Polinómios primitivos e matrizes companheiras

Pedro Patricio, Maio de 2006

Dado um polinómio mónico $f(x) = a_0 + a_1 x + \ldots a_{n-1}x^{n-1} + x^n$, podemos definir o vector dos coeficientes $\mathbf{r}_{f(x)} = [a_0\, a_1\, \ldots\, a_{n-1}]^T$, e a matriz companheira $L[f(x)] = \begin{bmatrix} 0 \ldots 0 & \\ I_{n-1} & -\mathbf{r}_{f(x)} \end{bmatrix}$.

Assume-se que $f(x) \in \mathbb{Z}_p[x]$ é irredutível, e portanto, que $\mathbb{Z}_p[x]/(f(x))$ é um corpo. Pretende-se calcular os coeficientes de $x^k \mod f(x)$. De facto, mostraremos que $\mathbf{r}_{x^k} = L[f(x)]^{k-1}[0\,1\,0 \ldots 0]^T$, desde que $k \geq 1$. A prova é feita por indução.

Para $k = 1$ é imediato.

Suponhamos, então, que $\mathbf{r}_{x^k} = L[f(x)]^{k-1}[0\,1\,0 \ldots 0]^T$. Para facilitar a escrita, $L = L[f(x)]$, e $x^k \mod f(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} = (L^{k-1} \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix})^T \begin{bmatrix} 1 \\ x \\ x^2 \\ \vdots \\ x^{n-1} \end{bmatrix}$.

$$x^{k+1} = x^k x = (L^{k-1} \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix})^T \begin{bmatrix} 1 \\ x \\ x^2 \\ \vdots \\ x^{n-1} \end{bmatrix} x = (b_0 + b_1 x + \cdots + b_{n-1}x^{n-1})x = -b_{n-1}a_0 +$$

$$(b_0 - b_{n-1}a_1)x + (b_1 - b_{n-1}a_2)x^2 + \cdots + (b_{n-2} - b_{n-1}a_{n-1})x^{n-1}$$

$$\text{Tal é igual a } (\begin{bmatrix} 0 & \ldots & 0 & -a_0 \\ 1 & & & -a_1 \\ & & & \\ 0 & \ldots & 0 & -a_{n-1} \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix})^T \begin{bmatrix} 1 \\ x \\ \vdots \\ x^{n-1} \end{bmatrix} = (LL^{k-1} \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix})^T \begin{bmatrix} 1 \\ x \\ \vdots \\ x^{n-1} \end{bmatrix}.$$

Portanto,

$$\mathbf{r}_{x^{k+1}} = L^k \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$