TEMA 10 APENDICE

SISTEMAS DE NUMERACION

Sea B un numero entero mayor o igual que 2. Entonces todo numero natural n distinto de cero se puede poner de forma unica como $n = a_k B^k + a_{k-1} B^{k-1} + \dots + a_1 B + a_0$ donde $a_i \in \{0, 1, \dots, B-1\}$ para todo $i \in \{0, 1, \dots, k\}$ y $a_k \neq 0$.

A la $(k+1)$-tupla $(a_k, a_1, \dots, a_0)$ la llamaremos la expresion en base B del numero natural n. Por definicion (0) es la expresion en base B del numero cero.

Ejemplo

$(2,2,1)$ es la expresion en base 3 del numero 25 ya que

$$2 \cdot 3^2 + 2 \cdot 3^1 + 1 = 25$$

Ejercicio

¿Que numero tiene la expresion 101010 en base 2?

-D-

$$1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 0 = 32 + 8 + 2 = 42.$$

Metodo para pasar de base 10 a base B

- Expresar en base 7 el numero 1538

$$\begin{array}{l}
1538 \;\underline{|\,7\quad\quad} \\
\;\;13 \quad\; 219 \;\underline{|\,7\quad\quad} \\
\quad\;68 \quad\;\; 09 \quad 31 \;\underline{|\,7\quad} \\
\quad\;\; 5 \qquad\;\; 2 \qquad 3 \quad 4
\end{array}$$

$(4, 3, 2, 5)$ es la expresion buscada.

• Expresar en base 12 el numero 2315

```
2315 |12
 111   192 |12
  035   72  16 |12
   (11)  (0)  (4)  (1)
               <-
```

$(1,4,0,11)$ es la expresion buscada.

Metodo para pasar de base B a base B'

La expresion de un numero en base 3 es 12101. Calcular la expresion de dicho numero en base 5.

El numero es $1\cdot 3^4 + 2\cdot 3^3 + 1\cdot 3^2 + 0\cdot 3 + 1 = 145$

```
145 |5
 45   29 |5
 (0)  (4)  5 |5
          (0) (1)
          <-
```

$(1,0,4,0)$.

Método para pasar de base B a base B^r

• Ejercicio

Calcular la expresion en base 8 del numero que en base 2 tiene la expresion 10010101110110001010101

-D-

Como $8=2^3$ damos cortes de 3 en 3 de derecha a izquierda

$\underbrace{10}_{2}\,\underbrace{010}_{2}\,\underbrace{101}_{5}\,\underbrace{110}_{6}\,\underbrace{110}_{6}\,\underbrace{001}_{1}\,\underbrace{010}_{2}\,\underbrace{101}_{5}$

y cada uno de esos cortes los paso a base 10

Ejercicio

La expresion de un numero en base 9 es 874316. Calcular la expresion de dicho numero en base 3.

-D-

Pasamos cada digito a base 3 (representado con 2 cifras ya que $9 = 3^2$).

$$\begin{array}{cccccc} 8 & 7 & 4 & 3 & 1 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \overline{22} & \overline{21} & \overline{11} & \overline{10} & \overline{01} & \overline{20} \end{array}$$

Suma y producto en base B

Si nos dan dos numeros escritos en base B y nos piden su suma ó su producto, entonces una forma de hacerlo es pasar los numeros a base 10 realizar la operacion en base 10 y pasar el resultado a base B. Pero tambien podemos realizar directamente las operaciones en base B como muestran los siguientes ejemplos.

Ejemplo

Calcular $(4,3,2,4,3)_5 + (3,4,1,3)_5$

-D-

$$\begin{array}{r} 4\,3\,2\,4\,3 \\ +\ 3\,4\,1\,3 \\ \hline 1\,0\,2\,2\,1\,1 \end{array}$$

$(4,3,2,4,3)_5 + (3,4,1,3)_5 = (1,0,2,2,1,1)_5$

Ejemplo

Calcular $(2,3,4,1)_5 \times (3,4)_5$

-D-

$$
\begin{array}{rrrrrr}
 & & 2 & 3 & 4 & 1 \\
 & & & \times & 3 & 4 \\
\hline
 & 2 & 1 & 0 & 1 & 4 \\
1 & 3 & 1 & 2 & 3 & \\
\hline
2 & 0 & 1 & 2 & 4 & 4
\end{array}
$$

$(2,3,4,1)_5 \times (3,4)_5 = (2,0,1,2,4,4)_5$.

EJERCICIO

Encontrar la base (si existe) en que $(3,4,3,2)_B \times (3,4)_B = (1,5,6,6,5,1)_B$

-D-

Nótese que como aparece el dígito 6 entonces $B \geq 7$.

$$(3B^3+4B^2+3B+2)(3B+4) = B^5+5B^4+6B^3+6B^2+5B+1 \Rightarrow$$

$$\Rightarrow 9B^4+24B^3+25B^2+18B+8 = B^5+5B^4+6B^3+6B^2+5B+1 \Rightarrow$$

$$\Rightarrow B^5-4B^4-18B^3-19B^2-13B-7=0.$$

Calculamos sus raíces enteras por el método de Ruffini. Las posibles soluciones son divisores de 7. Pero como $B \geq 7$ únicamente nos interesa si 7 es o no raíz.

$$
\begin{array}{r|rrrrrr}
 & 1 & -4 & -18 & -19 & -13 & -7 \\
7 & & 7 & 21 & 21 & 14 & 7 \\
\hline
 & 1 & 3 & 3 & 2 & 1 & \underline{0}
\end{array}
$$

Por tanto la igualdad es cierta en base 7.

PROPOSICIÓN

Si $a_1, \dots, a_k, m \in \mathbb{Z}$, entonces:

1) $(a_1 + \dots + a_k) \bmod m = (a_1 \bmod m + \dots + a_k \bmod m) \bmod m$.

2) $(a_1 \cdot \dots \cdot a_k) \bmod m = (a_1 \bmod m \cdot \dots \cdot a_k \bmod m) \bmod m$.

EJERCICIO

Demostrar que un número escrito en base 10 es múltiplo de 3 si y sólo si la suma de sus cifras es múltiplo de 3.

-D-

$(a_n, \dots, a_1, a_0)_{10}$ es múltiplo de 3 $\iff a_n 10^n + \dots + a_1 10 + a_0$ es múltiplo de 3 $\iff (a_n 10^n + \dots + a_1 10 + a_0) \bmod 3 = 0 \iff$

$(a_n 10^n \bmod 3 + \dots + a_1 10 \bmod 3 + a_0 \bmod 3) \bmod 3 = 0 \iff$

$\iff \left((a_n \bmod 3 \cdot 10 \bmod 3 \cdot \overset{(n}{\dots} \cdot 10 \bmod 3) \bmod 3 + \dots + (a_1 \bmod 3 \cdot 10 \bmod 3) \bmod 3 + a_0 \bmod 3 \right) \bmod 3 = 0 \iff$ (como $10 \bmod 3 = 1$)

$\iff \left((a_n \bmod 3) \bmod 3 + \dots + (a_1 \bmod 3) \bmod 3 + a_0 \bmod 3 \right) \bmod 3 = 0$

$\iff (a_n \bmod 3 + \dots + a_1 \bmod 3 + a_0 \bmod 3) \bmod 3 = 0 \iff$

$\iff (a_n + \dots + a_1 + a_0) \bmod 3 = 0 \iff a_n + \dots + a_1 + a_0$ es múltiplo de 3.

EJERCICIO

Demostrar que un número escrito en base 10 es múltiplo de 5 si y sólo si termina en cero o en cinco.

-D-

$(a_n, \ldots, a_1, a_0)_{10}$ es múltiplo de 5 $\Leftrightarrow$ $a_n 10^n + \ldots + a_1 10 + a_0$ es múltiplo de 5 $\Leftrightarrow$ $(a_n 10^n + \ldots + a_1 10 + a_0) \bmod 5 = 0 \Leftrightarrow (a_n 10^n \bmod 5 + \ldots$

$\ldots + a_1 10 \bmod 5 + a_0 \bmod 5) \bmod 5 = 0 \Leftrightarrow$ (como $a_n 10^n \bmod 5 = 0, \ldots$

$\ldots, a_1 10 \bmod 5 = 0) \Leftrightarrow (a_0 \bmod 5) \bmod 5 = 0 \Leftrightarrow a_0 \bmod 5 = 0$

$\Leftrightarrow$ (como $a_0 \in \{0, \ldots, 9\}$) $\Leftrightarrow a_0 \in \{0, 5\}$.

EJERCICIO

¿Cuándo es un número escrito en base 8 múltiplo de 7?

¿Cuándo es un número escrito en base 8 múltiplo de 4?

EJERCICIO

Calcular todos los números naturales que al expresarlos en base 8 terminan en 12 y al expresarlos en 9 terminan en 25.

-D-

Si $(a_n, \ldots, a_2, 1, 2)_8$ y $(b_k, \ldots, b_2, 2, 5)_9$ son las expresiones en base 8 y 9 del número natural x, entonces

$x = a_n 8^n + \ldots + a_2 8^2 + 8 + 2$ y $x = b_k 9^k + \ldots + b_2 9^2 + 2 \cdot 9 + 5$. Por tanto $x \equiv 10 \pmod{64}$ y $x \equiv 23 \pmod{81}$.

LA FUNCION φ DE EULER

Sea $m \in \mathbb{N} \setminus \{0,1\}$. Entonces definimos $\varphi(m)$ como el numero de elementos del conjunto $\{1, 2, \dots, m-1\}$ que son primos relativos con m.

EJEMPLO

$\varphi(9) = 6$

Notese que si p es un numero primo entonces $\varphi(p) = p-1$.

TEOREMA

1) Si p es un numero primo y $n \in \mathbb{N} \setminus \{0\}$, entonces $\varphi(p^n) = p^n - p^{n-1}$.

2) Si $\{m, n\} \subseteq \mathbb{N} \setminus \{0,1\}$ y $m.c.d\{m,n\} = 1$, entonces $\varphi(m.n) = \varphi(m) \cdot \varphi(n)$

3) Si $m = p_1^{a_1} \cdot \dots \cdot p_r^{a_r}$ es la descomposicion en primos de m, entonces $\varphi(m) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdot \dots \cdot (p_r^{a_r} - p_r^{a_r - 1})$.

EJEMPLO

$$\varphi(48) = \varphi(2^4 \cdot 3) = (2^4 - 2^3) \cdot (3^1 - 3^0) = 8 \cdot 2 = 16.$$

TEOREMA DE EULER-FERMAT

Sea $\{a, m\} \subseteq \mathbb{N} \setminus \{0,1\}$ tq $m.c.d\{a,m\} = 1$. Entonces

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

EJERCICIO

Calcular el resto de dividir 53^{168} entre 48.

-D-

~~Sabemos que 53^{168} mod 48 coincide con~~

$53^{168} \bmod 48 = 5^{168} \bmod 48 =$ al valor de 5^{168} en $\mathbb{Z}_{48}^{*}$.

Como $\varphi(48)=16$, entonces aplicando el Teorema de Euler-Fermat tenemos que $5^{16} \equiv 1 \pmod{48}$ y por tanto $5^{16}=1$ en $\mathbb{Z}_{48}$. Como $168 = 16 \cdot 10 + 8$, entonces en $\mathbb{Z}_{48}$ tenemos que $5^{168} = 5^{16 \cdot 10 + 8} = \left(5^{16}\right)^{10} \cdot 5^{8} = 5^{8} = 1$

$5^2 = 25 \quad 5^4 = 1. \quad 5^8 = 1$

$$\begin{array}{r|l} 25 \cdot 25 = 625 & 48 \\ \hline 145 & 13 \\ 01 & \end{array}$$

Comenzaremos mostrando otro método para resolver ecuaciones diofanticas con 2 incognitas.

Ejercicio

Resolver la ecuacion diofantica $12x+15y=42$.

-D-

m.c.d$\{12,15\}=3$ y $3|42$. Por tanto, la ecuacion tiene solucion y ademas tiene las mismas soluciones que $4x+5y=14$.

$4x+5y=14 \Rightarrow 4x-14=-5y \Rightarrow 4x\equiv 14 \pmod 5 \Rightarrow$

$\Rightarrow 4x\equiv 4 \pmod 5 \Rightarrow \boxed{x=1+5k}$

$4x+5y=14 \Rightarrow 5y=14-4x \Rightarrow 5y=14-4(1+5k) \Rightarrow$

$\Rightarrow 5y=10-20k \Rightarrow \boxed{y=2-4k}$

Ejercicio

Resolver la ecuacion diofantica $8x+12y+18z=14$.

-D-

Como m.c.d$\{8,12,18\}=2$ y $2|14$, entonces la ecuacion tiene solucion. Ademas, tiene las mismas soluciones que la ecuacion $4x+6y+9z=7$. Para resolver esta ecuacion hacemos un cambio de variable. Como m.c.d$\{4,6\}=2$ entonces hacemos el cambio $4x+6y=2u$, y nos queda la ecuacion $2u+9z=7$. Vamos a resolver dicha ecuacion

$$2u+9z=7 \Rightarrow 2u \equiv 7 \pmod 9 \Rightarrow u=8+9k$$

$$9z=7-2u \Rightarrow 9z=7-2(8+9k) \Rightarrow 9z=-9-18k \Rightarrow$$

$$\Rightarrow \boxed{z=-1-2k}$$

Ahora de la igualdad $4x+6y=2u$ deducimos que $2x+3y=u$ y por tanto $2x+3y=8+9k$. Vamos a resolver esta ultima ecuacion como si fuera una ecuacion diofantica con dos incognitas.

$$3y \equiv 8+9k \pmod 2 \Rightarrow y \equiv k \pmod 2 \Rightarrow$$

$$\Rightarrow \boxed{y=k+2\bar{k}}$$

Como $2x+3y=8+9k \Rightarrow 2x=8+9k-3(k+2\bar{k}) \Rightarrow$

$$\Rightarrow 2x=8+6k-6\bar{k} \Rightarrow \boxed{x=4+3k-3\bar{k}}$$

NOTA

En el ejercicio anterior la ecuacion $y \equiv k \pmod 2$ la hemos podido resolver directamente. En general nos queda una ecuacion del tipo $3y \equiv 2k+1 \pmod 7$. ¿Como se resuelve esta ecuacion? Calculamos con ayuda del algoritmo extendido de Euclides $u, v \in \mathbb{Z}$ tq $3u+7v=1$ y entonces $u(2k+1) \bmod 7$ es una solución de la ecuación.

Como $3(-2)+7\cdot 1=1$ entonces $-2(2k+1) \bmod 7 = (-4k-2) \bmod 7 = 3k+5$ es una solución. Por tanto, todas las soluciones de $3y \equiv 2k+1 \pmod 7$ son

$$y = 3k+5+7\overline{k}.$$

EJERCICIO

Resolver la ecuación diofántica $33x-21y+15z=24$.

ORDEN PRODUCTO CARTESIANO

Sean $(A_1, \leq_1), (A_2, \leq_2), \ldots, (A_n, \leq_n)$ conjuntos ordenados. Entonces en el conjunto $A_1 \times A_2 \times \cdots \times A_n$ definimos la siguiente relación de orden $(a_1, \ldots, a_n) \leq_p (b_1, \ldots, b_n)$ si $a_1 \leq_1 b_1, \ldots, a_n \leq_n b_n$. A dicho orden lo llamaremos orden producto cartesiano de los órdenes $\leq_1, \leq_2, \ldots, \leq_n$.

EJEMPLO

Dados los conjunto ordenados $(\mathbb{Z}, \leq_u)$ y $(\mathbb{N}, \leq_m)$ dotamos a $\mathbb{Z} \times \mathbb{N}$ del orden producto cartesiano, esto es,

$(a,b) \leq_p (c,d)$ si $a \leq_u c$ y $b \leq_m d$.

Entonces $(-2,3) \leq_p (0,6)$ y $(-2,3) \nleq_p (0,4)$.

Calcular los elemento notables de $B=\{(2,3),(3,6),(-1,1),(4,7)\}$.

Maximales $(B)=\{(3,6),(4,7)\}$.

B no tiene maximo.

Minimales $(B)=\{(-1,1)\}$

$(-1,1)$ es el minimo de B.

(Cotas superiores de B) $=\{(a,b)\in \mathbb{Z}\times\mathbb{N}$ tq $4\leq_u a$ y b es multiplo de $42\}$.

El supremo de B es $(4,42)$

(Cotas inferiores de B) $=\{(a,b)\in\mathbb{Z}\times\mathbb{N}$ tq $a\leq_u -1$ y $b=1\}$

El infimo de B es $(-1,1)$

ORDEN LEXICOGRAFICO

El orden usual de $\mathbb{N}^n$ es el orden producto cartesiano de $(\mathbb{N},\leq_u),\dots,(\mathbb{N},\leq_u)$. Por tanto,

$(a_1,\dots,a_n)\leq_p(b_1,\dots,b_n)$ si $a_1\leq_u b_1,\dots,a_n\leq_u b_n$.

Este orden no es total ya que $(2,3)\not\leq_p(1,4)$ y $(1,4)\not\leq_p(2,3)$.

Existen ordenes en $\mathbb{N}^n$ que son totales, por ejemplo el orden lexicografico que se define de la siguiente forma $(a_1,\dots,a_n)\leq_{lex}(b_1,\dots,b_n)$ si $(a_1,\dots,a_n)=(b_1,\dots,b_n)$ ó $(a_1,\dots,a_n)\neq(b_1,\dots,b_n)$ y la primera coordenada distinta de cero de $(a_1-b_1, \dots, a_n-b_n)$ es negativa.

Ejemplo

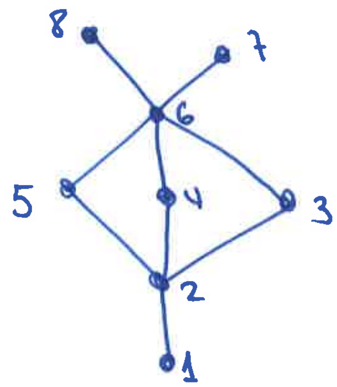
Ordenar de menor a mayor con el orden lexicográfico los elementos del conjunto $\{(1,1,1),(0,1,1),(0,0,2),(2,3,1),(1,0,4)\}$.

-D-

$$(0,0,2) \leq_{lex} (0,1,1) \leq_{lex} (1,0,4) \leq_{lex} (1,1,1) \leq_{lex} (2,3,1).$$

REPRESENTACION GRAFICA DE ORDENES

Cuando nos dan un gráfico de la forma



nos están dando un orden: un elemento a es menor que un elemento b si existe un camino siempre ascendente que conecta a y b. Por tanto, $2 \leq 7$ y $3 \nleq 4$.

- Calcular los elementos notables de $B=\{2,3,4\}$.

Maximales$(B)=\{3,4\}$, B no tiene máximo, Minimales$(B)=\{2\}$, mínimo$(B)=2$, (Cotas superiores de B$)=\{6,7,8\}$, Sup$(B)=6$, (Cotas inferiores de B$)=\{1,2\}$, Inf$(B)=2$

EL CUERPO DE LOS NUMEROS COMPLEJOS

El conjunto de los numeros complejos es $\mathbb{C}=\{a+bi \mid a,b\in\mathbb{R}\}$ donde $i^2=-1$. Si $a+bi$ es un numero complejo entonces a es la parte real y bi la parte imaginaria.

En $\mathbb{C}$ se define una suma y un producto de la siguiente forma: $(a+bi)+(c+di)=(a+c)+(b+d)i$ y

$$(a+bi)\cdot(c+di)=(ac-bd)+(bc+ad)i.$$

$$\begin{array}{r}
a+bi \\
c+di \\
\hline
ac+bci \\
adi-bd \\
\hline
(ac-bd)+(bc+ad)i
\end{array}$$

PROPOSICION

$(\mathbb{C},+,\cdot)$ es un cuerpo.

NOTA

$1+0\cdot i$ es el elemento neutro para el producto.

$0+0\cdot i$ es el elemento neutro para la suma, $-(a+bi)=(-a)+(-b)i$ y si $a+bi\neq 0$ entonces

$$(a+bi)^{-1}=\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i.$$

$$\left(\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i\right)(a+bi)=\frac{a^2}{a^2+b^2}-\frac{abi}{a^2+b^2}+$$
$$+\frac{abi}{a^2+b^2}+\frac{b^2}{a^2+b^2}=\frac{a^2+b^2}{a^2+b^2}=1$$

TEOREMA FUNDAMENTAL DEL ALGEBRA.

Si $a(x)\in\mathbb{C}[x]$ y $gr(a(x))\geq 1$, entonces $a(x)$ tiene al menos una raiz.

COROLARIO

Un polinomio $a(x)\in\mathbb{C}[x]$ es irreducible si y solo si $gr(a(x))=1$.

- Si $a+bi\in\mathbb{C}$ entonces su conjugado es $a-bi$.

PROPOSICION

La aplicacion $f:\mathbb{C}\longrightarrow\mathbb{C}$ definida por $f(a+bi)=a-bi$ verifica las siguientes propiedades:

1) $f((a+bi)+(c+di))=f(a+bi)+f(c+di)$
2) $f((a+bi)\cdot(c+di))=f(a+bi)\cdot f(c+di)$
3) $f(r)=r$ para todo $r\in\mathbb{R}$.
4) $f(0)=0$.

COROLARIO

Si $a+bi$ es una raíz de $a(x)\in\mathbb{R}[x]$, entonces $a-bi$ es también raíz de $a(x)$.

COROLARIO

Si $a(x)\in\mathbb{R}[x]$ es irreducible entonces $gr(a(x))\in\{1,2\}$.

NOTA

1) Todos los polinomios de grado 1 de $\mathbb{R}[x]$ son irreducibles.

2) Un polinomio de grado 2 de $\mathbb{R}[x]$ es irreducible si y solo si no tiene raíces reales.

IRREDUCIBILIDAD EN $\mathbb{Q}[x]$

~~Sea $a(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$~~ el problema de saber si un polinomio de $\mathbb{Q}[x]$ es o no irreducible es un problema muy difícil. No obstante existen algoritmos que nos determinan si un polinomio en $\mathbb{Q}[x]$ es o no irreducible. Nuestro objetivo en esta sección será dar dos criterios que nos dicen que si un polinomio de $\mathbb{Q}[x]$ verifica determinadas condiciones entonces es irreducible.

CRITERIO DE EISENSTEIN

Si $a(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$ es un polinomio de grado mayor o igual que 2 y existe un número primo p tq $p\nmid a_n$, $p\mid a_i$ para todo $i\in\{0,1,\ldots,n-1\}$ y $p^2\nmid a_0$,

$a(x)$ es un polinomio irreducible de $\mathbb{Q}[x]$.

EJERCICIO

Demostrar que el polinomio $x^7+6x^5+4x^2+2x^3+2$ es irreducible en $\mathbb{Q}[x]$.

-D-

Si tomamos $p=2$ y aplicamos el criterio de Eisenstein obtenemos que el polinomio es irreducible.

EJERCICIO.

Demostrar que si $n \in \mathbb{N}\setminus\{0,1\}$ y p es un número primo entonces $\sqrt[n]{p} \notin \mathbb{Q}$.

-D-

Aplicando el criterio de Eisenstein deducimos que $x^n - p$ es un polinomio irreducible de $\mathbb{Q}[x]$. Por tanto $x^n - p$ no tiene raíces en $\mathbb{Q}$ y por consiguiente $\sqrt[n]{p} \notin \mathbb{Q}$.

EJERCICIO

Sea $n \in \mathbb{N}\setminus\{0\}$. Demostrar que en $\mathbb{Q}[x]$ existen infinitos polinomios de grado n irreducibles.

-D-

Basta observar que todos los polinomios del siguiente conjunto son irreducibles $\{x^n - p \mid p$ es un número primo$\}$ y que números primos hay infinitos.

CRITERIO DE REDUCCION

Sea p un numero primo positivo, $a(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ un polinomio de grado $n \geq 1$ y $\bar{a}(x) = \bar{a}_0 + \bar{a}_1 x + \dots + \bar{a}_n x^n \in \mathbb{Z}_p[x]$ donde $\bar{a}_i = a_i \bmod p$. Si $gr(a(x)) = gr(\bar{a}(x))$ y $\bar{a}(x)$ es irreducible en $\mathbb{Z}_p[x]$ entonces $a(x)$ es irreducible en $\mathbb{Q}[x]$.

EJERCICIO

Demostrar que el polinomio $a(x) = x^4 + 17x^3 + 5x^2 + 3x + 1$ es irreducible en $\mathbb{Q}[x]$.

-D-

Tomo $p=2$. Veamos que $\bar{a}(x) = x^4 + x^3 + x^2 + x + 1$ es irreducible en $\mathbb{Z}_2[x]$.

$\bar{a}(x)$ no tiene raices.

x^2+x+1 es el unico polinomio monico e irreducible de grado 2 de $\mathbb{Z}_2[x]$.

$$\begin{array}{l|l} x^4+x^3+x^2+x+1 & x^2+x+1 \\ \cline{2-2} x^4+x^3+x^2 & x^2 \\ \hline \qquad\qquad x+1 & \end{array}$$

Por tanto el polinomio $\bar{a}(x)$ es irreducible en $\mathbb{Z}_2[x]$. Aplicando el criterio de reduccion podemos afirmar que $a(x)$ es irreducible en $\mathbb{Q}[x]$.

ECUACIONES EN CONGRUENCIAS EN $\mathbb{K}[x]$

Sean $\{a(x), b(x), m(x)\} \subseteq \mathbb{K}[x]$. Escribiremos $a(x) \equiv b(x) \pmod{m(x)}$ si $m(x) \mid a(x) - b(x)$.

- Una ecuación de grado 1 en $\mathbb{K}[x]$ es una ecuación de la forma $a(x) X \equiv b(x) \pmod{m(x)}$.

TEOREMA

1) La ecuación $a(x) X \equiv b(x) \pmod{m(x)}$ tiene solución si y sólo si $\text{m.c.d}\{a(x), m(x)\} \mid b(x)$.

2) Si $d(x) = \text{m.c.d}\{a(x), m(x)\}$ y $d(x) \mid b(x)$, entonces las ecuaciones $a(x) X \equiv b(x) \pmod{m(x)}$ y $\frac{a(x)}{d(x)} X \equiv \frac{b(x)}{d(x)} \left(\text{mod } \frac{m(x)}{d(x)}\right)$ tienen las mismas soluciones.

3) Si $\text{m.c.d}\{a(x), m(x)\} = 1$ y $u(x)$ es una solución de $a(x) X \equiv b(x) \pmod{m(x)}$ entonces el conjunto formado por todas las soluciones de la ecuación es $\{u(x) + k(x) m(x) \mid k(x) \in \mathbb{K}[x]\}$.

4) La ecuación $a(x) X + c(x) \equiv b(x) \pmod{m(x)}$ tiene las mismas soluciones que $a(x) X \equiv b(x) - c(x) \pmod{m(x)}$.

5) La ecuación $a(x) X \equiv b(x) \pmod{m(x)}$ tiene las mismas soluciones que $(a(x) \text{ mod } m(x)) X \equiv b(x) \text{ mod } m(x) \pmod{m(x)}$.

6) Si $u(x), v(x) \in \mathbb{K}[x]$ y $a(x) u(x) + m(x) v(x) = 1$, entonces $b(x) u(x) \text{ mod } m(x)$ es una solución de $a(x) X \equiv b(x) \pmod{m(x)}$.

EJERCICIO

Resolver la ecuacion $(x+1)X \equiv x \pmod{x^2}$ en $\mathbb{Z}_2[x]$

-D-

$m.c.d\{x^2, x+1\} = 1$.

Le aplicamos el algoritmo extendido de Euclides a x^2 y $x+1$

$$(a_0(x), a_1(x)) = (x^2, x+1) \overset{q(x)=x+1}{=} (x+1, 1) = (1, 0)$$

$$(s_0(x), s_1(x)) = (1, 0) = (0, 1) = (1, un)$$

$$(t_0(x), t_1(x)) = (0, 1) = (1, x+1) = (x+1, un)$$

$$\begin{array}{l|l} x^2 & x+1 \\ \hline x^2+x & x+1 \\ \hline x & \\ x+1 & \\ \hline 1 & \end{array}$$

$$x^2 \cdot 1 + (x+1)(x+1) = 1.$$

$$\begin{array}{l|l} x^2+x & x^2 \\ \hline x^2 & 1 \\ \hline x & \end{array}$$

Por el punto 6) del teorema anterior sabemos que $x(x+1) \bmod x^2 = x$ es una solucion de la ecuacion $(x+1)X \equiv x \pmod{x^2}$. Aplicando ahora el punto 3) del teorema anterior tenemos que el conjunto de todas las soluciones de la ecuacion es $\{x + p(x)x^2 \text{ tq } p(x) \in \mathbb{Z}_2[x]\}$.

SISTEMAS DE ECUACIONES EN CONGRUENCIAS EN $\mathbb{K}[x]$

Resolver el siguiente sistema en $\mathbb{Z}_2[x]$

$$\left.\begin{array}{l} (x+1)X \equiv x \pmod{x^2} \\ x \cdot X \equiv x+1 \pmod{x^2+x+1} \end{array}\right\}$$

-D-

$m.c.d\{x+1, x^2\} = 1$ y $m.c.d\{x, x^2+x+1\} = 1$.

Por tanto las dos ecuaciones tienen solución y ya están simplificadas.

Resolvemos la primera ecuación $X = x + k(x)\cdot x^2$ y sustituimos en la segunda ecuación.

$$x\left(x+k(x)\cdot x^2\right) \equiv x+1 \left(\text{mod } x^2+x+1\right) \Rightarrow$$

$$\Rightarrow x^2 + k(x)x^3 \equiv x+1 \left(\text{mod } x^2+x+1\right) \Rightarrow$$

$\Rightarrow k(x)\,x^3 \equiv x^2+x+1 \left(\text{mod } x^2+x+1\right) \Rightarrow$ (Aplicando el punto 5) del Teorema anterior) $\Rightarrow k(x) \equiv 0 \left(\text{mod } x^2+x+1\right) \Rightarrow$

$\Rightarrow k(x) = 0 + \bar{k}(x)\left(x^2+x+1\right)$. Por tanto,

$$X = x + \left(0+\bar{k}(x)\left(x^2+x+1\right)\right)x^2 \Rightarrow X = x + \bar{k}(x)\,x^2\left(x^2+x+1\right)$$

$$\Rightarrow X = x + \bar{k}(x)\left(x^4+x^3+x^2\right).$$

ECUACIONES DIOFANTICAS EN $\mathbb{K}[x]$

Resolver la siguiente ecuación en $\mathbb{Z}_3[x]$

$$(x^2+1)X + x^2 Y = x+2.$$

-D-

$$(x^2+1)X \equiv x+2 \left(\text{mod } x^2\right) \Rightarrow X \equiv x+2 \left(\text{mod } x^2\right)$$

$$\Rightarrow \boxed{X = x+2+k(x)\,x^2}$$

$$x^2 Y = x+2 + (2x^2+2)\left(x+2+k(x)\,x^2\right) \Rightarrow$$

$\Rightarrow x^2 \cdot Y = (x+2) + (x+2)(2x^2+2) + k(x)\, x^2(2x^2+2) \Rightarrow$

$\Rightarrow x^2 \cdot Y = (x+2)2x^2 + k(x)\, x^2(2x^2+2) \Rightarrow \boxed{Y = (2x+1) + k(x)(2x^2+2)}$

EJERCICIO

Resolver en el anillo $\mathbb{Z}_7[x]_{x^3+2x^2+2x+1}$ la ecuacion

$$(3x^2+4)A + 3x+1 = (2x^2+5)A + x+5$$

$\Rightarrow$

$$(x^2+6)A = 5x+4$$

Vamos a calcular el m.c.d de x^2+6 y x^3+2x^2+2x+1

$$(a_0(x), a_1(x)) = (x^3+2x^2+2x+1, x^2+6) = (x^2+6, 3x+3) = (3x+3, 0)$$

$$\text{m.c.d}\{x^3+2x^2+2x+1, x^2+6\} = x+1 \Rightarrow \text{No existe } (x^2+6)^{-1}$$

$$(x^2+6)A \equiv 5x+4 \ (\text{mod } x^3+2x^2+2x+1)$$

$$\begin{array}{r|l} 5x+4 & x+1 \\ \hline 2x+2 & 5 \\ \hline 6 & \end{array}$$

Como $x+1 \nmid 5x+4$ la congruencia no tiene solucion

y por tanto ~~dos~~ la ecuacion no tiene solucion.

INTERPOLACION

Sea $\mathbb{K}$ un cuerpo y sea $\{(\alpha_1,\beta_1),\dots,(\alpha_n,\beta_n)\}\subseteq\mathbb{K}^2$ con $\alpha_i\neq\alpha_j$ si $i\neq j$. El problema de interpolacion consiste en calcular un polinomio $a(x)\in\mathbb{K}[x]$ tq $a(\alpha_1)=\beta_1,\dots,a(\alpha_n)=\beta_n$.

Teorema de Lagrange

Existe un unico polinomio $a(x)\in\mathbb{K}[x]$ tq $gr(a(x))<n$ y $a(\alpha_1)=\beta_1,\dots,a(\alpha_n)=\beta_n$. Ademas, dicho polinomio es

$a(x)=\beta_1 L_1(x)+\dots+\beta_n L_n(x)$ donde

$$L_i(x)=\left((\alpha_i-\alpha_1)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_n)\right)^{-1}(x-\alpha_1)\dots(x-\alpha_{i-1})(x-\alpha_{i+1})\dots(x-\alpha_n)$$

EJERCICIO

Calcular $a(x)\in\mathbb{Z}_7[x]$ tq $a(1)=3$, $a(2)=0$ y $a(4)=3$.

-D-

$a(x)=3\cdot L_1(x)+0\cdot L_2(x)+3\cdot L_3(x)$

$$L_1(x)=\left((1-2)(1-4)\right)^{-1}(x-2)(x-4)=5(x^2+x+1)=5x^2+5x+5$$

$$L_3(x)=\left((4-1)(4-2)\right)^{-1}(x-1)(x-2)=6(x^2+4x+2)=6x^2+3x+5.$$

$$a(x)=3(5x^2+5x+5)+3(6x^2+3x+5)=x^2+x+1+4x^2+2x+1\Rightarrow$$

$$\Rightarrow \boxed{a(x)=5x^2+3x+2}$$

Comprobacion: $a(1)=5+3+2=3$

$a(2)=5\cdot4+3\cdot2+2=6+6+2=0$

$a(4)=5\cdot2+3\cdot4+2=3+5+2=3$

METODO DE NEWTON

Sea $a(x) \in \mathbb{K}[x]$. Entonces son equivalentes las siguientes condiciones:

1) $a(\alpha_1) = \beta_1, \dots, a(\alpha_n) = \beta_n$.

2) $a(x)$ es solucion del sistema $\left.\begin{array}{l} X \equiv \beta_1 \ (\text{mod } x-\alpha_1) \\ \vdots \qquad\quad \vdots \\ X \equiv \beta_n \ (\text{mod } x-\alpha_n) \end{array}\right\}$

EJERCICIO

Calcular todos los polinomios $a(x) \in \mathbb{Z}_7[x]$ tq $a(1) = 3$, $a(2) = 0$ y $a(4) = 3$.

-D-

$\left.\begin{array}{l} X \equiv 3 \ (\text{mod } x+6) \\ X \equiv 0 \ (\text{mod } x+5) \\ X \equiv 3 \ (\text{mod } x+3) \end{array}\right\}$

$X = 3 + k(x)(x+6)$

$3 + k(x)(x+6) \equiv 0 \ (\text{mod } x+5)$

$\Updownarrow$

$k(x)(x+6) \equiv 4 \ (\text{mod } x+5) \Rightarrow$

$\Rightarrow k(x) \equiv 4 \ (\text{mod } x+5) \Rightarrow k(x) = 4 + \bar{k}(x)(x+5)$

$X = 3 + (4 + \bar{k}(x)(x+5))(x+6) = 4x + 6 + \bar{k}(x)(x+5)(x+6)$

$4x+6+\bar{k}(x)(x+5)(x+6) \equiv 3 \ (\text{mod } x+3) \Rightarrow \bar{k}(x)(x+5)(x+6) \equiv$

$\equiv 3x+4 \ (\text{mod } x+3) \Rightarrow 6\bar{k}(x) \equiv 2 \ (\text{mod } x+3) \Rightarrow$

$\Rightarrow \bar{k}(x) \equiv 5 \ (\text{mod } x+3) \Rightarrow \bar{k}(x) = 5 + \bar{\bar{k}}(x)(x+3)$

$X = 4x+6+(5+\bar{\bar{k}}(x)(x+3))(x+5)(x+6) = 4x+6+5(x+5)(x+6) +$

$+ \bar{\bar{k}}(x)(x+3)(x+5)(x+6) = 5x^2+3x+2+\bar{\bar{k}}(x)(x+3)(x+5)(x+6)$.