1. Criterio de irreducibilidad de polinomios módulo un primo

Si $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}_p[x]$, podemos calcular el mcd de f con su polinomio derivada $f'(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a1$ en $\mathbb{Z}_p[x]$, Si $g_1(x) = \text{mcd}(f, f') \neq 0$. Entonces, $f(x)$ es reducible

$$g(x) = \frac{f(x)}{g_1(x)} \Longleftrightarrow f(x) = g(x)g_1(x)$$

En caso contrario, $f(x)$ es libre de cuadrados y su factorización única es en irreducibles distintos de $\mathbb{Z}_p[x]$. O sea, $f(x) = f_1(x)\cdots f_r(x)$.
Y si llamamos $n_i = \text{gr}\big(f_i(x)\big)$, se tiene $n = \sum_{i=1}^r n_i$.

Como cada irreducible de grado n_i es un factor del polinomio $x^{p^{n_i}} - x$ que también es libre de cuadrados. Entonces, $F_{p^{n_i}}$ es el c.f. más pequeño que contiene a las raíces de $f_i(x)$.

Como un c.f. está contenido en otro si y sólo si tienen la misma característica p y sus exponentes se dividen. El menor cuerpo que contiene a todas las raíces de $f(x)$, libre de cuadrados, es F_{p^m}, donde $m = \text{mcm}(n_1, \ldots, n_r)$ ya que es el menor cuerpo que contiene a cada uno de los $F_{p^{n_i}}$. Y tenemos que

Teorema 1. *$f(x) \in \mathbb{Z}_p[x]$ libre de cuadrados es irreducible si y sólo si $n = m$.*

Para hacerlo efectivo necesitamos hallar el m mínimo tal que F_{p^m} contenga a todas las raíces. Pero es equivalente a hallar el mínimo tal que $f(x) | x^{p^m} - x$.

Luego el algoritmo se inicia con $g = x^p$; $k = 1$; Y va sucesivamente dividiendo $g - x$ por f. Si no da resto cero, se calcula $g = g^p$. O sea,

```
g = x^p; g1 = PolynomialRemainder[g - x, f, x, Modulus -> mod];
Mientras[Length[g1] > 0,
g = PolynomialMod[g^mod, f, Modulus -> mod];
g1 = PolynomialRemainder[g - x, f, x, Modulus -> mod]; k++];
Return[k];
```

Ejemplo 1. $f = 1 + x + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^{10} + x^{11} + x^{14} \in \mathbb{Z}_2[x]$ *es libre de cuadrados porque el mcd con su derivada es 1.*

Aplicando el algoritmo anterior retorna 33.
Luego el menor c.f. que contiene a sus raíces es $F_{2^{33}}$.

Como $33 > 14$, $f(x)$ *es reducible en* $\mathbb{Z}_2[x]$.
Y como $33 = 3*11$ *y* $3+11 = 14$ *que es el grado del polinomio. Como además son los únicos enteros positivos tales que satisfacen esas condiciones. Necesariamente* $f(x)$ *descompone en dos polinomios irreducibles de grados* 3 *y* 11 *respectivamente. Para hallarlos calculamos la matriz de Berlekamp* $B - Id$ *y resolvemos el s.l. asociado.*

Como sale rango(B-Id) = 12, hay 14-12=2 soluciones independientes. La 1ª no da polinomio f*-reductor y la 2ª da los coeficientes de*

$$h(x) = x + x^2 + x^4 + x^5 + x^7 + x^9 + x^{10} + x^{11} + x^{12}$$

que si es f*-reductor porque los mcds módulo 2 son*

$$\left.\begin{array}{l} f_1(x) = mcd\big(f(x), h(x)\big) = 1 + x + x^3 \\ f_2(x) = mcd\big(f(x), h(x) - 1\big) = 1 + x^2 + x^3 + x^5 + x^6 + x^9 + x^{11} \end{array}\right\} \Longrightarrow f(x) = f_1(x) f_2(x)$$

O sea, hemos obtenido las factorización en irreducibles de $f(x)$.
No es necesario comprobar la irreducibilidad de los dos factores porque el algoritmo inicial lo asegura.

El proceso se puede aplicar recursivamente si el mcd con la derivada es distinto de cero. Por ej.

Ejemplo 2. $f = 1 + x + x^5 + x^6 + x^8 + x^{10} + x^{11} + x^{17} + x^{20} \in \mathbb{Z}_2[x]$ *no es libre de cuadrados porque el mcd con su derivada es* $g = 1 + x^2 + x^6$

Como el cociente módulo 2 es

$$f/g = 1 + x + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^{10} + x^{11} + x^{14}$$

Coincide con el polinomio del ejemplo anterior.

Luego para factorizar f, tenemos que factorizar $g = 1 + x^2 + x^6$.
Como la derivada de este último es cero módulo 2 es una potencia módulo 2, que se ve a ojo

$$g = 1 + x^2 + x^6 = (1 + x + x^3)^2$$

Finalmente, la factorización completa es

$$f(x) = (1 + x + x^3)^2(1 + x + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^{10} + x^{11} + x^{14}) =$$
$$= (1 + x + x^3)^3(1 + x^2 + x^3 + x^5 + x^6 + x^9 + x^{11})$$