Esempio di fattorizzazione con Berlekamp

Troviamo la decomposizione in fattori irriducibili di $x^{20}+1 \in \mathbb{Z}_5[x]$.
Prima osservazione: essendo $\mathbb{Z}_5[x]$ un anello di caratteristica prima $p=5$, vale: $x^{20}+1=(x^4+1)^5$. Quindi si tratta di fattorizzare $f=x^4+1$.
Dati inziali: $p=5$, $d=\deg(f)=4$.
Si tratta di dividere x^{jp} per f con $j=0,\dots,d-1$ cioè $j=0,1,2,3$ e calcolare i resti r_0,r_1,r_2,r_3 delle divisioni:
$x^0=0\cdot f+1, \quad x^5=()\cdot f+4x, \quad x^{10}=()\cdot f+x^2, \quad x^{15}=()\cdot f+4x^3.$
Pertanto:
$r_0=1, \qquad r_1=4x, \qquad r_2=x^2, \qquad r_3=4x^3.$
Osservazione. Per calcolare i resti, in questo esempio, si può procedere come segue: una volta trovato che $x^5=qf+4x$ (con q opportuno che non serve calcolare), allora $x^{10}=x^5\cdot x^5=(qf+4x)\cdot(qf+4x)=()\cdot f+16x^2$, quindi $r_2=16x^2=x^2$. Analogamente $x^{15}=x^{10}\cdot x^5=\big(()\cdot f+x^2\big)\cdot(()\cdot f+4x)=()\cdot f+4x^3$.

Calcoliamo ora la matrice Q, le cui colonne sono i coefficienti di r_0,r_1,r_2,r_3, rispettivamente.
Abbiamo:
$r_0=1+0x+0x^2+0x^3, \quad r_1=0+4x+0x^2+0x^3,$
$r_2=0+0x+4x^2+0x^3, \quad r_3=0+0x+0x^2+4x^3.$
Pertanto:

$$Q=\begin{pmatrix}1&0&0&0\\0&4&0&0\\0&0&1&0\\0&0&0&4\end{pmatrix} \quad \text{e quindi} \quad Q-I=\begin{pmatrix}0&0&0&0\\0&3&0&0\\0&0&0&0\\0&0&0&3\end{pmatrix}$$

Allora il $\ker(Q-I)$ è dato dai vettori ${}^t(b_0,b_1,b_2,b_3)$ tali che $b_1=0,\ b_3=0$. Quindi una base di $\ker(Q-I)$ è data da ${}^t(1,0,0,0),\ {}^t(0,0,1,0)$. Quindi lo spazio vetoriale G dato dai polinomi $g\in\mathbb{Z}_5[x]$ tali che $\deg(g)<d$ e $f|(g^5-g)$ è il seguente:

$$G=\{a+bx^2 \mid a,b\in\mathbb{Z}_5\}$$

Scegliamo un elemento di $g\in G$ di grado almeno 1, per esempio $g=x^2$. Allora abbiamo:

$$f=\operatorname{mcd}(f,x^2)\cdot\operatorname{mcd}(f,x^2+1)\cdot\operatorname{mcd}(f,x^2+2)\cdot\operatorname{mcd}(f,x^2+3)\cdot\operatorname{mcd}(f,x^2+4)$$

Osservazione. Come calcolare i massimi comun divisori in questo esempio: si tratta innanzitutto di dividere f per x^2, per x^2+1 ecc. e calcolare i resti. Quindi si tratta di calcolare un rappresentante di $[f]$ nell'anello quoziente $\mathbb{Z}_5[x]/(x^2)$ o nell'anello quoziente $\mathbb{Z}_5[x]/(x^2+1)$ ecc. Ad esempio, nell'anello quoziente $\mathbb{Z}_5[x]/(x^2+1)$ vale: $[x^2]=-1$, quindi $[f]=[x^4+1]=[x^2]^2+1=(-1)^2+1=2$. Quindi il resto della divisione di x^4+1 per x^2+1 vale 2. Allora $\operatorname{mcd}(x^4+1,x^2+1)=\operatorname{mcd}(2,x^2+1)=1$. Similmente, il $\operatorname{mcd}(f,x^2+2)$ si calcola cercando il rappresentante canonico di $[f]$ in $\mathbb{Z}_5[x]/(x^2+2)$, dove vale: $[x^2]=[3]$. Quindi $[x^4+1]=[x^2]^2+[1]=[3]^2+[1]=0$. Pertanto $\operatorname{mcd}(x^4+1,x^2+2)=\operatorname{mcd}(0,x^2+2)=x^2+2$.
La decomposizione di sopra di f allora risulta:

$$f=1\cdot 1\cdot(x^2+2)\cdot(x^2+3)\cdot 1$$

Poichè la dimensione del nucleo di $Q - I$ è 2 e poichè abbiamo trovato due fattori di f, se i due fattori sono privi di quadrati, sono irriducibili e sono la decomposizione di f in fattori irriducibili (III teorema di Berlekamp). Calcolando $\mathrm{mcd}\,(x^2+2, D(x^2+2))$ e $\mathrm{mcd}\,(x^2+3, D(x^2+3))$ si vede subito che i due fattori sono in effetti privi di quadrati. Pertanto abbiamo che la decomposizione in fattori irriducibili di $x^{20}+1$ è la seguente:

$$x^{20} + 1 = (x^2 + 2)^5 \cdot (x^2 + 3)^5$$