realidad el entero d existe porque por $\text{mcd}(b, \varphi(m)) = 1$. Puesto que $bd = \varphi(m)q + 1$, evaluemos:

$$c^d \equiv a^{bd} \equiv a^{\varphi(m)q+1} \equiv a^{\varphi(m)q} a \equiv a \pmod{m}.$$

□

Notemos que si conocemos los enteros m, b y a^b, entonces para recuperar el valor de a, es suficiente determinar el valor de d, para lo cual se requiere conocer $\varphi(m)$ y por lo tanto, es suficiente conocer la factorización de m. Esto puede resultar extremadamente complicado y es parte del éxito de los códigos modernos.

La congruencia $ax + b \equiv 0 \pmod{m}$ es la misma que $ax \equiv -b \pmod{m}$. Así, con un cambio apropiado de signo podemos pensar en $ax \equiv b \pmod{m}$. Lo anterior tiene su semejanza con la aritmética usual de $\mathbb{Z}$: La ecuación $ax = b$ es soluble en $\mathbb{Z}$ si y sólo si $a \mid b$. El siguiente resultado generaliza a la proposición anterior.

Corolario 2.5. *Sea* $g = \text{mcd}(a, m)$. *Si* $g \nmid b$, *entonces* $ax \equiv b \pmod{m}$ *no es soluble. Si* $g \mid b$, *entonces la congruencia* $ax \equiv b \pmod{m}$ *tiene* g *soluciones incongruentes.*

Demostración: Sea $a = ga_0$, $m = gm_0$ y x_0 una solución de $ax \equiv b \pmod{m}$. Entonces

$$ax_0 - b = mt_0 \qquad \text{y} \qquad b = ax_0 - mt_0 = g(a_0x_0 - m_0t_0).$$

De lo anterior se sigue que si $g \nmid b$, entonces la congruencia $ax \equiv b \pmod{m}$ no puede tener solución.

Ahora consideremos la congruencia $ax \equiv b \pmod{m}$ junto con la hipótesis $g \mid b$. Si u es solución de $ax \equiv b \pmod{m}$, entonces

$$m \mid au - b,$$

así que

$$\frac{m}{g} \mid \frac{a}{g}u - \frac{b}{g},$$

y u es solución de

$$\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}.$$

Por tanto tenemos que u es solución de $ax \equiv b \pmod{m}$ si y sólo si u es solución de $\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$. Sea x_1 alguna solución particular de

$$\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}.$$

Entonces $x_1 + t\frac{m}{g}$ es solución de $\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$ y también es solución de $ax \equiv b \pmod{m}$.

Un simple cálculo muestra que si $t_1, t_2 \in \{0, 1, ..., g-1\}$ con $t_1 \neq t_2$, entonces

$$x_1 + t_1\frac{m}{g} \not\equiv x_1 + t_2\frac{m}{g} \pmod{m}.$$

Sólo falta probar que cualquier solución de $ax \equiv b \pmod{m}$ es de la forma $x_1 + t\frac{m}{g}$, donde x_1 es una solución particular de

$$\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}.$$

Como $\text{mcd}\left(\frac{a}{g}, \frac{m}{g}\right) = 1$, entonces la congruencia

$$\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}},$$

tiene solución única x_1 módulo $\frac{m}{g}$. Sea u cualquier solución de $ax \equiv b \pmod{m}$. Puesto que u también es solución de

$$\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}},$$

entonces se tiene

$$u \equiv x_1 \pmod{\frac{m}{g}}.$$

De lo anterior, $u = t\frac{m}{g} + x_1$, para algún $t \in \mathbb{Z}$.

□

Observemos que en el corolario anterior las soluciones de $ax \equiv b \pmod{m}$, dependen esencialmente de las soluciones de

$$\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}.$$

En el curso de la demostración del corolario anterior obtuvimos un método seguro para resolver una congruencia lineal. Sin embargo, para valores muy grandes de m, este método puede ser poco eficaz. La manera en que podemos resolver una congruencia lineal con módulo grande está descrita en el Teorema 1.3. Se trata de descomponer el módulo en factores primos y plantear un sistema de congruencias. Después se resuelve cada congruencia y nuevamente por el Teorema 1.3 se recupera una solución de la congruencia original. A pesar de lo anterior, descomponer un número en sus factores primos también puede ser una tarea bastante complicada.

Estamos seguros que cualquier lector ha manipulado en no pocas ocasiones al campo de los números reales $\mathbb{R}$. La aritmética de este conjunto descansa esencialmente en la suma y el producto y en las propiedades que estas operaciones satisfacen. En especial, sabemos que si a y b son números reales diferentes de 0, entonces $ab \neq 0$.

Definición 2.6. *Un campo es un conjunto K con dos operaciones binarias que llamaremos suma$(+)$ y producto$(\cdot)$. Ambas operaciones son asociativas, conmutativas y K contiene dos elementos distinguidos que denotaremos por* $0,\ 1$ *(neutro aditivo y neutro multiplicativo respectivamente) y tal que*

1. $0 + a = a$ *para* $a \in K$.
2. *Para* $a \in K$, *existe* $b \in K$ *tal que* $a + b = 0$ *(existencia de inverso aditivo).*
3. $a \cdot 1 = a$ *para* $a \in K$.
4. *Si* $a \in K$ *y* $a \neq 0$, *existe* $b \in K$ *tal que* $a \cdot b = 1$ *(existencia de inverso multiplicativo).*
5. *Para* $a, b, c \in K$ *se tiene* $a(b + c) = ab + ac$ *(ley distributiva).*

Si recordamos la definición de grupo, veremos que un campo es un grupo abeliano con dos operaciones diferentes que además están relacionadas por la propiedad 5 de la definición de campo.

Un ejemplo muy importante de campo es $\mathbb{Z}_p$ si p es primo. La asociatividad y conmutatividad de la suma y producto módulo p son consecuencia directa de la asociatividad y conmutatividad de la suma y producto de números enteros. El neutro aditivo y multiplicativo son [0] y [1] respectivamente. También es claro que todos los elementos de $\mathbb{Z}_p$ tienen inverso aditivo. En general tenemos:

Corolario 2.7. $\mathbb{Z}_n$ *es un campo si y sólo si* n *es un número primo.*

Demostración: Supongamos que $\mathbb{Z}_n$ es un campo y $n = ab$. En particular, a tiene inverso multiplicativo. Es decir, la congruencia $ax \equiv 1 \pmod{n}$ tiene solución única. Según el Corolario 2.5 $\text{mcd}(a, n) \mid 1$ y así $\text{mcd}(a, n) = 1$. Por otro lado, $a \mid n$ y por lo tanto $\text{mcd}(a, n) = a = 1$.

Inversamente, si n es primo, entonces para $1 \leq a \leq n - 1$ se tiene que $\text{mcd}(a, n) = 1$ y la congruencia $ax \equiv 1 \pmod{n}$ tiene solución única. Es decir, a tiene inverso multiplicativo. La ley distributiva en $\mathbb{Z}_p$ es consecuencia de la propiedad distributiva de $\mathbb{Z}$.

□

Según el corolario anterior, existe una infinidad de *campos finitos*, uno para cada primo p. No todos los campos finitos tienen p elementos. Se puede probar que cualquier campo finito tiene como cardinalidad una potencia de un número primo. Está fuera de nuestro alcance la justificación de este hecho. En el resto de este trabajo escribiremos $\mathbb{F}_p$ en lugar de $\mathbb{Z}_p$ y con esta notación estaremos indicando que $\mathbb{F}_p$ es un campo finito con p elementos. Indicaremos $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$.

PROBLEMAS

1. Resolver cada una de las siguientes congruencias:

   a) $132x \equiv -22 \pmod{194}$.

   b) $84x \equiv 156 \pmod{605}$.

   c) $16x \equiv -3 \pmod{-24}$.

   d) $-5x \equiv 1 \pmod{18}$.

2. Resolver las siguientes ecuaciones usando sólo congruencias:

   a) $9x + 12y = 27$.

   b) $-16x + 7y = 4$.

   c) $143x - 739y = 57$.

   d) $251x + 340y = 136$.

3. Un entero $1 < x < 500$ deja residuos $1, 4, 5$ cuando es dividido entre $2, 5, 7$ respectivamente. Encontrar el valor de x.

4. Encontrar el inverso aditivo y multiplicativo de cada elemento diferente de 0 en cada uno de los siguientes campos finitos:

$$\mathbb{F}_7, \quad \mathbb{F}_{11}, \quad \mathbb{F}_{23}, \quad \mathbb{F}_{43}$$

3 Sistemas de congruencias lineales

En la sección anterior dimos una descripción de cómo resolver $ax \equiv b \pmod{m}$ descomponiendo m como producto de factores primos. Si $m = \prod_{i=1}^{r} p_i^{\alpha_i}$, entonces usando el Teorema 1.3, resolver $ax \equiv b \pmod{m}$ es equivalente a resolver el sistema de congruencias $ax \equiv b \pmod{p_i^{\alpha_i}}$. Si para alguna i se tiene que la congruencia $ax \equiv b \pmod{p_i^{\alpha_i}}$ no es soluble, entonces $ax \equiv b \pmod{m}$ no es soluble.

Con lo anterior tenemos dos problemas a la vista. Uno de ellos es resolver un sistema de congruencias donde los módulos son potencias de primos. El segundo problema consiste en resolver una congruencia donde el módulo es una potencia de un primo. Por el momento estudiaremos un sistema de congruencias relativamente simple.

Teorema 3.1. *Sean $m_1, \ldots, m_r$ enteros diferentes de 0 con $\text{mcd}(m_i, m_j) = 1$ si $i \neq j$. Supongamos que cada una de las congruencias $b_i x \equiv a_i \pmod{m_i}$ tiene al menos una solución. Entonces el sistema*

$$\begin{aligned} b_1 x &\equiv a_1 \pmod{m_1} \\ b_2 x &\equiv a_2 \pmod{m_2} \\ &\vdots \qquad\quad \vdots \\ b_r x &\equiv a_r \pmod{m_r} \end{aligned}$$

es soluble.

Demostración: Sean $m = \prod_{i=1}^{r} m_i$, s_i solución de $\dfrac{m}{m_i} x \equiv 1 \pmod{m_i}$ y x_i solución de $b_i x \equiv a_i \pmod{m_i}$ con $i = 1, \ldots, r$. Entonces el número

$$x = \sum_{i=1}^{r} \frac{m}{m_i} s_i x_i$$

es solución de cada una de las congruencias del sistema.

□

Ejemplo 3.2. *Como ejemplo consideremos el sistema*

$$\begin{aligned} 3x &\equiv 1 \pmod{7} \\ 8x &\equiv -2 \pmod{-6} \\ x &\equiv 2 \pmod{5} \end{aligned}$$

Rescatando las hipótesis del Teorema 3.1 tenemos:

$$\begin{array}{rcrcrcl} x_1 & = & -2 & \textit{es solución de} & 3x & \equiv & 1 \pmod 7 \\ x_2 & = & -1 & \text{"} & 8x & \equiv & -2 \pmod{-6} \\ x_3 & = & 2 & \text{"} & x & \equiv & 2 \pmod 5 \\ s_1 & = & -4 & \text{"} & (-6)(5)x & \equiv & 1 \pmod 7 \\ s_2 & = & -1 & \text{"} & (7)(5)x & \equiv & 1 \pmod{-6} \\ s_3 & = & 2 & \text{"} & (7)(-6)x & \equiv & 1 \pmod 5 \end{array}$$

Por tanto

$$x = (-6)(5)(-2)(-4) + (7)(5)(-1)(-1) + (7)(-6)(2)(2) = -373$$

es solución del sistema.

Corolario 3.3. [Teorema Chino del Residuo[4]] *Sean $m_1, \ldots, m_r$ enteros diferentes de 0 y primos relativos por pares. Si $a_1, \ldots, a_r \in \mathbb{Z}$, entonces el sistema de congruencias*

$$\begin{array}{rl} x & \equiv a_1 \pmod{m_1} \\ x & \equiv a_2 \pmod{m_2} \\ \vdots & \quad \vdots \\ x & \equiv a_r \pmod{m_r} \end{array}$$

tiene solución única módulo $\text{mcm}(m_1, ..., m_r)$.

Demostración: Se tiene que $x = a_i$ es solución de $x \equiv a_i \pmod{m_i}$. Ahora apliquemos el Teorema 3.1.

□

Notemos que en el Teorema Chino del Residuo, la hipótesis $\text{mcd}(m_i, m_j) = 1$, $i \neq j$ es indispensable pues de esta forma se asegura la existencia de una solución del sistema. Si para algún par de índices $i \neq j$ se tiene $\text{mcd}(m_i, m_j) > 1$, entonces todo puede suceder. Por ejemplo, se puede verificar fácilmente que el sistema

$$\begin{array}{rcl} x & \equiv & 1 \pmod 6 \\ x & \equiv & 3 \pmod{15} \end{array}$$

no tiene solución. En la misma dirección tenemos que $x = 18$ es solución del sistema

$$\begin{array}{rcl} x & \equiv & 0 \pmod 6 \\ x & \equiv & 3 \pmod{15} \end{array}$$

[4]El calendario solar chino fue elaborado entre el siglo VII y el siglo IV a.c. y se usó para encontrar períodos en común a varios ciclos de fenómenos astronómicos. De manera sorprendente, este calendario da una regla para resolver un sistema lineal de congruencias.

Apliquemos el Teorema Chino del Residuo para mostrar que la función φ es multiplicativa.

Teorema 3.4. *Si* $\mcd(m,n)=1$*, entonces* $\varphi(mn)=\varphi(m)\varphi(n)$.

Demostración: De manera natural tenemos tres sistemas de residuos involucrados:

$$SRR(mn)=\{x_1,\ldots,x_t\},\ \ SRR(m)=\{r_1,\ldots,r_k\},\ \ SRR(n)=\{s_1,\ldots,s_j\}$$

donde $t=\varphi(mn)$, $k=\varphi(m)$ y $j=\varphi(n)$. La idea de la demostración es construir una función biyectiva

$$f:\{x_1,\ldots,x_t\}\longrightarrow\{r_1,\ldots,r_k\}\times\{s_1,\ldots,s_j\}.$$

Observemos que para $i=1,\ldots,t$ se tiene $\mcd(x_i,mn)=1$. Por lo tanto $\mcd(x_i,m)=\mcd(x_i,n)=1$. Como $\mcd(x_i,m)=1$, entonces existe un único r_α en $SRR(m)$ tal que $x_i\equiv r_\alpha \pmod m$. De la misma manera podemos escoger un único $s_\beta\in SRR(n)$ tal que $x_i\equiv s_\beta \pmod n$.

Definimos $f(x_i)=(r_\alpha,s_\beta)$. Puesto que r_α,s_β son únicos, entonces f es una función.

Sea $f(x_i)=(r_\alpha,s_\beta)$ y $f(x_j)=(r_\gamma,s_\delta)$. Si $f(x_i)=f(x_j)$, entonces

$$r_\alpha\equiv r_\gamma \pmod m \qquad \text{y} \qquad s_\beta\equiv s_\delta \pmod n.$$

Por lo tanto f es inyectiva.

Para la suprayectividad consideremos $(r,s)\in SRR(m)\times SRR(n)$. Estudiemos el sistema

$$\begin{aligned} x &\equiv r \pmod m,\\ x &\equiv s \pmod n.\end{aligned}$$

El Teorema Chino del Residuo asegura que el sistema tiene solución única módulo mn. Denotemos por x a la solución. Por el Teorema 1.4 tenemos

$$\mcd(x,m)=\mcd(r,m)=\mcd(x,n)=\mcd(s,n)=1,$$

así $\mcd(x,mn)=1$ y por tanto existe un único $x_i\in SRR(mn)$ tal que

$$x\equiv x_i \pmod{mn}.$$

Claramente $f(x_i)=(r,s)$ y f es entonces suprayectiva. La conclusión es evidente.

□

Sea $n\neq 0$. Entonces $SRR(n)=SRR(-n)$. En nuestra próxima discusión podemos suponer que $n>0$ y que

$$\varphi(n)=|\{x\in\mathbb{N}:1\leq x\leq n,\ \mcd(x,n)=1\}|.$$

Lema 3.5. *Si p es primo, entonces $\varphi(p^n) = p^n - p^{n-1}$.*

Demostración: Notemos primero que si $1 \leq j \leq p-1$, entonces para todo $k \in \mathbb{Z}$ se tiene que $\text{mcd}(pk+j, p) = 1$ y por lo tanto $\text{mcd}(pk+j, p^n) = 1$. Observemos el siguiente arreglo:

$$\begin{array}{ccccc}
1 & 2 & 3 & \cdots & p \\
p+1 & p+2 & p+3 & \cdots & 2p \\
2p+1 & 2p+2 & 2p+3 & \cdots & 3p \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
(p-1)p+1 & (p-1)p+2 & (p-1)p+3 & \cdots & pp \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
(p^{n-1}-1)p+1 & (p^{n-1}-1)p+2 & (p^{n-1}-1)+3 & \cdots & p^{n-1}p.
\end{array}$$

Notamos que en cada renglón existen $p-1$ números que son primos relativos con p. Puesto que hay p^{n-1} renglones, entonces en todo el arreglo hay $p^{n-1}(p-1)$ números que son primos relativos con p^n.

□

Teorema 3.6. *Si $n > 1$, entonces $\varphi(n) = n\prod_{p|n}(1 - \frac{1}{p})$.*

Demostración: Sea $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ donde $p_i \neq p_j$ si $i \neq j$. Entonces

$$\varphi(n) = \varphi(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) =$$

$$\prod_{i=1}^{k} p_i^{\alpha_i}(1 - \frac{1}{p_i}) = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{k}(1 - \frac{1}{p_i}) = n\prod_{p|n}(1 - \frac{1}{p}).$$

□

Corolario 3.7. *Si $n \geq 1$, entonces $\sum_{d|n} \varphi(d) = n$.*

Demostración: Primero mostraremos que $\sum_{d|p^\alpha} \varphi(d) = p^\alpha$. En efecto,

$$\sum_{d|p^\alpha} \varphi(d) = 1 + (p-1) + (p^2 - p) + \ldots + (p^\alpha - p^{\alpha-1}) = p^\alpha.$$

Ahora consideremos la factorización $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. Por lo tanto, usando la multiplicatividad de la función φ tenemos

$$\sum_{d|n} \varphi(d) = \left(\sum_{d|p_1^{\alpha_1}} \varphi(d) \right) \left(\sum_{d|p_2^{\alpha_2}} \varphi(d) \right) \cdots \left(\sum_{d|p_r^{\alpha_r}} \varphi(d) \right) = \prod_{i=1}^{r} p_i^{\alpha_i} = n.$$

□

Lema 3.8. *Si p es primo y $\alpha \geq 1$, entonces $a^{p^\alpha} \equiv a^{p^{\alpha-1}} \pmod{p^\alpha}$.*

Demostración: La prueba es muy sencilla, sólo tenemos que utilizar el binomio de Newton. Sabemos que $a^p \equiv a \pmod{p}$. Esto significa que $a^p = a + kp$ para cierto entero k. Por lo tanto

$$(a^p)^{p^{\alpha-1}} = (a + kp)^{p^{\alpha-1}} = a^{p^{\alpha-1}} + p^\alpha Q.$$

Puesto que el último sumando es 0 módulo p^α, tenemos $a^{p^\alpha} \equiv a^{p^{\alpha-1}} \pmod{p^\alpha}$.
□

Como consecuencia del lema anterior tenemos una generalización del Teorema de Euler.

Teorema 3.9. [Teorema de Euler Generalizado] *Sean $a, m \in \mathbb{Z}$. Entonces*

$$a^{m-\varphi(m)} \equiv a^m \pmod{m}.$$

Demostración: Sea $m = \prod_{i=1}^{n} p_i^{\alpha_i}$. Entonces

$$m - \varphi(m) = \prod_{i=1}^{n} p_i^{\alpha_i} - \varphi\Big(\prod_{i=1}^{n} p_i^{\alpha_i} \Big) =$$

$$\prod_{i=1}^{n} p_i^{\alpha_i} - \varphi\Big(\prod_{i=1}^{n-1} p_i^{\alpha_i} \Big) \varphi(p_n^{\alpha_n}) =$$

$$\prod_{i=1}^{n} p_i^{\alpha_i} - \varphi\Big(\prod_{i=1}^{n-1} p_i^{\alpha_i} \Big) (p_n^{\alpha_n} - p_n^{\alpha_n - 1}) =$$

$$\prod_{i=1}^{n} p_i^{\alpha_i} - \varphi\Big(\prod_{i=1}^{n-1} p_i^{\alpha_i} \Big) (p_n^{\alpha_n}) + \varphi\Big(\prod_{i=1}^{n-1} p_i^{\alpha_i} \Big) (p_n^{\alpha_n - 1}) =$$

$$\left(\prod_{i=1}^{n-1} p_i^{\alpha_i} - \varphi\Big(\prod_{i=1}^{n-1} p_i^{\alpha_i}\Big)\right) p_n^{\alpha_n} + \varphi\Big(\prod_{i=1}^{n-1} p_i^{\alpha_i}\Big)(p_n^{\alpha_n - 1}).$$

Si $x = \prod_{i=1}^{n-1} p_i^{\alpha_i}$, entonces $m - \varphi(m) = (x - \varphi(x))p_n^{\alpha_n} + \varphi(x)p_n^{\alpha_n - 1}$.

Por lo tanto

$$a^{m-\varphi(m)} = a^{(x-\varphi(x))p_n^{\alpha_n} + \varphi(x)p_n^{\alpha_n - 1}} = a^{(x-\varphi(x))p_n^{\alpha_n}} a^{\varphi(x)p_n^{\alpha_n - 1}}.$$

Por el Lema 3.8 tenemos

$$a^{(x-\varphi(x))p_n^{\alpha_n}} \equiv a^{(x-\varphi(x))p_n^{\alpha_n - 1}} \pmod{p_n^{\alpha_n}}.$$

Nuevamente, usando dos veces el Lema 3.8

$$a^{m-\varphi(m)} \equiv a^{(x-\varphi(x))p_n^{\alpha_n - 1}} a^{\varphi(x)p_n^{\alpha_n - 1}} \equiv a^{xp_n^{\alpha_n - 1}} \equiv a^{xp_n^{\alpha_n}} \pmod{p_n^{\alpha_n}}.$$

Puesto que $xp_n^{\alpha_n} = m$, entonces $a^{m-\varphi(m)} \equiv a^m \pmod{p_n^{\alpha_n}}$.

Si en lugar de haber elegido a $p_n^{\alpha_n}$ hubiésemos seleccionado a $p_j^{\alpha_j} (1 \leq j \leq m)$, tendríamos

$$a^{m-\varphi(m)} \equiv a^m \pmod{p_j^{\alpha_j}}.$$

Por lo tanto, por el Teorema 1.3 concluimos que

$$a^{m-\varphi(m)} \equiv a^m \pmod{m}.$$

□

Observemos que si $\text{mcd}(a, m) = 1$, entonces $\text{mcd}(a^m, m) = 1$ y

$$a^{m-\varphi(m)} \equiv a^m a^{-\varphi(m)} \equiv a^m \pmod{m}.$$

Por lo tanto, por el Teorema 1.2 tenemos $a^{-\varphi(m)} \equiv 1 \pmod{m}$. ¿Contradice esto al Teorema de Euler?

PROBLEMAS

1. Calcular $\varphi(1697)$ y $\varphi(1699)$.
2. Mostrar que si n tiene k factores primos impares, entonces $2^k \mid \varphi(n)$.
3. Usar el Teorema 3.6 para mostrar que $\varphi(n) < n$.

4. Sea n un entero positivo compuesto. Mostrar que $\varphi(n) \leq n - \sqrt{n}$. Sugerencia: Si p es el menor primo que divide a n, entonces $p \leq \sqrt{n}$ y así $\varphi(n) \leq n(1 - \frac{1}{p})$.

5. Mostrar que si $d \mid n$, entonces $\varphi(d) \mid \varphi(n)$.

6. Mostrar que existe una infinidad de enteros n tal que $\varphi(n)$ es un cuadrado perfecto.

7. Mostrar que $\varphi(n) = \varphi(2n)$ si y sólo si n es impar.

8. Mostrar que si n es par, entonces $\varphi(2n) = 2\varphi(n)$.

9. Mostrar que $\varphi(3n) = 3\varphi(n)$ si y sólo si $3 \mid n$.

10. Mostrar que $\varphi(3n) = 2\varphi(n)$ si y sólo si $3 \nmid n$.

11. Si p y $p + 2$ son primos gemelos, entonces $\varphi(p + 2) = \varphi(p) + 2$.

12. Si $d \mid n$, entonces $\varphi(d) \mid \varphi(n)$.

13. Si $d \mid n$ y $0 < d < n$, entonces $d - \varphi(d) < n - \varphi(n)$.

14. Si $m, n \in \mathbb{Z}$ y $g = \text{mcd}(m, n)$, entonces $\varphi(m)\varphi(n) = \dfrac{\varphi(mn)\varphi(g)}{g}$. Observar que este resultado generaliza al Teorema 3.4.

15. Si $m, n \geq 1$, entonces $\varphi(m)\varphi(n) = \varphi(\text{mcd}(m, n))\varphi(\text{mcm}(m, n))$. ¿Por qué este resultado generaliza al Teorema 3.4?

16. Si p es primo y $h + k = p - 1$ con h, k positivos, entonces

$$h!k! + (-1)^h \equiv 0 \pmod{p}.$$

17. Mostrar que si p es primo, entonces $(p - 1)! \equiv p - 1 \pmod{\sum_{i=1}^{p-1} i}$.

18. ¿Qué se puede decir si en el Teorema Chino del Residuo algún $m_i = 0$?

19. Considerar la siguiente colección de congruencias:

    a) $x \equiv -3 \pmod 7$
    b) $x \equiv -2 \pmod{11}$
    c) $x \equiv 7 \pmod{12}$
    d) $x \equiv 4 \pmod{13}$
    e) $x \equiv 8 \pmod{14}$
    f) $x \equiv -5 \pmod{15}$
    g) $x \equiv -2 \pmod{17}$

h) $x \equiv -1 \pmod{18}$.

Resolver el sistema de congruencias para cada una de las siguientes elecciones:

i) a) y b).

ii) a), c) y d).

iii) b), d), y g).

iv) a), e) y f).

v) a), b), d), g), h).

20. Resolver los siguientes sistemas de congruencias:

$$\begin{array}{rcrl} 3x & \equiv & 5 & \pmod{22} \\ 11x & \equiv & 3 & \pmod{28} \\ 5x & \equiv & 89 & \pmod{99}, \end{array} \qquad \begin{array}{rcrl} -2x & \equiv & 1 & \pmod{4} \\ 5x & \equiv & -2 & \pmod{7} \\ x & \equiv & 0 & \pmod{-99}. \end{array}$$

21. Mostrar que el sistema de congruencias

$$\begin{array}{rcl} x & \equiv & a \pmod{m} \\ x & \equiv & b \pmod{n} \end{array}$$

tiene solución si y sólo si $\mathrm{mcd}(m,n) \mid a-b$.

22. Sin usar el problema anterior, demostrar que el sistema de congruencias

$$\begin{array}{rcl} x & \equiv & 1 \pmod{6} \\ x & \equiv & 3 \pmod{15} \end{array}$$

no tiene solución.

23. Sean m, n enteros positivos tales que $\mathrm{mcd}(m,n) = 1$. Considerar la lista de enteros $1 \le x \le mn$:

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

En la j-ésima columna, una entrada típica es de la forma $am + j$ con j fija y $1 \le j \le m$.

a) Mostrar que $\mathrm{mcd}(am+j, m) = \mathrm{mcd}(j, m)$ para $1 \le j \le m$. Concluir que todas las entradas de la j-ésima columna o son primos relativos con m o todas las entradas no lo son.

b) Mostrar que hay exactamente $\varphi(m)$ columnas que contienen todas sus entradas primos relativos con m.

c) Mostrar que todas las entradas de la j-ésima columna forman un $SCR(n)$ y concluir que en ella existen $\varphi(n)$ enteros que son primos relativos con n.

d) Usar los tres incisos anteriores para mostrar que en toda la lista existen $\varphi(m)\varphi(n)$ enteros primos relativos con mn. Comparar con el Teorema 3.4.

24. Sea $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la factorización del entero m y donde $p_i \neq p_j$ si $i \neq j$. Considerar el polinomio $f(x) = a_0 + a_1 x + \ldots a_n x^n$ con $a_i \in \mathbb{Z}$. Usar el Teorema Chino del Residuo para justificar que la congruencia $f(x) \equiv 0 \pmod{m}$ es soluble si y sólo si cada una de las congruencias $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$, $1 \leq i \leq k$ es soluble.

25. Encontrar un entero positivo x que al ser dividido por $3, 4, 5$ y 6 deja residuo $2, 3, 4$ y 5 respectivamente (Brahmagupta siglo 7 a.c). Observar que no se puede aplicar el Teorema Chino del residuo. Sugerencia: Usar el Teorema Chino del Residuo en las tres primeras congruencias y dar la forma general de la solución. Después considerar la última congruencia módulo 6 y la solución general que se obtuvo al resolver las tres primeras congruencias.

26. Encontrar tres enteros consecutivos tal que cada uno de ellos es divisible por un cuadrado > 1.

27. Supongamos que queremos deshacernos de una cierta cantidad de teclados viejos de computadora. Si los guardamos en cajas de 7 sobran 5 y si los guardamos en cajas de 11 sobran 3, pero si los guardamos en cajas de 8 no sobra alguno. ¿Cuántos teclados tenemos?

3.1 La ecuación $\varphi(x) = n$

Como una aplicación de lo que hemos estudiado acerca de la función φ, resolveremos la ecuación $\varphi(x) = n$ con $n \in \mathbb{N}$. Claramente $n > 1$ impar implica que $\varphi(x) = n$ no es soluble. El método que proponemos depende principalmente de la factorización del entero n. Esto puede complicar encontrar la solución, en caso de que exista. Sin embargo, con la ayuda de una computadora y con un programa adecuado, el método se puede implementar para valores grandes de n. Esto de ninguna manera significa que el algoritmo que proponemos sea el más eficiente. Simplemente estamos afirmando que se puede implementar escribiendo un programa en lenguaje C o algún otro, o instalando en tu computadora algún paquete de álgebra computacional, por ejemplo GAP o MAGMA. En todo caso sugerimos intentar escribir un programa, pues es más creativo que ser un simple ejecutante de programas ya establecidos.

Sea $x = \prod p_i^{\alpha_i}$ con $p_i \neq p_j$ para $i \neq j$. Entonces

$$\varphi(x) = \prod p_i^{\alpha_i} \frac{p_i - 1}{p_i} = n.$$

Si definimos $d_i = p_i - 1$, de la igualdad $\prod p_i^{\alpha_i} \dfrac{d_i}{p_i} = n$ obtenemos que $d_i \mid n$ y

$$x = \frac{n}{\prod d_i} \prod p_i.$$

Puesto que $d_i \neq d_j$ para $i \neq j$ y $d_i \mid n$, entonces $\prod d_i$ es un producto de divisores de n (no necesariamente todos) tal que $d_i + 1$ es un primo p_i. De la igualdad

$$\frac{n}{\prod d_i} = \prod p_i^{\alpha_i - 1},$$

se obtiene que cualquier divisor primo de $\dfrac{n}{\prod d_i}$ necesariamente debe ser algún p_i. Esta última afirmación es una condición adicional para x.

Como ejemplo, consideremos la ecuación $\varphi(x) = 4$. Los números d_i que dividen a 4 y tal que $d_i + 1 = p_i$ es un número primo son

$$d_1 = 1, \quad d_2 = 2, \quad d_3 = 4.$$

Por lo tanto $p_1 = 2,\ p_2 = 3,\ p_3 = 5$. Consideremos los posibles $\prod d_i$ tal que $\dfrac{4}{\prod d_i}$ es un entero. Recordemos que sólo debemos tomar en cuenta aquellos números de la forma $\dfrac{4}{\prod d_i}$ tal que cualquier divisor primo de éste sea algún p_i. Con lo anterior construimos la siguiente tabla:

$$\begin{array}{lcl l lcl}
\dfrac{4}{d_1} & = & 4 & \text{y así} & x & = & \dfrac{4}{d_1} p_1 = 8 \\
\dfrac{4}{d_2} & = & 2 & \text{"} & x & = & \dfrac{4}{d_2} p_2 = 6 \\
\dfrac{4}{d_3} & = & 1 & \text{"} & x & = & \dfrac{4}{d_3} p_3 = 5 \\
\dfrac{4}{d_1 d_2} & = & 2 & \text{"} & x & = & \dfrac{4}{d_1 d_2} p_1 p_2 = 12 \\
\dfrac{4}{d_1 d_3} & = & 1 & \text{"} & x & = & \dfrac{4}{d_1 d_2} p_1 p_3 = 10
\end{array}$$

Con los valores obtenidos de x se pueden observar que las soluciones de $\varphi(x) = 4$ son $x = 5,\ 8,\ 10,\ 12$.

PROBLEMAS

1. Encontrar todas las soluciones de $\varphi(x) = 26$ y $\varphi(x) = 24$.

2. Sea p un número primo tal que $2p + 1$ es compuesto. Mostrar que la ecuación $\varphi(x) = 2p$ no tiene solución.

3. Mostrar que si p y $2p + 1$ son primos, entonces $\varphi(x) = 2p$ es soluble. Analizar los casos $p = 2$ y $p \neq 2$ y contar todas las soluciones.

4. Mostrar que 14 es el menor entero positivo par para el cual $\varphi(x) = 14$ no es soluble.

5. Mostrar que la ecuación $\varphi(x) = n$ tiene un número finito de soluciones.

6. Supongamos que p y $2p - 1$ son primos impares. Por ejemplo 7 y 13. Si $n = 2(2p - 1)$, entonces $\varphi(n) = \varphi(n + 2)$.

7. Supongamos que la ecuación $\varphi(x) = n$ tiene solución única. Sea n_0 tal que $\varphi(n_0) = n$. Mostrar que $4 \mid n_0$. Una conjetura de R. Carmichael asegura que el número de soluciones de $\varphi(x) = n$ no puede ser 1. Este es un buen problema de investigación y te invitamos a averiguar cuál es el estado del arte de esta conjetura.

4 La congruencia $f(x) \equiv 0 \pmod{m}$

En esta sección seguiremos con nuestro estudio de las raíces de una congruencia de la forma $f(x) \equiv 0 \pmod{m}$. El objetivo del siguiente resultado consiste en mostrar que la solubilidad de $f(x) \equiv 0 \pmod{m}$ depende esencialmente de la solubilidad de $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$, donde $m = \prod_{i=1}^{k} p_i^{\alpha_i}$.

Teorema 4.1. *Si $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ y $f(x) \in \mathbb{Z}[x]$ no es un polinomio constante, entonces $f(x) \equiv 0 \pmod{m}$ tiene solución si y sólo si para cada i, la congruencia $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ es soluble. Mas aún, si t_i denota el número de soluciones de $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$, entonces $f(x) \equiv 0 \pmod{m}$ tiene exactamente $t_1 t_2 \cdots t_k$ soluciones incongruentes módulo m.*

Demostración: Si $f(x) \equiv 0 \pmod{m}$ tiene solución, entonces por el Teorema 1.1 parte 4, cada una de las congruencias $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ es soluble. Inversamente, si x_i denota una solución de $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$, entonces el Teorema Chino del Residuo asegura que el sistema

$$\begin{aligned} x &\equiv x_1 \pmod{p_1^{\alpha_1}} \\ x &\equiv x_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \quad\quad \vdots \\ x &\equiv x_k \pmod{p_k^{\alpha_k}}, \end{aligned}$$

tiene solución única x. De lo anterior

$$f(x) \equiv f(x_i) \equiv 0 \pmod{p_i^{\alpha_i}},$$

y aplicando el Teorema 1.3 obtenemos que $f(x) \equiv 0 \pmod{m}$. Para terminar nuestro resultado sólo nos resta contar las soluciones de la congruencia $f(x) \equiv 0 \pmod{m}$.

Consideremos los siguientes conjuntos:

$$\begin{aligned} T_1 &= \{x_{11}, x_{21}, \ldots, x_{t_1 1}\}, \\ T_2 &= \{x_{12}, x_{22}, \ldots, x_{t_2 2}\}, \\ &\vdots \quad\quad \vdots \\ T_k &= \{x_{1k}, x_{2k}, \ldots, x_{t_k k}\}, \end{aligned}$$

donde el i-ésimo conjunto denota las soluciones de $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$. Para $(x_{i_1 1}, x_{i_2 2}, ..., x_{i_k k}) \in T_1 \times T_2 \times \cdots \times T_k$ tenemos que el sistema de congruencias

$$\begin{aligned} x &\equiv x_{i_1 1} \pmod{p_1^{\alpha_1}} \\ x &\equiv x_{i_2 2} \pmod{p_2^{\alpha_2}} \\ &\vdots \quad\quad \vdots \\ x &\equiv x_{i_k k} \pmod{p_k^{\alpha_k}}, \end{aligned}$$

tiene solución única módulo m por el Teorema Chino del Residuo. De lo anterior y por el Teorema 1.1 parte 5, concluimos que

$$\begin{aligned} f(x) &\equiv f(x_{i_1 1}) \equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) &\equiv f(x_{i_2 2}) \equiv 0 \pmod{p_2^{\alpha_2}} \\ &\vdots \quad\quad \vdots \\ f(x) &\equiv f(x_{i_k k}) \equiv 0 \pmod{p_k^{\alpha_k}}. \end{aligned}$$

Nuevamente, el Teorema 1.3 nos da $f(x) \equiv 0 \pmod{m}$. Escojamos soluciones $(x_1, \ldots, x_k), (x'_1, \ldots, x'_k) \in T_1 \times \cdots \times T_k$ con $x_i \not\equiv x'_i \pmod{p_i^{\alpha_i}}$, para alguna i.

Supongamos que y es solución del sistema

$$\begin{aligned} x &\equiv x_1 \pmod{p_1^{\alpha_1}} \\ x &\equiv x_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \quad\quad \vdots \\ x &\equiv x_k \pmod{p_k^{\alpha_k}}, \end{aligned}$$

y que y' resuelve el sistema

$$\begin{aligned} x &\equiv x_1' \pmod{p_1^{\alpha_1}} \\ x &\equiv x_2' \pmod{p_2^{\alpha_2}} \\ &\vdots \qquad\qquad \vdots \\ x &\equiv x_k' \pmod{p_k^{\alpha_k}}. \end{aligned}$$

Si $y \equiv y' \pmod{m}$, entonces necesariamente $y \equiv y' \pmod{p_i^{\alpha_i}}$. Por tanto, en la i-ésima congruencia tendríamos que $x_i \equiv x_i' \pmod{p_i^{\alpha_i}}$. Así que $y \not\equiv y' \pmod{m}$ y de esta manera hemos probado que $f(x) \equiv 0 \pmod{m}$ tiene al menos $t_1 t_2 \cdots t_k$ soluciones incongruentes módulo m.

Para ver que son exactamente todas, debemos escoger cualquier solución z de $f(x) \equiv 0 \pmod{m}$ y ver que z proviene de algún elemento de $T_1 \times T_2 \times \cdots \times T_k$. En efecto, $z = p_i^{\alpha_i} q_i + r_i$ con $0 \leq r_i < p_i^{\alpha_i}$ para $1 \leq i \leq k$. Así que

$$z \equiv r_i \pmod{p_i^{\alpha_i}} \quad \text{y} \quad f(z) \equiv f(r_i) \equiv 0 \pmod{p_i^{\alpha_i}}.$$

De lo anterior se sigue que r_i es algún x_{ji} y z es solución del sistema

$$\begin{aligned} x &\equiv r_1 \pmod{p_1^{\alpha_1}} \\ x &\equiv r_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \quad \vdots \\ x &\equiv r_k \pmod{p_k^{\alpha_k}}. \end{aligned}$$

y por tanto hay exactamente $t_1 t_2 \cdots t_k$ soluciones incongruentes módulo m de $f(x) \equiv 0 \pmod{m}$.

□

Si $a, b \in \mathbb{Z},\ n \in \mathbb{N}$, entonces por la fórmula del binomio de Newton tenemos

$$(a+b)^n = a^n + na^{n-1}b + b^2 Q(a,b),$$

donde $Q(a,b)$ es una expresión que depende de a, b. Si $f(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n$, entonces la derivada formal de $f(x)$ es por definición

$$f'(x) = c_1 + 2c_2 x + \cdots + nc_n x^{n-1}.$$

Con un cálculo elemental puede verificarse fácilmente que

$$f(a+b) = f(a) + bf'(a) + b^2 Q(a,b),$$

donde $Q(a,b)$ es una expresión que depende de a, b.

En seguida probaremos que las soluciones de una congruencia módulo p^s se pueden encontrar por medio de las soluciones de una congruencia módulo p^{s-1}. Aplicando este argumento las veces que sea necesario, se puede ver que para resolver una congruencia módulo p^s, es necesario resolver primero una congruencia módulo p.

Teorema 4.2. *Sea z alguna solucion de $f(x) \equiv 0 \pmod{p^s}$. Entonces z depende de alguna solución de la congruencia $f(x) \equiv 0 \pmod{p^{s-1}}$, con $s > 1$.*

Demostración: Si z solución de $f(x) \equiv 0 \pmod{p^s}$, entonces z es solución de $f(x) \equiv 0 \pmod{p^{s-1}}$ y por lo tanto el conjunto A de soluciones de la congruencia $f(x) \equiv 0 \pmod{p^{s-1}}$ no es vacío. Por lo anterior, existe $X \in A$ tal que $z \equiv X \pmod{p^{s-1}}$. Así

$$z = X + tp^{s-1} \tag{1}$$

para alguna $t \in \mathbb{Z}$. Debemos encontrar las condiciones para las cuales t existe. De (1) tenemos

$$f(z) = f(X + tp^{s-1}) = f(X) + tp^{s-1}f'(X) + t^2(p^{s-1})^2Q,$$

y puesto que $s > 1$ se tiene

$$(p^{s-1})^2 \equiv 0 \pmod{p^s}.$$

Por lo tanto, lo que deseamos es que

$$f(z) \equiv f(X) + tp^{s-1}f'(X) \equiv 0 \pmod{p^s} \tag{2}$$

Puesto que $f(X) \equiv 0 \pmod{p^{s-1}}$, tenemos $f(X) = Mp^{s-1}$, para algún $M \in \mathbb{Z}$. En resumidas cuentas (2) toma la forma

$$f(z) \equiv f(X) + tp^{s-1}f'(X) \equiv Mp^{s-1} + tp^{s-1}f'(X) \equiv 0 \pmod{p^s},$$

de donde

$$p^{s-1}(M + tf'(X)) \equiv 0 \pmod{p^s},$$

lo cual es equivalente a

$$M + tf'(X) \equiv 0 \pmod{p} \tag{3}$$

Puesto que $M = \dfrac{f(X)}{p^{s-1}}$, entonces podemos escribir (3) como

$$tf'(X) \equiv -M \equiv -\frac{f(X)}{p^{s-1}} \pmod{p} \tag{4}$$

Concluimos nuestro resultado estudiando tres casos de esta última congruencia.

Caso 1 Si $f'(X) \not\equiv 0 \pmod{p}$, entonces $\text{mcd}(p, f'(X)) = 1$ y de ésta forma $tf'(X) \equiv -M \pmod{p}$ tiene solución única módulo p en la variable t. En este caso no es trascendente que M sea congruente con 0 módulo p.

Caso 2 Si $f'(X) \equiv 0 \pmod{p}$ y $M \not\equiv 0 \pmod{p}$, entonces para toda $t \in \mathbb{Z}$ tenemos $tf'(X) \equiv 0 \pmod{p}$. Es claro que en esta situación ningún valor de t puede ser solución de la congruencia $tf'(X) \equiv -M \pmod{p}$. Por lo tanto este caso no tiene solución.

Caso 3 Si $f'(X) \equiv 0 \pmod{p}$ y $M \equiv 0 \pmod{p}$, entonces para todo valor de $t \in \mathbb{Z}$ se tiene $tf'(X) \equiv 0 \pmod{p}$, así que para toda $t \in \mathbb{Z}$ se cumple

$$tf'(X) \equiv -M \pmod{p}.$$

En este caso existen p soluciones incongruentes.

□

Como consecuencia del teorema anterior tenemos que si $f(x) \equiv 0 \pmod{p^s}$ tiene al menos una solución, entonces ésta depende de alguna solución de $f(x) \equiv 0 \pmod{p}$. Usaremos la congruencia (4) y (1) del teorema anterior para dar un ejemplo.

Ejemplo 4.3. *Considera la congruencia* $x^3 + x + 2 \equiv 0 \pmod{5^2}$. *Observemos que* $X = 4$ *es una solución de* $x^3 + x + 2 \equiv 0 \pmod{5}$ *y* $f'(4) = 49$. *Por lo tanto, la congruencia que debemos resolver es*

$$49t \equiv -\frac{f(4)}{5} \equiv -14 \pmod{5}.$$

Esta es equivalente a $4t \equiv 1 \pmod{5}$. *La solución está dada por* $t = 4$ *y de este modo, usando (1) del teorema anterior tenemos que* $z = 4 + 4 \cdot 5 = 24$ *es una solución de* $x^3 + x + 2 \equiv 0 \pmod{5^2}$.

5 La congruencia $f(x) \equiv 0 \pmod{p}$

Si $\mathbb{F}$ es un campo, definimos el *anillo de polinomios* con coeficientes en $\mathbb{F}$ como

$$\mathbb{F}[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in \mathbb{F},\ n \in \mathbb{N}_0\}.$$

Si $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{F}[x]$, decimos que $f(x)$ es de grado n si $a_n \neq 0$. Escribimos $gr(f(x)) = n$ para indicar que $f(x)$ es un polinomio de grado n. Un polinomio de grado 0 es un polinomio constante $\neq 0$. Los

polinomios los podemos sumar y multiplicar. Si $f(x) = a_0 + a_1x + \ldots + a_nx^n$ y $g(x) = b_0 + b_1x + \ldots + b_mx^m$, entonces

$$f(x) + g(x) = c_0 + c_1x + \ldots c_sx^s, \quad \text{donde} \quad c_k = a_k + b_k,$$

y

$$f(x)g(x) = c_0 + c_1x + \ldots c_{n+m}x^{n+m},$$

donde $c_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0$. Esta suma y producto de polinomios son asociativos, conmutativos, tienen su neutro respectivamente y además satisfacen la ley distributiva.

Al polinomio constante 0 le asignamos grado $-\infty$, simplemente para que el grado de un producto sea consistente y satisfaga que el grado de un producto es la suma de los grados. Así, se puede mostrar fácilmente que:

1. $gr(f(x) + g(x)) \leq \max\{gr(f(x)), gr(g(x))\}$,
2. $gr(f(x)g(x)) = gr(f(x)) + gr(g(x))$.

Toda la teoría de divisibilidad que desarrollamos en $\mathbb{Z}$ es válida en el anillo $\mathbb{F}[x]$. En particular tenemos el algoritmo de la división.

Teorema 5.1. [Algoritmo de la división] *Si* $f(x),\ g(x) \in \mathbb{F}[x]$ *con* $g(x) \neq 0$, *entonces existen únicos* $q(x),\ r(x) \in \mathbb{F}[x]$ *tales que*

$$f(x) = g(x)q(x) + r(x), \ \ con \ \ r(x) = 0 \ \ ó \ \ gr(r(x)) < gr(g(x)).$$

Demostración: La prueba acerca de la existencia de la expresión la haremos por inducción sobre el grado de $f(x)$. Observemos que si $gr(f(x)) < gr(g(x))$, entonces $q(x) = 0$ y $r(x) = f(x)$ nos da lo que buscamos. Si $gr(f(x)) = gr(g(x)) = 0$, entonces $f(x),\ g(x) \in \mathbb{F} \setminus \{0\}$. En este caso $q(x) = f(x)g(x)^{-1}$ y $r(x) = 0$.

Sea $gr(f(x)) = n$, $gr(g(x)) = m$. Por lo anterior, podemos suponer que $1 \leq m \leq n$. Nuestra hipótesis de inducción consiste en suponer que el teorema es cierto para $g(x)$ y cualquier polinomio de grado $< n$. Escribimos

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \quad \text{y} \ \ g(x) = b_0 + b_1x + \ldots + b_mx^m.$$

Observemos que $a_n \neq 0$ y $b_m \neq 0$. El polinomio $f_1(x) = f(x) - a_nb_m^{-1}x^{n-m}g(x)$ es un elemento de $\mathbb{F}[x]$ y el coeficiente de x^n es $a_n - (a_nb_m^{-1})b_m = 0$. Por lo tanto $gr(f_1(x)) < n$. Aplicamos la hipótesis de inducción a $f_1(x)$ y $g(x)$ para obtener

$$f_1(x) = g(x)q_1(x) + r(x),$$

donde $r(x) = 0$ ó $gr(r(x)) < gr(g(x))$. De la igualdad

$$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x) = g(x)q_1(x) + r(x),$$

se sigue que $f(x) = g(x)(a_n b_m^{-1} x^{n-m} + q_1(x)) + r(x)$. Si escribimos

$$q(x) = a_n b_m^{-1} x^{n-m} + q_1(x),$$

entonces $f(x) = g(x)q(x) + r(x)$ y así obtenemos la expresión deseada.

Dejamos como ejercicio mostrar que si los coeficientes están en un campo, entonces el grado de un producto es la suma de los grados. Usaremos esto para demostrar la unicidad de la expresión. Supongamos que

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x),$$

con $gr(r(x)) < gr(g(x))$ y $gr(r_1(x)) < gr(g(x))$. De la igualdad

$$r(x) - r_1(x) = (q_1(x) - q(x))g(x),$$

se sigue que

$$gr(r(x) - r_1(x)) = gr((q_1(x) - q(x))g(x)).$$

Hasta aquí no hay nada sorprendente. Si $q_1(x) - q(x) \neq 0$, tenemos $(q_1(x) - q(x))g(x) \neq 0$ y por lo tanto

$$gr((q_1(x) - q(x))g(x)) = gr(q_1(x) - q(x)) + gr(g(x)) \geq$$
$$gr(g(x)) > gr(r(x) - r_1(x)),$$

lo cual es imposible. Así que necesariamente $q_1(x) - q(x) = 0$ y $r(x) = r_1(x)$. □

Definición 5.2. *En el Teorema anterior, si $r(x)$ es el polinomio idénticamente 0, entonces diremos que $g(x)$ divide a $f(x)$. Escribiremos $g(x) \mid f(x)$ para indicar que $g(x)$ divide a $f(x)$.*

Un caso particularmente importante de campo es $\mathbb{F}_p$. Así que podemos considerar polinomios con coeficientes en $\mathbb{F}_p[x]$. Si $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{F}_p[x]$ y $p \nmid a_n$, entonces el grado de $f(x)$ es n. Vamos a escribir $gr_p(f(x))$ para indicar el grado de $f(x)$. Un polinomio es mónico si $gr_p(f(x)) = n$ y $a_n \equiv 1 \pmod{p}$. Por ejemplo, $f(x) = -1 + 3x^2 - 4x^3$ es un polinomio mónico en $\mathbb{F}_5[x]$.

Definición 5.3. *Sea $f(x) \in \mathbb{F}_p[x]$. Una solución o raíz de $f(x)$ en $\mathbb{F}_p$ es un elemento $\alpha \in \mathbb{F}_p$ tal que $f(\alpha) \equiv 0 \pmod{p}$.*

Teorema 5.4. [Teorema del Factor] *Sea $f(x) \in \mathbb{F}_p[x]$ no constante. Entonces $a \in \mathbb{F}_p$ es raíz de $f(x)$ si y sólo si $x - a \mid f(x)$.*

Demostración: Es conscuencia directa de las definiciones.

□

El Teorema del factor es válido para polinomios con coeficientes en cualquier campo, además si el polinomio no tiene raíces en $\mathbb{F}$, esto no significa que el polinomio en cuestión no se pueda factorizar en algún *lugar*.

Teorema 5.5. [Teorema del Residuo] *Si p es primo y $f(x) \in \mathbb{F}_p[x]$ no es el polinomio cero, entonces existe $r(x) \in \mathbb{F}_p[x]$ mónico tal que:*

1. *$gr_p(r(x)) \leq p - 1$*
2. *$f(x)$ y $r(x)$ tienen exactamente las mismas soluciones en $\mathbb{F}_p$.*

Demostración: Por el algoritmo de la división podemos escribir

$$f(x) = (x^p - x)q(x) + R(x)$$

donde $gr_p(R(x)) \leq p - 1$ ó $R(x)$ es el polinomio idénticamente cero. Por el Pequeño Teorema de Fermat 1.19 tenemos $x^p - x \equiv 0 \pmod{p}$ para todo $x \in \mathbb{Z}$. Esto demuestra que para toda $x \in \mathbb{F}_p$ se tiene $f(x) \equiv R(x) \pmod{p}$ y por lo tanto $f(x)$ y $R(x)$ tienen exactamente las mismas soluciones.

Supongamos que $R(x) = b_0 + b_1x + \ldots + b_sx^s$ y $p \nmid b_s$. Según el Corolario 2.3, existe un único $b \in \mathbb{Z}$ tal que $bb_s \equiv 1 \pmod{p}$. Es claro que $R(x)$ y $bR(x)$ tienen las mismas soluciones. El polinomio $r(x) = bR(x)$ satisface el teorema.

□

Sea $f(x) = x^2 - 1 \in \mathbb{Z}_8[x]$. Entonces el grado de $f(x)$ es 2 y con un cálculo elemental se puede verificar que $1, 3, 5, 7$ son las raíces de $f(x)$ en $\mathbb{Z}_8$. El siguiente resultado muestra que cuando el módulo es un número primo p, entonces el número de raíces de $f(x) \in \mathbb{F}_p[x]$ no excede al grado del polinomio ni a p.

Teorema 5.6. [Lagrange] *Sea $f(x) \in \mathbb{F}_p[x]$. Si $n = gr_p(f(x))$, entonces el número de soluciones en $\mathbb{F}_p$ de $f(x)$ no es mayor que n.*

Demostración: La prueba es por inducción sobre el grado de la congruencia. Si $n = 1$, entonces $f(x) = a_0 + a_1x$ y $p \nmid a_1$. El Corolario 2.3 nos asegura que $f(x)$ tiene solución única.

Supongamos que el teorema es válido para todos los polinomios en $\mathbb{F}_p[x]$ de grado menor que n. Sea $f(x) \in \mathbb{F}_p[x]$ de grado n. Si $f(x)$ no tiene raíces en

$\mathbb{F}_p$, el teorema es cierto; así que podemos suponer que $f(x)$ tiene al menos una solución en $\mathbb{F}_p$ a la cual llamaremos a. Por el Teorema del Factor,

$$f(x) = (x - a)q(x),$$

con $gr_p(q(x)) = n - 1$. Por la hipótesis de inducción, $q(x)$ tiene a lo más $n - 1$ raíces en $\mathbb{F}_p$ y cualquiera de éstas es solución de $f(x)$, por tanto $f(x)$ tiene a lo más n raíces en $\mathbb{F}_p$.

□

Notamos que en el curso de la demostración del teorema anterior no intervino la forma de los elementos del campo $\mathbb{F}_p$, es decir, el resultado es válido si reemplazamos $\mathbb{F}_p$ por cualquier campo $\mathbb{F}$.

Por simple inspección, el polinomio $f(x) = x^5 - x + 1 \in \mathbb{F}_5[x]$ no tiene soluciones en $\mathbb{F}_5$. Esto no contradice de ninguna manera el Teorema de Lagrange. La existencia de soluciones de un polinomio con coeficientes en $\mathbb{F}_p$ depende esencialmente de la naturaleza del polinomio. Se puede mostrar que existe un campo $\mathbb{F}$ que contiene a $\mathbb{F}_p$ en donde $f(x)$ tiene al menos una solución. Este resultado corresponde a la Teoría de Galois y esperamos que nuestro ejemplo sirva como una invitación a incursionar en esta teoría.

Corolario 5.7. *Sea $f(x) \in \mathbb{F}_p[x]$. Si $f(x)$ tiene más de $gr_p(f(x))$ soluciones, entonces cualquier clase $a \in \mathbb{F}_p$ satisface $f(a) \equiv 0 \pmod{p}$.*

□

Para finalizar, presentamos uno de los resultados más completos (pero poco práctico), el cual es una prueba para decidir si un entero es primo.

Teorema 5.8. [Teorema de Wilson] *n es primo si y sólo si*

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

Demostración: Si $n = p$ es primo, entonces

$$f(x) = x^{p-1} - 1 \equiv 0 \pmod{p},$$

tiene $p - 1$ soluciones $x = 1, 2, \ldots, p - 1$. Consideremos la congruencia

$$h(x) = (x - 1)(x - 2) \cdots (x - (p - 1)) \equiv 0 \pmod{p}.$$

Esta congruencia polinomial también tiene $p-1$ soluciones $x = 1, 2, \ldots, p-1$. Observemos que

$$g(x) = f(x) - h(x) \equiv 0 \pmod{p},$$

es una congruencia de grado a lo más $p-2$ y tiene $p-1$ soluciones incongruentes. Por lo tanto 0 también es solución de $g(x) \equiv 0 \pmod{p}$ y así

$$0 \equiv g(0) \equiv -1 - (-1)^{p-1}(p-1)! \pmod{p}.$$

Si p es impar, entonces $(-1)^{p-1} = 1$ y por lo tanto $(p-1)! \equiv -1 \pmod{p}$. El caso $p = 2$ es evidente.

Por último, supongamos que $(n-1)! \equiv -1 \pmod{n}$ y n compuesto. Por ser n compuesto, admite un divisor d con $1 < d < n$. Por lo tanto $d \mid (n-1)!$ y $(n-1)! \equiv 0 \pmod{d}$. Esto último es imposible por el Teorema 1.1 parte 4.

□

Corolario 5.9. *Sea p un número primo. La congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución si y sólo si $p = 2$ ó $p \equiv 1 \pmod{4}$.*

Demostración: Supongamos que $p \equiv 3 \pmod{4}$. Para cualquier $x \in \mathbb{Z}$ tal que $\text{mcd}(x, p) = 1$ tenemos $x^{p-1} \equiv 1 \pmod{p}$ y $\dfrac{p-1}{2}$ es impar. Por lo tanto

$$x^{p-1} \equiv (x^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Lo anterior significa $x^2 \not\equiv -1 \pmod{p}$ para cualquier x tal que $\text{mcd}(x, p) = 1$.

Inversamente, si $p = 2$, entonces claramente $1^2 \equiv -1 \pmod{2}$. Si $p = 4n+1$, entonces el conjunto

$$A = \{1, 2, \ldots, j, \ldots, \frac{p-1}{2}, \frac{p+1}{2}, \ldots, p-j, \ldots, p-2, p-1\},$$

tiene exactamente $4n$ elementos. Si $j \in A$ es tal que $1 \leq j \leq \dfrac{p-1}{2}$, entonces $\dfrac{p+1}{2} \leq p - j \leq p - 1$. En general tenemos $p - j \equiv -j \pmod{p}$. Así por el Teorema de Wilson

$$(p-1)! \equiv \prod_{j=1}^{p-1}(p-j) \equiv \prod_{j=1}^{\frac{p-1}{2}} j \prod_{j=1}^{\frac{p-1}{2}}(p-j) \equiv \prod_{j=1}^{\frac{p-1}{2}} j \prod_{j=1}^{\frac{p-1}{2}}(-j) \equiv \prod_{j=1}^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} j^2 \equiv$$

$$\prod_{j=1}^{\frac{p-1}{2}}(-1)^{2n} j^2 \equiv \Big(\prod_{j=1}^{\frac{p-1}{2}} j\Big)^2 \equiv \Big(\frac{p-1}{2}\Big)! \equiv -1 \pmod{p}.$$

□

Notemos que la parte final de la demostración del corolario anterior nos da explícitamente una solución de $x^2 + 1 \equiv 0 \pmod{p}$, concretamente $\Big(\dfrac{p-1}{2}\Big)!$. Obviamente si a es solución, entonces $p - a$ es la otra solución. Pensemos en el primo $p = 353$. Calcular $\Big(\dfrac{353-1}{2}\Big)!$ puede ser poco manejable hasta para una

computadora. ¿Puede el lector dar una alternativa para no recurrir a calcular el número $\left(\frac{p-1}{2}\right)!$

Corolario 5.10. *Si p es un número primo de la forma $4n+3$ y si $a, b \in \mathbb{Z}$ satisfacen $a^2 + b^2 \equiv 0 \pmod{p}$, entonces $a \equiv b \equiv 0 \pmod{p}$.*

Demostración: Si $p \nmid a$, entonces existe $c \in \mathbb{Z}$ tal que $ac \equiv 1 \pmod{p}$. Así que

$$(bc)^2 \equiv b^2c^2 \equiv -a^2c^2 \equiv -1 \pmod{p}.$$

Lo anterior significa que la congruencia $x^2 \equiv -1 \pmod{p}$ es soluble, en contradicción con el corolario anterior. Por lo tanto $a \equiv 0 \pmod{p}$. De la ecuación $a^2 + b^2 \equiv 0 \pmod{p}$ se sigue que $p \mid b^2$ y así $p \mid b$.

□

El Corolario anterior nos servirá para demostrar que ciertos primos racionales siguen teniendo la misma cualidad cuando son vistos en una estructura algebraica más grande. Observemos que: $1^2+2^2 \equiv 0 \pmod{5}$ y $1 \not\equiv 0 \pmod{5}$, $2 \not\equiv 0 \pmod{5}$. De hecho, cualquier primo racional p de la forma $4n+1$ se puede escribir como $a^2 + b^2$ y $a \not\equiv 0 \pmod{p}$, $b \not\equiv 0 \pmod{p}$. En el teorema **??** del Capítulo 5 daremos una prueba elemental de este hecho.

PROBLEMAS

1. Sea $\mathbb{F}$ un campo y $f(x), g(x) \in \mathbb{F}[x]$.
   b) Mostrar que $gr(f(x) + g(x)) \leq gr(f(x)) + gr(g(x))$.
   c) Mostrar que $gr(f(x)g(x)) = gr(f(x)) + gr(g(x))$.
2. Mostrar que la ecuación $x^2 - 10y^2 = \pm 3$ no tiene soluciones enteras x, y.
3. Supongamos que la congruencia $f(x) \equiv 0 \pmod{m}$ tiene m soluciones incongruentes. Si $a \in \mathbb{Z}_m$, entonces $f(a) \equiv 0 \pmod{m}$.
4. Demostrar el Corolario 5.7.
5. Encontrar $R(x)$ en el Teorema del Residuo 5.5 para cada uno de los siguientes casos:
   a) $f(x) = 3x^5 + x^4 + 2x^3 + 5x + 6$ en $\mathbb{F}_5[x]$.
   b) $f(x) = -2x^4 - 3x + 2$ en $\mathbb{F}_7[x]$.
   c) $f(x) = x^4 - 5x^3 + x^2 - 3x + 2$ en $\mathbb{F}_{11}[x]$.
   d) $f(x) = x^4 + 1$ en $\mathbb{F}_{13}[x]$.

6. El polinomio $f(x) \in \mathbb{F}_p[x]$ es irreducible si $f(x) = h(x)g(x)$ con $h(x), g(x) \in \mathbb{F}_p[x]$, entonces alguno de los factores es un polinomio constante no cero. Considerar la siguiente lista de polinomios:

   a) $x^2 - 13$.
   b) $x^2 - 5x + 6$.
   c) $x^2 + 2x - 2$.
   d) $x^3 + x + 2$.
   e) $x^3 - 2$.
   f) $x^3 + 2x^2 - 3x - 1$.

   ¿Cuáles de ellos son irreducibles cuando son considerados en

   $$\mathbb{F}_2[x], \quad \mathbb{F}_5[x], \quad \mathbb{F}_7[x], \quad \mathbb{F}_{11}[x]?$$

7. Si un polinomio no es irreducible, entonces diremos que es reducible. Lo anterior significa que si $f(x) = h(x)g(x)$, entonces $h(x)$ y $g(x)$ tienen grado positivo. Con los polinomios del problema anterior averiguar cuáles de ellos son reducibles en $\mathbb{F}_2[x], \mathbb{F}_5[x], \mathbb{F}_7[x], \mathbb{F}_{11}[x]$.

8. Sea $\mathbb{F}$ un campo y $f(x) \in \mathbb{F}[x]$ de grado 1. Demostrar que $f(x)$ tiene una única raíz en $\mathbb{F}$.

9. Sea $\mathbb{F}$ un campo y $f(x) \in \mathbb{F}[x]$ de grado 2. Demostrar que si $f(x)$ no tiene raíces en $\mathbb{F}$, entonces $f(x)$ es irreducible.

10. Acomodar los enteros $1, 2, 3, \ldots, 28$ en pares a, b de tal forma que $ab \equiv 1 \pmod{29}$.

11. Usar el Corolario 5.9 para encontrar explícitamente una solución de $x^2 \equiv -1 \pmod{p}$ con $p = 41, 149$.

12. Sea $n > 1$. Mostrar que n es primo si y sólo si $(n-2)! \equiv 1 \pmod{n}$.

13. Considerar la función $f(n) = \operatorname{sen}\left(\pi \dfrac{(n-1)! + 1}{n}\right)$. Mostrar que n es primo si y sólo si $f(n) = 0$. Evaluar $f(29)$.

14. Mostrar que $18! \equiv -1 \pmod{437}$.

15. Sea $f(x)$ cualquiera de los siguientes polinomios:

   a) $x^3 - x + 3$.
   b) $x^3 + x^2 - 4$.
   c) $x^2 + x + 7$.
   d) $x^4 + x + 1$.

   Resolver la congruencia $f(x) \equiv 0 \pmod{m}$ para $m = 3,\ 9,\ 27$.

16. En el Teorema 4.2, resultó que en el Caso 2 si $f'(X) \equiv 0 \pmod{p}$ y $M \not\equiv 0 \pmod{p}$, entonces para toda $t \in \mathbb{Z}$ tenemos

$$tf'(X) \equiv 0 \pmod{p},$$

y por lo tanto, en esta situación ningún valor de t puede ser solución de la congruencia $tf'(X) \equiv -M \pmod{p}$. Así que no podemos construir una solución de $f(x) \equiv 0 \pmod{p^s}$. En este caso ¿qué sugiere usted?

17. ¿Puede ser que $f(x) \equiv 0 \pmod{p^s}$ tenga solución y $f(x) \equiv 0 \pmod{p^j}$ no sea soluble para algún $j < s$?

18. ¿Cuántas soluciones tiene cada uno de los siguientes polinomios?

    a) $f(x) = x^3 + x + 6$ en $\mathbb{Z}_{2^4.3^3}$.

    b) $f(x) = x^3 - x + 1$ en $\mathbb{Z}_{3^5.13^2}$.

    c) $f(x) = x^3 - x + 1$ en $\mathbb{Z}_{5^3.7}$.

    d) $f(x) = x^3 + 5x - 3$ en $\mathbb{Z}_{3^{10}.5^5}$.

19. Resolver $x^3 + 64x^2 + x + 30 \equiv 0 \pmod{216}$.

Bibliografía

[1] Dickson L. E., *History of the theory of numbers*, Vol. 1, Chelsea 1971.

[2] Hardy G.H., Wright E.M. *An introduction to the theory of numbers*. Oxford University Press 1979.

[3] Mathews G.B., *Theory of Numbers*, Cambridge, 1892.

[4] Nagell T. *Number theory*. Chelsea 1964.

[5] Morales Guerrero L.E., Rzedowski Calderón M., *Contando sobre números*. Avance y Perspectiva CINVESTAV-IPN vol. **18** (1999).

[6] Stark M.H., *An introduction to number theory*. MIT Press (1978).

[7] Zaldivar Cruz F., Fundamentos de álgebra, Editado por Fondo de Cultura Económica-Universidad Autónoma Metropolitana 2005.