3. Polinomios.

Sea R un anillo cualquiera. Un polinomio sobre R es una expresión de la forma

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$$

donde n es un entero no negativo, los coeficientes a_i,$0 \leq i \leq n$, son elementos de R, y x es la ideterminda sobre R.

Dos polinomios $f(x) = \sum_{i=o}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{n} b_i x^i$ sobre R son iguales si $a_i = b_i$ para $0 \leq i \leq n$. Definimos la suma de $f(x)$ y $g(x)$ como

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

Si $f(x) = \sum_{i=o}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{m} b_i x^i$ definimos el producto como

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ donde } c_k = \sum_{\substack{i+j=k \\ 0 \leq i \leq n, 0 \leq j \leq m}} a_i b_j$$

Con estas operaciones, los polinomios sobre R es un anillo al cual llamaremos el *anillo de polinomios sobre* R y lo notaremos por $R[x]$.

El cero en $R[x]$ es el polinomio con todos sus coeficientes nulos y lo representaremos por 0.

Si $f(x) = f_0 + f_1 x + \ldots f_m x^m$ es un polinomio sobre R y $f_m \neq 0$, entonces m es llamado el grado de $f(x)$, y a f_m se le llama el *líder* del polinomio. Si $f_m = 1$, entonces decimos que el polinomio es *mónico*.

Teorema 3.25 *Sea $f, g \in R[x]$. Entonces*

$$gr(f+g) \leq max(gr(f), gr(g))$$

$$gr(fg) \leq gr(f) + gr(g)$$

Si R es un dominio de integridad, entonces

$$gr(fg) = gr(f) + gr(g)$$

Teorema 3.26 *1. $R[x]$ es un anillo conmutativo si y sólo si lo es R.*

2. $R[x]$ es un anillo con identidad si y sólo si R posee identidad.

3. $R[x]$ es un dominio de integridad si y sólo si R es un dominio de integridad.

Sea $\mathbf{F}$ un cuerpo. Un polinomio $b(x)$ es divisible por $d(x)$ y $d(x)$ es un factor de $b(x)$ si existe un $q(x)$ tal que $b(x) = q(x)d(x)$. Si $d(x)$ es un factor de $b(x)$, entonces $cd(x)$ también es un factor para $c \neq 0 \in \mathbf{F}$. Las unidades de $\mathbf{F[x]}$ son los divisores del polinomio 1 que son todos los elementos no nulos de F.

Teorema 3.27 *Sea $g \neq 0$ un polinomio en $\mathbf{F[x]}$. Entonces para todo $f \in \mathbf{F[x]}$ existen dos polinomios $q, r \in \mathbf{F[x]}$ tal que*

$$f = qg + r, \text{ donde } gr(r) < gr(g)$$

El hecho de que $\mathbf{F[x]}$ permita un algoritmo de división, implica que todo ideal de $\mathbf{F[x]}$ es principal.

Teorema 3.28 $\mathbf{F[x]}$ *es un dominio de ideales principales y cualquier ideal $J \in \mathbf{F[x]}$ es generado por un único polinomio mónico de menor grado de J.*

Teorema 3.29 *Sean $f_1, f_2, \ldots, f_n \in \mathbf{F}[\mathbf{x}]$ con alguno de ellos no nulos. Entonces existe un único polinomio mónico $d \in \mathbf{F}[\mathbf{x}]$ con las siguientes propiedades:*

1. *d divide a cada $f_j, 1 \leq j \leq n$.*
2. *Cualquier polinomio $c \in \mathbf{F}[\mathbf{x}]$ que divida a $f_j, 1 \leq j \leq n$, divide a d. Es más, d se puede expresar como*

$$d = b_1 f_1 + \cdots + b_n f_n$$

con $b_1, \ldots, b_n \in \mathbf{F}[\mathbf{x}]$.

Sean $f, g \in \mathbf{F}[\mathbf{x}]$, el máximo común divisor se puede obtener gracias al algoritmo de Euclides de la siguiente forma:

$$\begin{array}{cc}
f = q_1 g + r_1 & 0 \leq gr(r_1) < gr(g) \\
g = q_2 r_1 + r_2 & 0 \leq gr(r_2) < gr(r_1) \\
r_1 = q_3 r_2 + r_3 & 0 \leq gr(r_3) < gr(r_2) \\
\vdots & \\
r_{s-2} = q_2 r_{s-1} + r_2 & 0 \leq gr(r_s) < gr(r_{s-1}) \\
r_{s-1} = q_{s+1} r_s &
\end{array}$$

donde $q_1, \ldots, q_{s+1}, r_1, \ldots, r_s \in \mathbf{F}[\mathbf{x}]$. El máximo común divisor viene dado por

$$mcd(f, g) = b^{-1} r_s$$

donde b es el coeficiente líder de r_s

Teorema 3.30 *Sean $f_1, f_2, \ldots, f_n \in \mathbf{F}[\mathbf{x}]$ con alguno de ellos no nulos. Entonces existe un único polinomio mónico $m \in \mathbf{F}[\mathbf{x}]$ con las siguientes propiedades:*

1. *m es múltiplo de cada $f_j, 1 \leq j \leq n$.*
2. *Cualquier polinomio $b \in \mathbf{F}[\mathbf{x}]$ múltiplo $f_j, 1 \leq j \leq n$, es un múltiplo de m.*

Además,

$$a^{-1} fg = mcm(f, g) mcd(f, g)$$

donde a es el coeficiente líder de fg.

Algoritmo de Euclides Extendido

Entrada: $p_1(x), p_2(x) \in J[x]$, $p_2(x) \neq 0$, $m = gr(p_1(x)) \geq gr(p_2(x)) = n$; J un cuerpo.

Salida: $p_h(x), f(x), g(x) \in J[x]$ tal que $gr(f(x)) < gr(p_1(x) - gr(p_h(x))$,$gr(g(x)) < gr(p_2(x) - gr(p_h(x))$ y $p_h(x) = p_1(x)g(x) + p_2(x)f(x)$

1. [Inicio] $[p_0(x), p_1(x)] := [p_1(x), p_2(x)]$;$[g_0(x), g_1(x)] := [1, 0]$;
2. [Ciclo] While $p_1(x) \neq 0$ do
   $q(x) :=$ Cociente$(p_0(x), p_1(x))$;
   $[p_0(x), p_1(x)] := [p_1(x), p_0(x) - p_1(x)q(x)]$
   $[g_0(x), g_1(x)] := [g_1(x), g_0(x) - g_1(x)q(x)]$
   $[f_0(x), f_1(x)] := [f_1(x), f_0(x) - f_1(x)q(x)]$
3. [Salida] Return $[p_h(x), g(x), f(x)] := [p_0(x), g_0(x), f_0(x)]$

Ejemplo 9:
Sea $p_1(x) = 7x^5 + 4x^3 + 2x + 1$ y $p_2(x) = 5x^3 + 2$ sobre el cuerpo $\mathbb{Z}_{11}$

Iteración	$q(x)$	$p_0(x)$	$p_1(x)$	$g_0(x)$	$g_1(x)$	$f_0(x)$	$f_1(x)$
0	–	$7x^5+4x^3+2x+1$	$5x^3+2$	1	0	0	1
1	$8x^2+3$	$5x^3+2$	$6x^2+2x+6$	0	1	1	$3x^2+8$
2	$10x+4$	$6x^+2x+6$	$9x$	1	$x+7$	$3x^2+8$	$3x^3+10x^2+8x+2$
3	$8x+7$	$9x$	6	$x+7$	$3x^2+8$	$3x^3+10x^2+8x+2$	$9x^4+4x^2+3x+10$
4	$7x$	6	0	$3x^2+8$	–	$9x^4+4x^2+3x+10$	–

Definición 3.31 *Un polinomio $p \in \mathbf{F}[\mathbf{x}]$ es irreducible sobre $\mathbf{F}$ si p tiene grado positivo y si $p = bc$ con $b, c \in \mathbf{F}[\mathbf{x}]$ implica que b o c es una constante.*

Lema 3.32 *Si un polinomio irreducible $p \in \mathbf{F}[\mathbf{x}]$ divide al producto $f_1 \dots f_m$ de polinomios en $\mathbf{F}[\mathbf{x}]$, entonces como mínimo un factor f_j es divisible por p.*

Teorema 3.33 (Factorización Única) *Cualquier polinomio $f \in \mathbf{F}[\mathbf{x}]$ de grado positivo se puede expresar como*

$$f = ap_1^{e_1} \dots p_k^{e_k}$$

con $a \in \mathbf{F}$ y $p_1, \dots, p_k \in \mathbf{F}[\mathbf{x}]$ son polinomios mónicos irreducibles distintos y $e_1, \dots, e_k$ enteros positivos. Además, dicha factorización es única.

Teorema 3.34 *Para todo $f \in \mathbf{F}[\mathbf{x}]$, el anillo cociente $\mathbf{F}[\mathbf{x}]/(\mathbf{f})$ es un cuerpo si y sólo si f es irreducible sobre $\mathbf{F}$.*

Definición 3.35 *Dos polinomios $g(x), h(x)$ en $F_q[x]$, se dicen que son congruentes módulo $f(x)$, y se denota por*

$$g(x) \equiv_{f(x)} h(x)$$

si y sólo si $g(x) - h(x)$ es divisible por $f(x)$.

Ejemplo 10:

1. Sea $f(x) = x \in \mathbf{F_2[x]}$. Entonces $\mathbf{F_2[x]/(x)} = \{\mathbf{[0], [1]}\}$.
2. Sea $f(x) = x^2 + x + 1 \in \mathbf{F_2[x]/(f)}$. Entonces $\mathbf{F_2[x]/(f)} = \{\mathbf{[0], [1], [x], [x+1]}\}$ y la tabla de operaciones viene dado por

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\times$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[x+1]$	$[1]$
$[x+1]$	$[0]$	$[x+1]$	$[1]$	$[x]$

Definición 3.36 *Un elemento $b \in \mathbf{F}$ es una raíz de $f \in \mathbf{F[x]}$ si $f(b) = 0$.*

Teorema 3.37 *Un elemento $b \in \mathbf{F[x]}$ es una raíz de $f \in \mathbf{F[x]}$ si y sólo si $x - b$ divide a $f(x)$.*

Definición 3.38 *Sea $b \in \mathbf{F}$ una raíz de $f \in \mathbf{F[x]}$. Si k es un entero positivo tal que $f(x)$ es divisible por $(x-b)^k$ pero no por $(x-b)^{k+1}$, entonces llamamos a k la multiplicidad de b. Si $k = 1$ entonces decimos que b es de multiplicidad simple.*

Teorema 3.39 *Un elemento $b \in \mathbf{F}$ es una raíz múltiple de $f \in \mathbf{F}$ si y sólo si es raíz de f y f'.*

Teorema 3.40 *El polinomio $f \in \mathbf{F[x]}$ de grado 2 o 3 es irreducible en $\mathbf{F[x]}$ si y sólo si no posee raices en $\mathbf{F[x]}$*

Congruencias módulo un polinomio $p(x) \in \mathbf{F}[\mathbf{x}]$ verifican las mismas propiedades que para enteros. Por ejemplo:

1. Si $f \equiv_m g$, entonces $fk \equiv_m kg$.
2. Si $f_1 \equiv_m g_1$ y $f_2 \equiv_m g_2$, entonces $f_1 + g_1 \equiv_m g_1 + g_2$ y $f_1 g_1 \equiv_m g_1 g_2$
3. Si $f \equiv_m g$ y $g \equiv_m h$ entonces $f \equiv_m h$.

Teorema 3.41 (Resto Chino) *Sea* $\mathbf{F}$ *un cuerpo y* $a_1(x), a_2(x), \ldots, a_n(x), m_1(x), m_2(x), \ldots, m_n(x) \in \mathbf{F}[\mathbf{x}]$, *tal que* $m_i(x)$ *y* $m_j(x)$ *sean coprimos . Entonces existe un* $f(x) \in \mathbf{F}[\mathbf{x}]$ *tal que*

$$\begin{gathered} f(x) \equiv_{m_1(x)} a_1(x) \\ f(x) \equiv_{m_2(x)} a_2(x) \\ \vdots \\ f(x) \equiv_{m_n(x)} a_n(x) \end{gathered}$$

Si $f_(x), f_2(x)$ *son dos soluciones, entonces* $f_1(x) \equiv_{M(x)} f_2(x)$ *con* $M(x) = \prod m_i(x)$

Las fórmulas para el algoritmo del resto chino para $i = 1, \ldots, n$

$$\begin{gathered} M_1(x) = 1 \\ M_i(x) = \prod_{j=1}^{i} m_j(x) \\ U_i(x) M_i(x) \equiv_{m_i(x)} 1 \\ b_1(x) = a_1(x) \\ w_i(x) = (a_i(x) - b_{i-1}(x)) U_i(x) \text{ módulo } m_i(x) \\ b_i(x) = b_{i-1}(x) + w_i(x) M_i(x) \end{gathered}$$

Ejemplo 11:
$f(x) \equiv_{x^2+x} x$ y $f(x) \equiv_{x^2+x+1} 1$ en $\mathbb{Z}_2[x]$ poseen la tabla

a_i	m_i	M_i	U_i	w_i	b_i
x	x^2+x	1	1	$-$	x
1	x^2+x+1	x^2+x	1	$1+x$	x^3

Calculo de polinomios irreducibles en $\mathbb{Z}_p[x]$

Definición 3.42 *Sea $m \in \mathbb{Z}^+$. La función de Mobiuis se define por*

$$\mu(m) = \begin{cases} 1, \textit{ si } m = 1 \\ 0, \textit{ si } m \textit{ es divisible por el cuadrado de un primo} \\ (-1)^k, \textit{ si } m \textit{ es el producto de } k \textit{ primos diferentes} \end{cases}$$

Ejemplo 12:

m	1	2	3	4	5	6	7	8	9	10
	1	−1	−1	0	−1	1	−1	0	0	1

El número de polinomios mónicos irreducibles de grado m en $\mathbb{Z}_p[x]$ para p primo viene dado por

$$N_p(m) = \frac{1}{m} \sum_{d|m} \mu(d) p^{m/d}$$

La probabilidad de que un polinomio aleatorio mónico sea irreducible es aproximandamente $1/m$.

Teorema 3.43 *Sea p un primo y $k \in \mathbb{Z}^+$*

1. *El producto de todos los polinomios mónicos irreducibles en $\mathbb{Z}_p[x]$ de grado un divisor de k es igual a*

$$x^{p^k} - x$$

2. *Sea $f(x)$ un polinomio de grado m en $\mathbb{Z}_p[x]$. Entonces $f(x)$ es irreducible sobre $\mathbb{Z}_p[x]$ si y sólo si*

$$mcd(f(x), x^{p^i} - x) = 1 \ \ \forall i, \ 1 \leq i \leq \lfloor \frac{m}{2} \rfloor$$

Test Irreducibilidad

Entrada: Un primo p y un polinomio mónico de grado $m \in \mathbb{Z}_p[x]$

Salida: Respuesta a , ¿ es $f(x)$ irreducible en $\mathbb{Z}_p[x]$?.

1. $u(x) := x$
2. For $i = 1$ to $\lfloor \frac{m}{2} \rfloor$ do
   2.1 $u(x) := u(x)^p$ mod $f(x)$
   2.2 $d(x) := mcd(f(x), u(x) - x)$
   2.3 if $d(x) \neq 1$ then Return("Reducible")
3. Return("Irreducible")

Generación de un polinomio irreducible mónico de grado m

Entrada: Un primo p y un $m \in \mathbb{Z}^+$

Salida: $f(x)$ mónico irreducible de grado m en $\mathbb{Z}_p[x]$

1. Generar $a_0, a_1, \ldots, a_{m-1}$ de forma aleatoria con $0 \leq a_i \leq p-1$ y $a_0 \neq 0$
2. $f(x) := a_0 + a_1 x + a_2 x^2 + \cdots + a_{m-1} x^{m-1} + x^m$
3. Testear si $f(x)$ es irreducible
   3.1 Si $f(x)$ es irreducible Return($f(x)$)
   3.2 Si $f(x)$ no es irreducible ir a 1.