Moltiplicare efficacemente i polinomi in caratteristica 2

Ottavio Giulio Rizzo
Ottavio.Rizzo@UniMI.it

Dipartimento di matematica «Federigo Enriques»
Università degli Studi di Milano

De Cifris Athesis — 15 aprile 2019

Campi finiti

Teorema

Sia $\mathbf{F}$ *un campo di* $n < \infty$ *elementi. Allora:*

- $n = p^s$ *con* p *primo ed* $s \in \mathbf{N}$ *opportuno;*
- $\mathbf{F} \simeq \dfrac{\mathbf{F}[x]}{\langle g(x) \rangle}$ *dove* $g(x) \in \mathbf{F}_p[x]$ *è irriducibile di grado* s.

Proposizione

Se $\#\mathbf{F} = \#\mathbf{F}' < \infty$, *allora* $\mathbf{F} \simeq \mathbf{F}'$. *Parliamo quindi del campo finito* $\mathbf{F}_{p^s} = GF(p^s)$ *di ordine* p^s.

Elementi primitivi

Definizione

$\alpha \in \mathbf{F}_{p^s}$ è *primitivo* se $\mathbf{F}_{p^s} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^s-2}\}$

Esempio

Sia $\mathbf{F} = \mathbf{F}_3[x]/\langle x^2+1\rangle$ e sia $i \in \mathbf{F}$ con $i^2 = -1$. Allora i non è un elemento primitivo, mentre $\alpha = i+1$ lo è:

$$\alpha^2 = (i+1)^2 = i^2 + 2i + 1 = 2i = -i, \qquad \alpha^3 = -i(i+1) = -i^2 - i = -i + 1$$
$$\alpha^4 = (-i)^2 = -1, \qquad \alpha^5 = \alpha^4 \cdot \alpha = -i - 1$$
$$\alpha^6 = -\alpha^2 = i, \qquad \alpha^7 = -\alpha^3 = i - 1$$

Proposizione

Sia $\alpha \in \mathbf{F}_{p^s}$ *e sia* $g(x) \in \mathbf{F}_p[x]$ *il suo polinomio minimo. Allora* α *è un elemento primitivo se e solo se* $g(x)$ *è irriducibile di grado* s *e il minimo* $n \in \mathbf{N} : g(x) | x^n - 1$ *è* $n = p^s - 1$.

Definizione

Chiamiamo *primitivo* un tale polinomio.

Proposizione

Sia $\alpha \in \mathbf{F}_{p^s}$ *e sia* $g(x) \in \mathbf{F}_p[x]$ *il suo polinomio minimo. Allora* α *è un elemento primitivo se e solo se* $g(x)$ *è irriducibile di grado* s *e il minimo* $n \in \mathbf{N} : g(x) | x^n - 1$ *è* $n = p^s - 1$.

Definizione

Chiamiamo *primitivo* un tale polinomio.

Esempio

Se $\mathbf{F} = \mathbf{F}_3[x]/\langle x^2 + 1 \rangle$ abbiamo $p^s - 1 = 8$. Allora

- i ha polinomio minimo $x^2 + 1 | x^4 - 1$
- $i + 1$ ha polinomio minimo $x^2 + x + 2$ che divide solo $x^8 - 1$.

Basi

Proposizione

Se $\alpha \in \mathbf{F} = \mathbf{F}_{p^s}$ *ha polinomio minimo di grado* s*, allora* $\{1, \alpha, \ldots, \alpha^{s-1}\}$ *è una base di* $\mathbf{F}$ *come* $\mathbf{F}_p$*-spazio vettoriale.*

Basi

Proposizione

Se $\alpha \in \mathbf{F} = \mathbf{F}_{p^s}$ *ha polinomio minimo di grado* s*, allora* $\{1, \alpha, \ldots, \alpha^{s-1}\}$ *è una base di* $\mathbf{F}$ *come* $\mathbf{F}_p$*-spazio vettoriale.*

Somme

La somma di due elementi di $\mathbf{F}$ è banale

Basi

Proposizione

Se $\alpha \in \mathbf{F} = \mathbf{F}_{p^s}$ *ha polinomio minimo di grado* s*, allora* $\{1, \alpha, \ldots, \alpha^{s-1}\}$ *è una base di* $\mathbf{F}$ *come* $\mathbf{F}_p$*-spazio vettoriale.*

Somme

La somma di due elementi di $\mathbf{F}$ è banale

Prodotti

Il prodotto di due elementi di $\mathbf{F}$ si ottiene dal prodotto di polinomi.

Problema

La struttura moltiplicativa di $\mathbf{F}$ dipende dalla scelta di α (del polinomio minimo di α).

Prodotto in campi finiti

Siano $\alpha \in \mathbf{F}$ come sopra, e sia $g(x)$ il polinomio minimo di α su $\mathbf{F}_p$. Abbiamo un morfismo di $\mathbf{F}_p$-algebre:

$$\psi : \mathbf{F}_p[x] \longrightarrow \frac{\mathbf{F}_p[x]}{\langle g(x) \rangle} \longrightarrow \mathbf{F}$$

$$\begin{array}{ccc} f(x) & \longmapsto & f(\alpha) \\ \| & & \| \\ \sum_{i=0}^{s-1} a_i x^i & \longmapsto & \sum_{i=0}^{s-1} a_i \alpha^i \end{array}$$

Siano

$$f(x) = \sum_{i=0}^{s-1} a_i x^i \qquad \nu = \psi(f) = \sum_{i=0}^{s-1} a_i \alpha^i$$

$$h(x) = \sum_{i=0}^{s-1} b_i x^i \qquad \mu = \psi(h) = \sum_{i=0}^{s-1} b_i \alpha^i$$

Allora

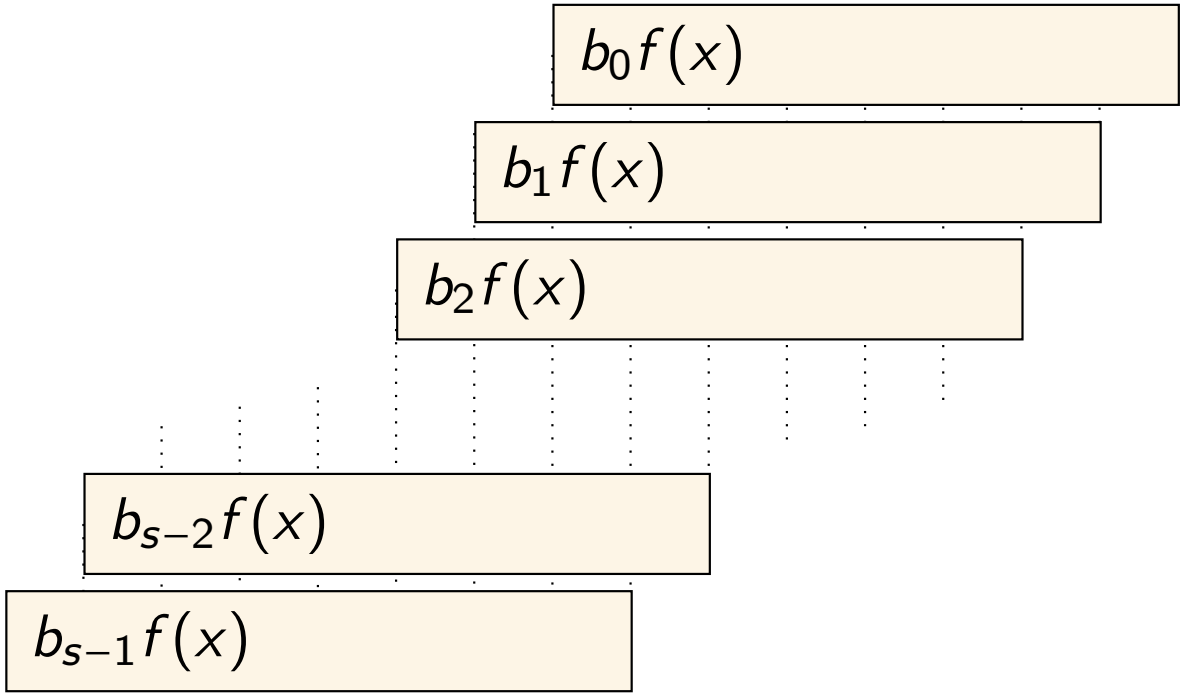
$$\nu \cdot \mu = \psi(f \cdot h) = (fh \bmod g)|_{x=\alpha}$$

Algoritmo scolastico

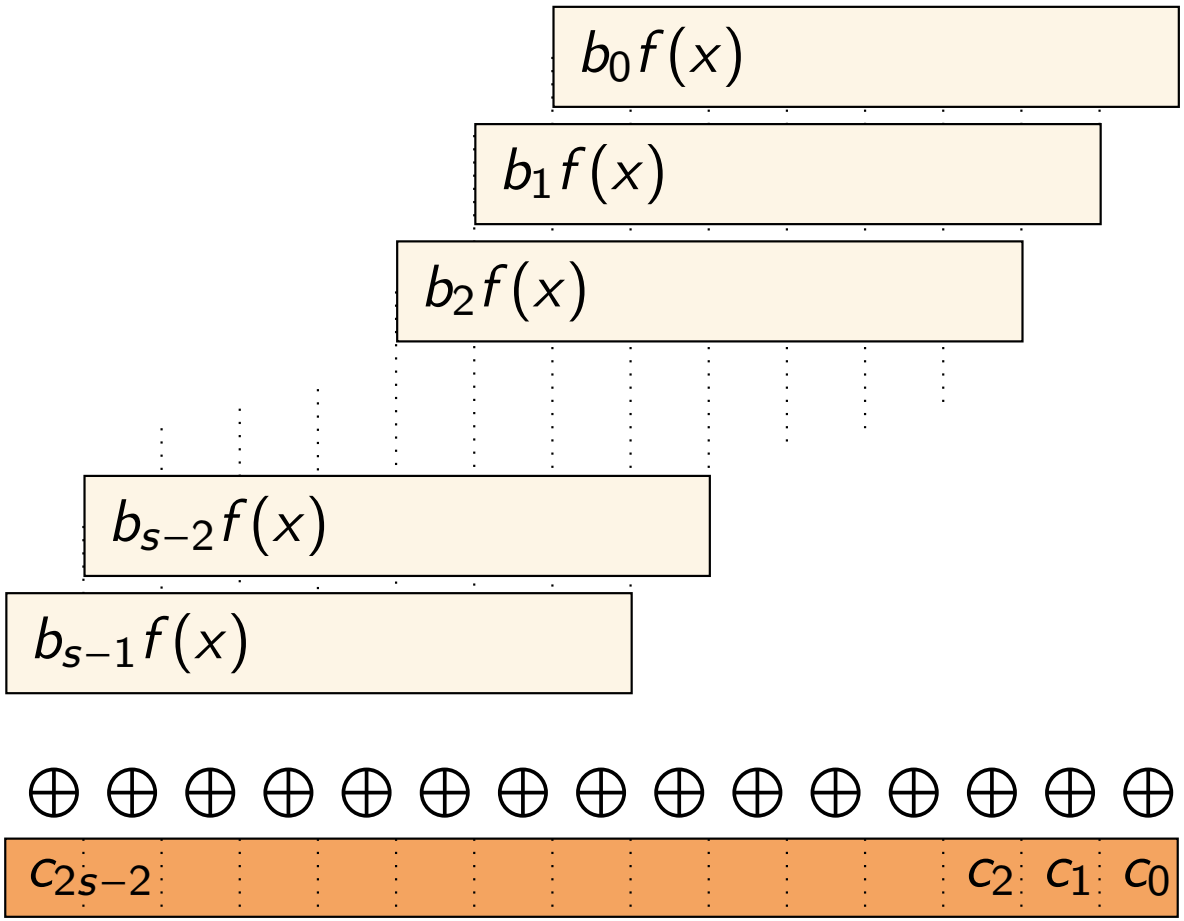
Siano $f(x) = \sum_{i=0}^{s-1} a_i x^i$, $h(x) = \sum_{i=0}^{s-1} b_i x^i$. Se $\ell(x) = f(x) \cdot h(x)$, allora

$$\ell(x) = \sum_{i=0}^{2s-2} c_i x^i, \text{ dove } c_i = \begin{cases} \sum_{j=0}^{i} a_j b_{i-j} & \text{se } 0 \le i \le s-1 \\ \sum_{j=i-s+1}^{s-1} a_j b_{i-j} & \text{se } s \le i \le 2s-2 \end{cases}$$

Algoritmo scolastico, p qualsiasi



Algoritmo scolastico, p qualsiasi



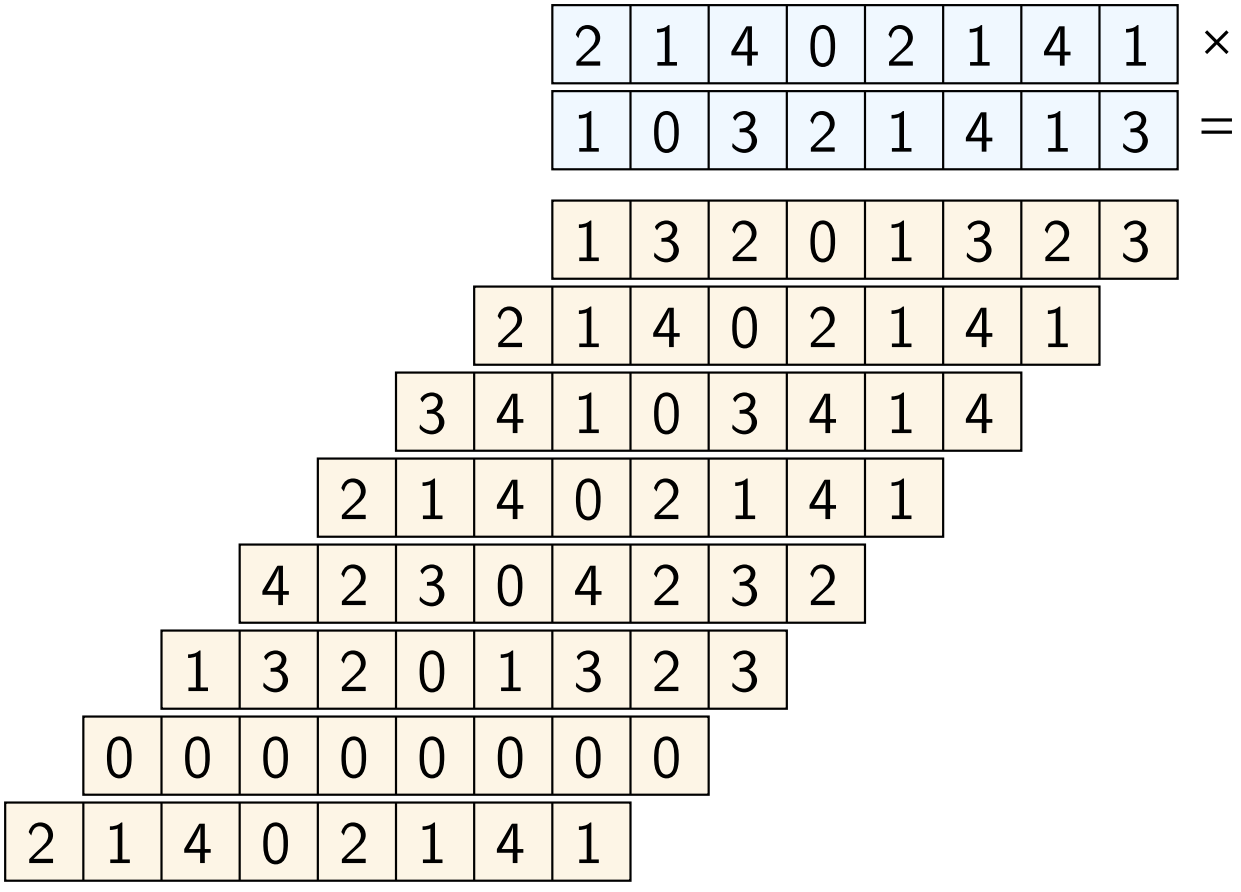
Un esempio

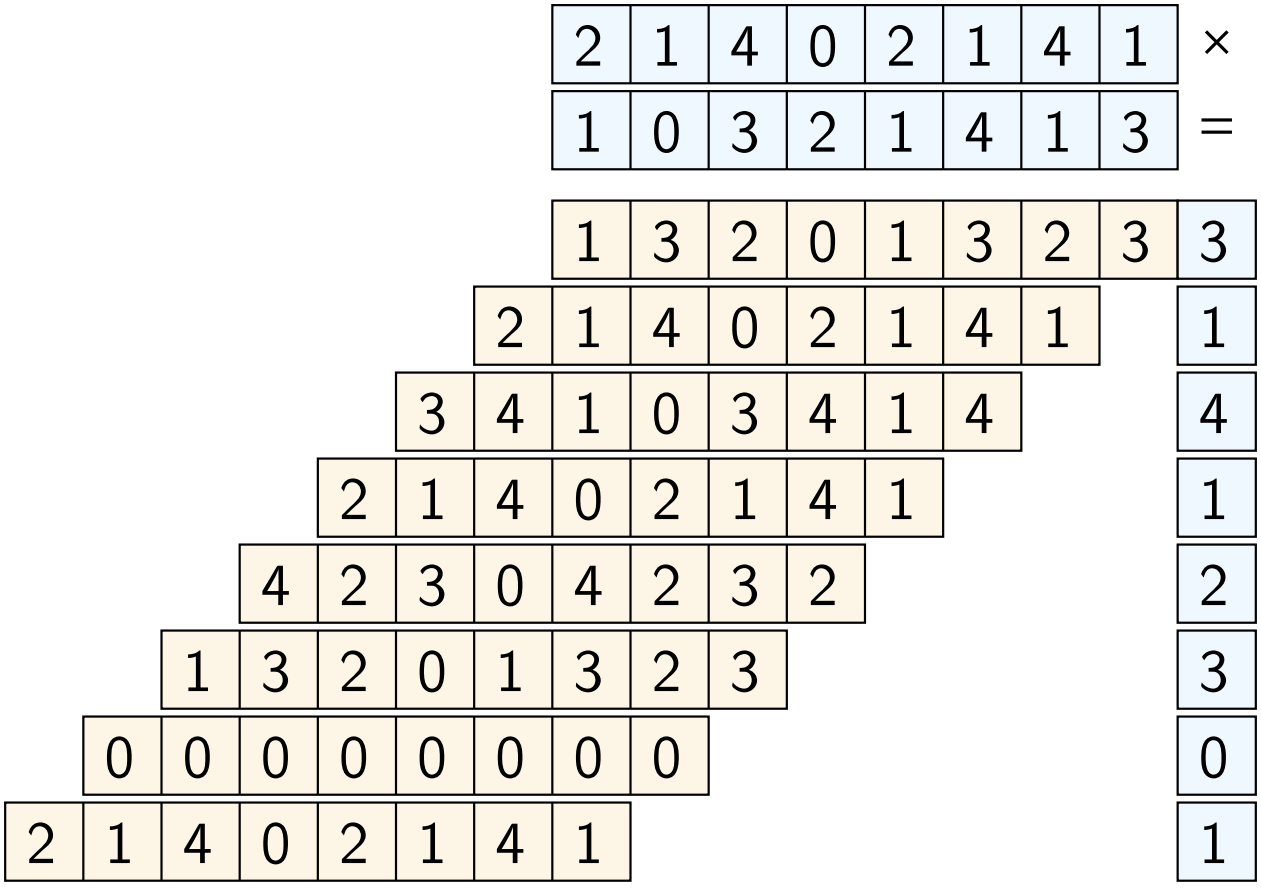
Sia $g(x) = x^8 + x^4 + 2 \in \mathbf{F}_5[x]$: è irriducibile.
Sia $\alpha \in \mathbf{F} := \mathbf{F}_5[x]/\langle g(x) \rangle$ una sua radice. Siano

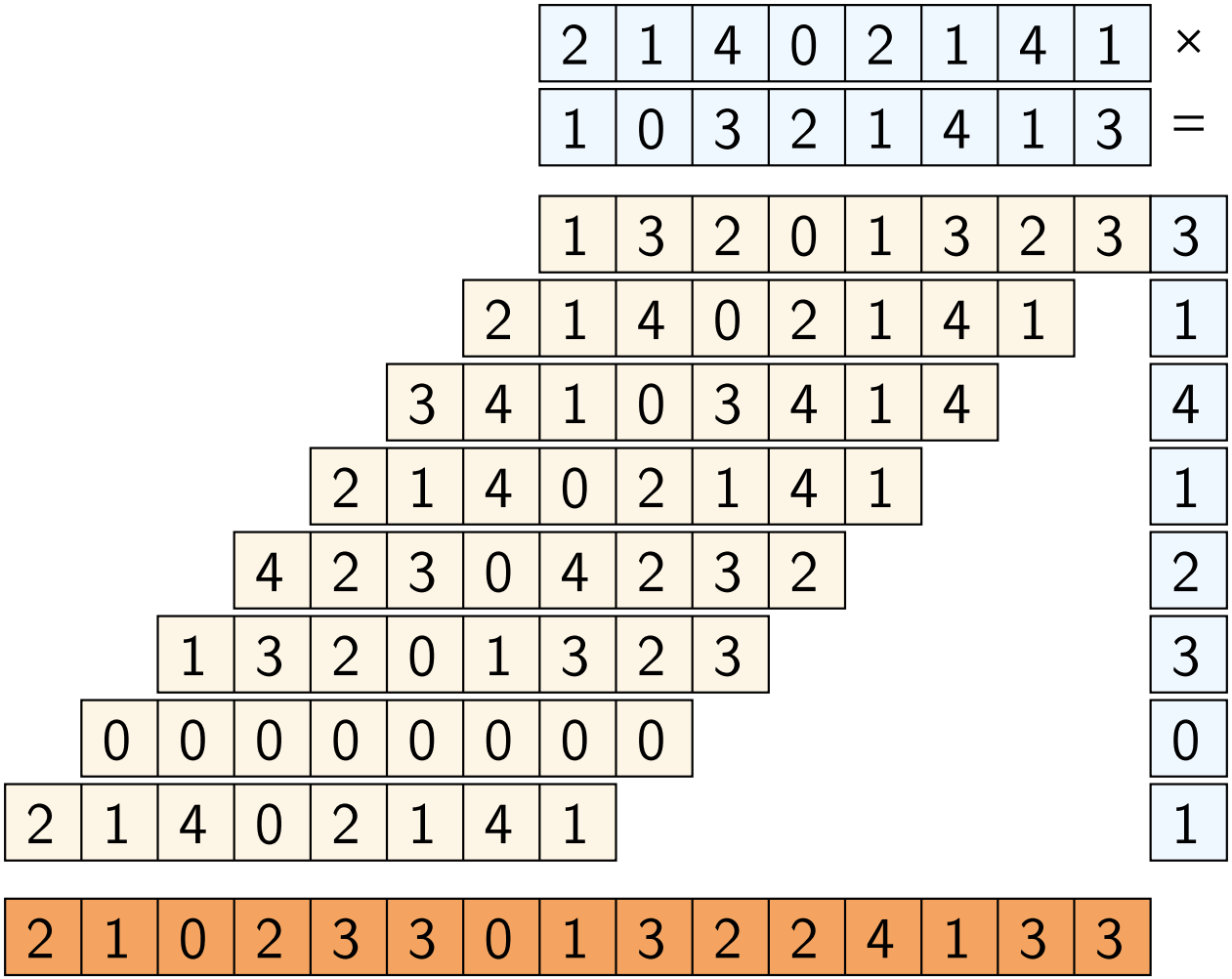
$$\nu = 2\alpha^7 + \alpha^6 + 4\alpha^5 + 2\alpha^3 + \alpha^2 + 4\alpha + 1$$
$$\mu = \alpha^7 + 3\alpha^5 + 2\alpha^4 + \alpha^3 + 4\alpha^2 + \alpha + 3$$

Cioè

$$f(x) = 2x^7 + x^6 + 4x^5 + 2x^3 + x^2 + 4x + 1$$
$$h(x) = x^7 + 3x^5 + 2x^4 + x^3 + 4x^2 + x + 3$$


2 1 4 0 2 1 4 1 ×
1 0 3 2 1 4 1 3 =
1 3 2 0 1 3 2 3
2 1 4 0 2 1 4 1
3 4 1 0 3 4 1 4
2 1 4 0 2 1 4 1
4 2 3 0 4 2 3 2
1 3 2 0 1 3 2 3
0 0 0 0 0 0 0 0
2 1 4 0 2 1 4 1


2 1 4 0 2 1 4 1 ×
1 0 3 2 1 4 1 3 =
1 3 2 0 1 3 2 3 3
2 1 4 0 2 1 4 1 1
3 4 1 0 3 4 1 4 4
2 1 4 0 2 1 4 1 1
4 2 3 0 4 2 3 2 2
1 3 2 0 1 3 2 3 3
0 0 0 0 0 0 0 0 0
2 1 4 0 2 1 4 1 1


2 1 4 0 2 1 4 1 ×
1 0 3 2 1 4 1 3 =
1 3 2 0 1 3 2 3 3
2 1 4 0 2 1 4 1 1
3 4 1 0 3 4 1 4 4
2 1 4 0 2 1 4 1 1
4 2 3 0 4 2 3 2 2
1 3 2 0 1 3 2 3 3
0 0 0 0 0 0 0 0 0
2 1 4 0 2 1 4 1 1
2 1 0 2 3 3 0 1 3 2 2 4 1 3 3

Un esempio

Sia $g(x) = x^8 + x^4 + 2 \in \mathbf{F}_5[x]$: è irriducibile.
Sia $\alpha \in \mathbf{F} := \mathbf{F}_5[x]/\langle g(x)\rangle$ una sua radice. Siano

$$\nu = 2\alpha^7 + \alpha^6 + 4\alpha^5 + 2\alpha^3 + \alpha^2 + 4\alpha + 1$$
$$\mu = \alpha^7 + 3\alpha^5 + 2\alpha^4 + \alpha^3 + 4\alpha^2 + \alpha + 3$$

Cioè

$$f(x) = 2x^7 + x^6 + 4x^5 + 2x^3 + x^2 + 4x + 1$$
$$h(x) = x^7 + 3x^5 + 2x^4 + x^3 + 4x^2 + x + 3$$

Quindi $f(x)h(x)$ vale

$$2x^{14} + x^{13} + 2x^{11} + 3x^{10} + 3x^9 + x^7 + 3x^6 + 2x^5 + 2x^4 + 4x^3 + x^2 + 3x + 3$$
$$\equiv 4x^7 + 3x^6 + 3x^5 + 2x^4 + 4x^2 + 4x + 3 \bmod g(x)$$
$$\nu\mu = 4\alpha^7 + 3\alpha^6 + 3\alpha^5 + 2\alpha^4 + 4\alpha^2 + 4\alpha + 3$$

Riassumendo

Il prodotto di due elementi qualsiasi in $\mathbf{F}_{p^s}$ richiede:

- il prodotto di due polinomi in $\mathbf{F}_p[x]$ di grado $s-1$;
- una riduzione di un polinomio di grado $2s-2$ modulo un polinomio di grado s.

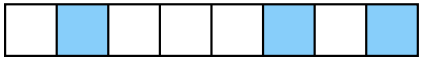
Poiché $x^n = 1$ in un gruppo di ordine n, l'inversione di un elemento di $\mathbf{F}_{p^s}$ richiede al peggio di calcolarne la potenza $p^s - 2$, il che richiede $O(s)$ moltiplicazioni.

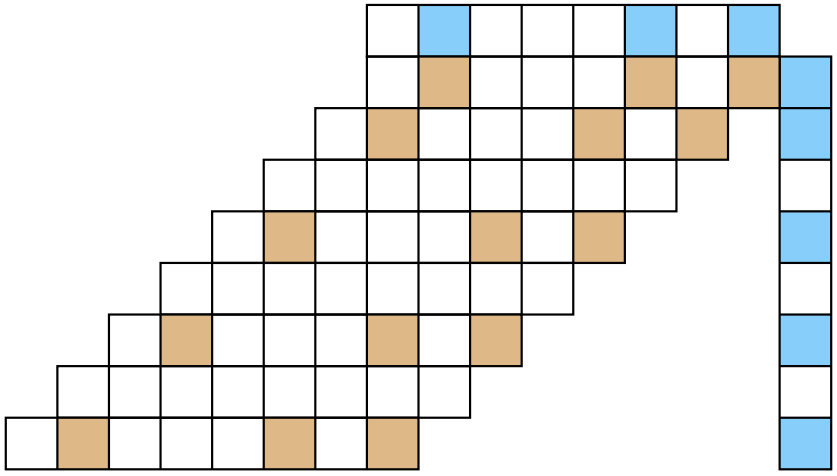
Problema chiave

Velocizzare la moltiplicazione di due polinomi di grado fissato

In caratteristica 2

$$f(x) = x^6 + x^2 + 1,\ h(x) = x^7 + x^5 + x^3 + x + 1: \quad f(x)h(x)?$$

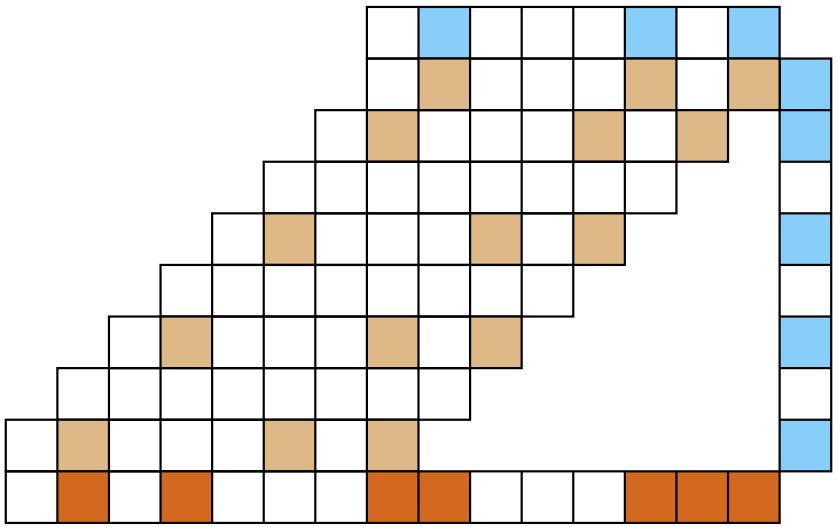
$f(x) =$  , $h(x) =$ 



In caratteristica 2

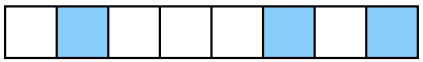
$$f(x) = x^6 + x^2 + 1,\ h(x) = x^7 + x^5 + x^3 + x + 1: \quad f(x)h(x)?$$

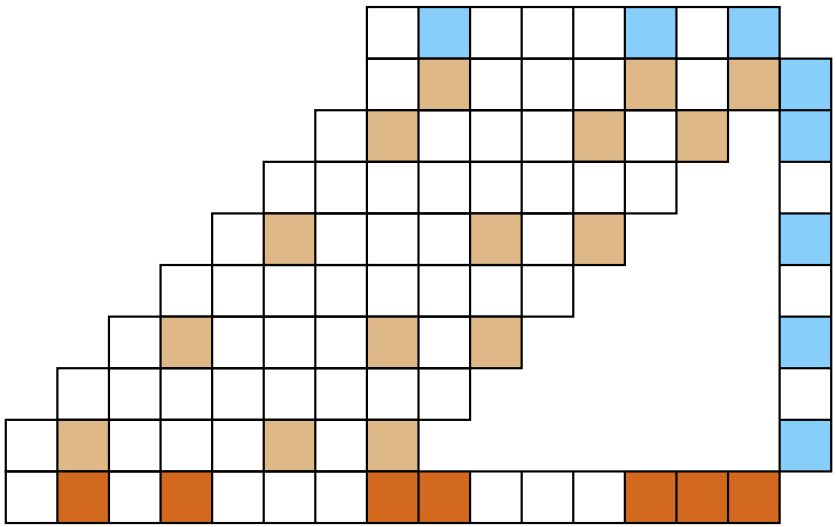
$$f(x) = \square\square\square\square\square\square\square\square,\ h(x) = \square\square\square\square\square\square\square\square$$



In caratteristica 2

$$f(x) = x^6 + x^2 + 1,\ h(x) = x^7 + x^5 + x^3 + x + 1: \quad f(x)h(x)?$$

$f(x) =$  , $h(x) =$ 

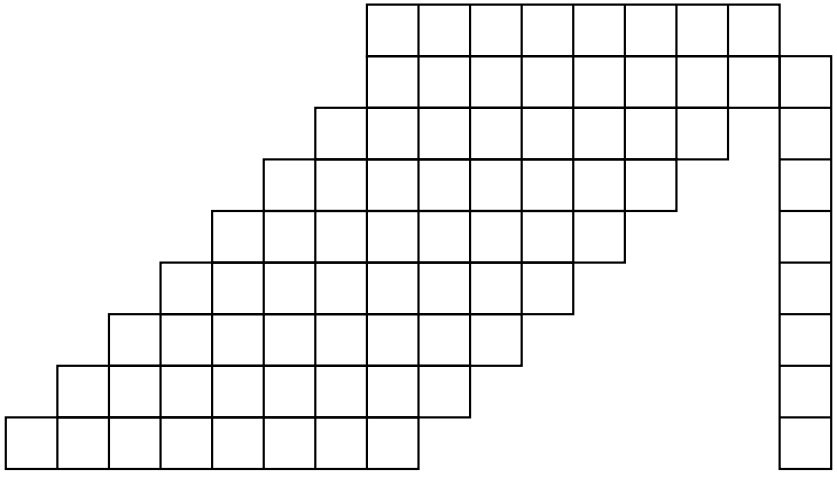


Quindi $f(x)h(x) = x^{13} + x^{11} + x^7 + x^6 + x^2 + x + 1$.

Un esercizio

Vogliamo calcolare il seguente prodotto in $\mathbf{F}_2[x]$:

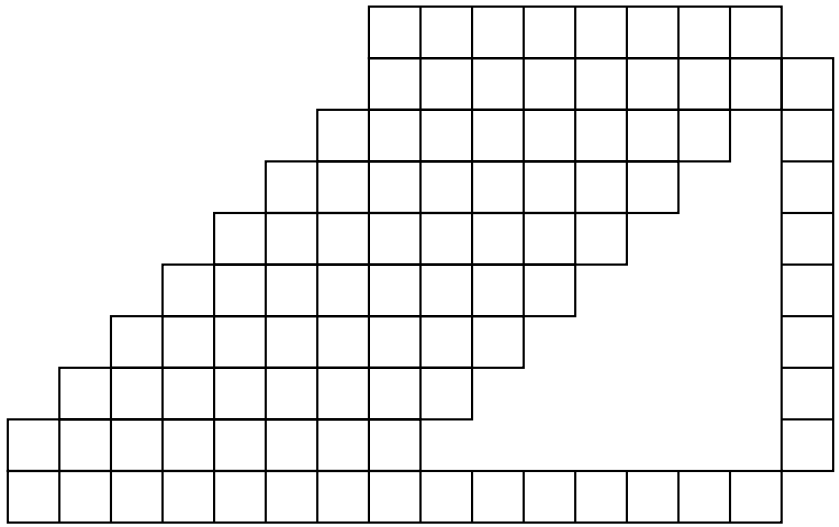
$$(x^7+x^5+x^4+x^2+1)(x^7+x^6+x^4+x^3+1)$$



Un esercizio

Vogliamo calcolare il seguente prodotto in $\mathbf{F}_2[x]$:

$$(x^7 + x^5 + x^4 + x^2 + 1)(x^7 + x^6 + x^4 + x^3 + 1)$$



Complessità

Indichiamo con $M_2(s)$ il costo del prodotto di due polinomi di grado $s-1$ su $\mathbf{F}_2$. Trascurando gli *shift*, sono necessarie

$$1+2+\cdots+(s-1)+s+(s-1)+\cdots+2+1 = s+2\sum_{i=1}^{s-1} i = s^2$$

somme di bit.

Fatto

$M_2(s) \leq s^2$

Algoritmo di Karatsuba

Notiamo, in particolare, che se M_{AS} indica il costo dell'algoritmo scolastico: $M_{\mathrm{AS}}(2s) = 4M_{\mathrm{AS}}(s)$. Possiamo fare di meglio!

Fatto (Anatolij Alekseevič Karacuba, 1960)

$M(2s) \simeq 3M(s)$. *Infatti*

$$(at+b)(ct+d) = act^2 + \big((a+b)(c+d) - ac - bd\big)t + bd$$

dove scriviamo

$$\begin{aligned} f(x) &= \left(a_{2s-1}x^{2s-1} + \cdots + a_s x^s\right) + \left(a_{s-1}x^{s-1} + \cdots + a_0\right) \\ &= \left(a_{2s-1}x^{s-1} + \cdots + a_s\right)x^s + \left(a_{s-1}x^{s-1} + \cdots + a_0\right) \\ a(x) &= a_{2s-1}x^{s-1} + \cdots + a_s, \quad b(x) = a_{s-1}x^{s-1} + \cdots + a_0, \quad t = x^s \end{aligned}$$

Un esempio

Calcoliamo $75 \cdot 49$ usando Karatsuba

Un esempio

Calcoliamo $75 \cdot 49$ usando Karatsuba

$$(at+b)(ct+d) = act^2 + \big((a+b)(c+d) - ac - bd\big)t + bd$$

Un esempio

Calcoliamo $75 \cdot 49$ usando Karatsuba

$$(7 \cdot 10 + 5)(4 \cdot 10 + 9) = 7 \cdot 4 \cdot 10^2 + \big((7 + 5)(4 + 9) - 7 \cdot 4 - 5 \cdot 9\big)10 + 5 \cdot 9$$

Un esempio

Calcoliamo $75 \cdot 49$ usando Karatsuba

$$(7 \cdot 10 + 5)(4 \cdot 10 + 9) = 7 \cdot 4 \cdot 10^2 + \big((7+5)(4+9) - 7 \cdot 4 - 5 \cdot 9\big)10 + 5 \cdot 9$$

cioè

$$ac = 7 \cdot 4$$

$$bd = 5 \cdot 9$$

$$(a+b)(c+d) = (7+5)(4+9)$$

Un esempio

Calcoliamo $75 \cdot 49$ usando Karatsuba

$$(7 \cdot 10 + 5)(4 \cdot 10 + 9) = 7 \cdot 4 \cdot 10^2 + \big((7+5)(4+9) - 7 \cdot 4 - 5 \cdot 9\big)10 + 5 \cdot 9$$

cioè

$$ac = 7 \cdot 4 = 28$$

$$bd = 5 \cdot 9 = 45$$

$$(a+b)(c+d) = (7+5)(4+9) = 12 \cdot 13 = 156$$

Un esempio

Calcoliamo $75 \cdot 49$ usando Karatsuba

$$(7 \cdot 10 + 5)(4 \cdot 10 + 9) = 7 \cdot 4 \cdot 10^2 + \big((7+5)(4+9) - 7 \cdot 4 - 5 \cdot 9\big)10 + 5 \cdot 9$$

cioè

$$ac = 7 \cdot 4 = 28$$

$$bd = 5 \cdot 9 = 45$$

$$(a+b)(c+d) = (7+5)(4+9) = 12 \cdot 13 = 156$$

$$75 \cdot 49 = 28\,00 + (156 - 28 - 45)0 + 45 = 3675$$

Complessità

Da $M(2s) \simeq 3M(s)$ ricaviamo, supponendo $s = 2^k$:

$$M(2^k) = 3M(2^{k-1}) = 3^2 M(2^{k-2}) = \cdots = 3^k M(1)$$

Quindi

$$M(s) \simeq s^{\ln_2 3}$$

Complessità in operazioni su bit

Dati due polinomi $f(x),\ h(x) \in \mathbf{F}_2[x]$ di grado $2s-1$: scriviamo

$$f = f_1 x^s + f_0, \quad h = h_1 x^s + h_0$$
$$fh = (f_1 x^s + f_0)(h_1 x^s + h_0)$$
$$= (f_1 h_1)(x^{2s} + x^s) + (f_1 + f_0)(h_1 + h_0)x^s + (f_0 h_0)(x^s + 1)$$

Costo in operazioni su bit

- $2s$: somme $\sigma_0 = f_1 + f_0,\ \sigma_1 = h_1 + h_0$
- $3M_2(s)$: prodotti $\pi_0 = f_1 h_1,\ \pi_1 = (f_1 + f_0)(h_1 + h_0),\ \pi_2 = (f_0 h_0)$
- $2(s-1)$: somme $\Pi_0 = \pi_0(x^{2s} + x^s),\ \Pi_2 = \pi_2(x^s + 1)$
- $2s-1$: somma $\Sigma_0 = \Pi_0 + \pi_1 x^s$
- $2s-1$: somma $\Sigma_0 + \Pi_2$

Per un totale di: $M_2(2s) = 3M_2(s) + 8s - 4$.

Da dove salta fuori Karatsuba?

Sia $P(t)$ un polinomio di grado due: se conosco il suo valore in tre punti lo posso determinare!

Interpolazione di Lagrange

Siano dati tre punti distinti $t_0, t_1, t_2 \in \mathbf{F}$. Sia $L_i(t) = \prod_{j \neq i} \frac{t - t_j}{t_i - t_j}$, $i = 0, 1, 2$.

Allora $P(t) = \sum L_i(t) P(t_i)$.

Da dove salta fuori Karatsuba?

Sia $P(t)$ un polinomio di grado due: se conosco il suo valore in tre punti lo posso determinare!

Interpolazione di Lagrange

Siano dati tre punti distinti $t_0, t_1, t_2 \in \mathbf{F}$. Sia $L_i(t) = \prod_{j \neq i} \frac{t - t_j}{t_i - t_j}$, $i = 0, 1, 2$.

Allora $P(t) = \sum L_i(t) P(t_i)$.

Ci basta infatti notare che $L_i(t_i) = 1$ mentre $L_i(t_j) = 0$ se $j \neq i$ e che il polinomio $P(t) - \sum L_i(t) P(t_i)$ ha grado due e tre radici distinte.

Da dove salta fuori Karatsuba?

Sia $P(t)$ un polinomio di grado due: se conosco il suo valore in tre punti lo posso determinare!

Interpolazione di Lagrange

Siano dati tre punti distinti $t_0, t_1, t_2 \in \mathbf{F}$. Sia $L_i(t) = \prod_{j \neq i} \frac{t - t_j}{t_i - t_j}$, $i = 0, 1, 2$.

Allora $P(t) = \sum L_i(t) P(t_i)$.

Ci basta infatti notare che $L_i(t_i) = 1$ mentre $L_i(t_j) = 0$ se $j \neq i$ e che il polinomio $P(t) - \sum L_i(t) P(t_i)$ ha grado due e tre radici distinte.
Quali tre punti possiamo scegliere?

Interpolazione proiettiva

Problema

Non ci sono tre punti in $\mathbf{F}_2$*!*

Interpolazione proiettiva

Problema

Non ci sono tre punti in $\mathbf{F}_2$*!*

La retta proiettiva

- Retta affine: $\mathbf{F}_2 = \{0, 1\}$
- Retta proiettiva: $\mathbf{P}^1(\mathbf{F}_2) = \{0, 1, \infty\}$

Sia $P(t) = (at + b)(ct + d)$. Allora

- $P(0) = bd$
- $P(1) = (a + b)(c + d)$
- $\left.\frac{P(t)}{t^2}\right|_{t=\infty} = ac$

Karatsuba raffinato

Bernstein, 2009

Siano $f(x), h(x) \in \mathbf{F}_2[x]$ di grado $s+k-1$ con $s/2 \leq k/2 \leq s$. Scriviamo

$$f = f_1 x^s + f_0, \quad h = h_1 x^s + h_0$$
$$fh = (f_1 h_1 x^s + f_0 h_0)(x^s + 1) + (f_1 + f_0)(h_1 + h_0) x^s$$

Quindi il costo in operazioni su bit è

$$M_2(s+k) \leq 2M_2(s) + M_2(k) + 4k + 3s - 3$$

Two-level Seven-way Recursion

Bernstein, 2009

Siano $f(x), h(x) \in \mathbf{F}_2[x]$ di grado $3s+k-1$ con $s/2 \le k/2 \le s$. Scriviamo

$$f = f_3 x^{3s} + f_2 x^{2s} + f_1 x^s + f_0, \quad h = h_3 x^{3s} + h_2 x^{2s} + h_1 x^s + h_0$$

$$\Sigma = f_3 h_3 x^{3s} + f_2 h2 x^{2s} + f_1 h_1 x^s + f_0 h_0$$

$$\Pi = (f_3 + f_2)(h_3 + h_2) x^{3s} + (f_1 + f_0)(h_1 + h_0) x^s$$

$$\Psi = \big((f_3 + f_1) x^s + f_2 + f_0\big)\big((h_3 + h_1) x^s + h_2 + h_0\big)$$

$$fh = (\Sigma + \Pi)(x^{2s} + 1) + \Psi x^{2s}$$

Quindi il costo in operazioni su bit è

$$M_2(3s+k) \le M(2s) + 5M(s) + M(k) + 19n + 8k - 8$$

CNH Three-Way Split Algorithm

Cenk, Negre, Hassan, 2011

Idea: Karatsuba per $(at^2+bt+c)(dt^2+et+f)$ interpolando su 5 punti.
Dove li trovo? $\mathbf{P}^1(\mathbf{F}_4) = \{0, 1, \alpha, \alpha+1, \infty\}$ dove α è una radice di x^2+x+1.
Il costo in operazioni su bit è

$$\begin{cases} M_2(3s) \leq 3M_2(s) + M_4(s) + 20s - 5 \\ M_4(3s) \leq 5M_4(s) + 56s - 19 \end{cases}$$

Karatsuba al prossimo livello

De Piccoli, Visconti, R, 2019

Aumentiamo il livello di Karatsuba: polinomi di grado $8-1$, $16-1$, $32-1$: migliora il limite nel caso ottimale, ma...

Karatsuba al prossimo livello

De Piccoli, Visconti, R, 2019

Aumentiamo il livello di Karatsuba: polinomi di grado $8-1$, $16-1$, $32-1$: migliora il limite nel caso ottimale, ma...

Algoritmo	Miglior caso	Grado
B's refined Karatsuba	$M(s) \leq 6.50 s^{\log_2 3} - 7{,}00 s + 1{,}50$	$s = 2^k$
B's 2-level 7-way	$M(s) \leq 6.43 s^{\log_2 3} - 6{,}80 s + 1{,}38$	$s = 4^k$
DVR's 3-level recursion	$M(s) \leq 6.34 s^{\log_2 3} - 6{,}68 s + 1{,}35$	$s = 8^k$
DVR's 4-level	$M(s) \leq 6.30 s^{\log_2 3} - 6{,}62 s + 1{,}31$	$s = 16^k$
DVR's 5-level	$M(s) \leq 6.28 s^{\log_2 3} - 6{,}57 s + 1{,}30$	$s = 32^k$

dove $\log_2 3 = 1{,}58$

Alcuni nuovi record

s	Prima	Nostro	Δ Gates	Depth (da)	Depth (a)	Algorithm
24	702	697	5	10	9	3-lev
32	1156	1148	8	11	10	3-lev
40	1703	1700	3	14	13	3-lev
47	2228	2214	14	13	11	4-lev
48	2259	2238	21	13	11	4-lev
63	3626	3612	14	14	12	4-lev
64	3673	3640	23	13	12	4-lev
72	4510	4510	0	25	15	3-lev
79	5329	5313	16	16	15	4-lev
80	5366	5345	21	16	15	4-lev
95	7073	6978	95	15	13	5-lev
96	7110	7006	104	16	13	5-lev
120	10438	10294	144	130	17	3-lev
127	11447	11277	170	17	14	5-lev
128	11466	11309	157	16	14	5-lev

n-Way Split Algorithm

De Piccoli, Visconti, Rizzo, 2019

- $\mathbf{P}^1(\mathbf{F}_{2^d})$ ha 2^d+1 elementi
- Possiamo interpolare polinomio di grado 2^d
- Formula di stile Karatsuba per polinomi di grado 2^{d-1}.

Se $f(x)=\sum_{i=0}^{2^d} f_i x^i$, e se α è un elemento primitivo di $\mathbf{F}_{2^d}$:

$$f(x) = \big(f(\infty)x + f(0)\big)(x^{2^d-1}+1) + \sum_{i=0}^{2^d-2} f(\alpha^i)\frac{x^{2^d}+x}{x+\alpha^i}$$

$$= \big(f(\infty)x + f(0)\big)(x^{2^d-1}+1) + \sum_{j=0}^{2^d-1}\left(\sum_{i=0}^{2^d-2}\alpha^{i(j-1)} f(\alpha^i)\right)x^{2^d-j}$$

Complessità

Fissato d, sia

$$P = -1 + \frac{1}{d}\sum_{k=0}^{d-1} \mathrm{MCD}(2^k - 1, 2^d - 1)$$

In particolare, se $2^d - 1$ è primo, $P = (2^d - 2)/d$. Allora il valore asintotico di $M_2(s)$ è $O(s^\epsilon)$ dove

$$\epsilon = \log_{2^d+1}\left(3 + \frac{(d^2+d)P}{2}\right)$$

$$\log_{2^{d-1}+1}$$