Campi finiti

Titolo nota 05/09/2013

K campo $(K, 0, 1, +, \cdot)$

$\mathbb{Z}/p\mathbb{Z} \dots \mathbb{F}_p$ $\qquad$ $\mathbb{R}[x]/I$ $\quad I = (p(x))$

$\parallel$

"polinomi" modulo $p(x)$".

$\mathbb{R} \longrightarrow \mathbb{F}_p$ $\qquad$ $\mathbb{F}_p[x]/(a(x))$ $\qquad$ $(a(x)) = \{ \text{multipli di } a(x) \}$

$a(x)$ non irriducibile $\longrightarrow$ $\dfrac{\mathbb{F}_p[x]}{(a(x))}$ non è dominio d'integrità.

$a(x)$ irriducibile è campo?

$\exists$ inverso di $b(x)$? Sì per Bézout.

$\Longrightarrow$ quanti elementi ha $\dfrac{\mathbb{F}_p[x]}{(a(x))}$?

$0, 1, \dots, p-1$

$x \; 2x \dots (p-1)x$

$x^2 \; \dots$

$\vdots \; \deg(a(x))-1 \; \dots$

+ tutte le somme = $\{$pol. di grado $< \deg(a(x)) = n\}$

$\Rightarrow$ p^n elementi.

Se esiste un pol. irriducibile di grado n in $\mathbb{F}_p[x]$, esiste un campo con p^n elementi.

$\mathbb{F}_4$ $\qquad$ x^2+x+1 è irriducibile

$$\mathbb{F}_2[x]/(x^2+x+1) \longrightarrow \{0, 1, x, x+1\} \doteq \mathbb{F}_4$$

$+, \cdot, \dots$

$x(x+1) = x^2+x = 1$

$\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ $\qquad$ $\alpha^2+\alpha+1=0$

$\mathbb{F}_{p^2}$ $\quad x^2+ax+b$ irriducibile

x^2+b $\quad -b$ non residuo quadratico

$\left(0 \quad x \to y+1 \quad y^2+2y+b+1\right)$

$\mathbb{F}_p(\alpha) \quad \alpha^2=-b \quad mx+n$

$(mx+n,\ x^2+b)=1 \Rightarrow$

$l(x)(mx+n)+h(x)(x^2+b)=1$

in $\mathbb{F}_p(\alpha)$, $l(\alpha)$ è inverso di $mx+n$.

$\mathbb{F}_{24} = \mathbb{F}_{16}$ $\qquad$ x^4+x+1 è irr. $\begin{cases} \text{non ha radici in } \mathbb{F}_2 \\ (x^2+x+1)^2 = x^4+x^2+1 \end{cases}$

$$\frac{\mathbb{F}_2[x]}{(x^4+x+1)} \to \mathbb{F}_2(\alpha) \quad \alpha^4 = \alpha+1$$

$\#\mathbb{F}_{x^4+x+1}$

$$0 \quad 1 \quad \alpha \quad \alpha+1$$
$$\alpha^2 \quad \alpha^2+1 \quad \alpha^2+\alpha \quad \alpha^2+\alpha+1$$
$$\alpha^3 \quad \alpha^3+1 \quad \alpha^3+\alpha \quad \alpha^3+\alpha+1$$
$$\alpha^3+\alpha^2 \quad \alpha^3+\alpha^2+1 \quad \alpha^3+\alpha^2+\alpha \quad \alpha^3+\alpha^2+\alpha+1$$

$\left\{ l_1\alpha^3 + l_2\alpha^2 + l_3\alpha + l_4 \;\middle|\; l_i \in \mathbb{F}_2 \right\} =$ sp. vett. su $\mathbb{F}_2$ di dim. 4.

Il prodotto non è quello di $\mathbb{Z}/16\mathbb{Z}$!
(neanche la somma)

Tutti gli $\alpha \in \mathbb{F}_{16}$ sono t.c. $\alpha + \alpha = 0$

invece in $\mathbb{Z}/16\mathbb{Z}$ bisogna arrivare a 16

Invece gli $a \in \mathbb{Z}/16\mathbb{Z}$ dispari sono t.c. $a^4 \equiv 1$

invece in $\mathbb{F}_{16}$ $\alpha^4 = \alpha + 1 \neq 1$

$\alpha^5 \to \alpha \cdot \alpha^4 = \alpha \cdot (\alpha+1) = \alpha^2 + \alpha$

$$(\alpha^2+\alpha+1)(\alpha^3+\alpha^2) = \alpha^2 + \alpha + \alpha + 1 + \alpha^3 + \alpha + 1 + \alpha^3 + \alpha^2 =$$

$$= \alpha.$$

$\mathbb{F}_8$ $\quad x^3+x+1$ è irr. (non ha radici)

$\longrightarrow \mathbb{F}_2(\alpha) \quad \alpha^3+\alpha+1=0$

Si può fare un campo con un numero di elementi $\neq p^k$?

Caratteristica di un campo: $0 \neq x \in K$

se $x+x+x-\dots = n\cdot x$ non fa mai $0 \rightarrow$ $\operatorname{char} K = 0$

se $x+x+\dots+x = n\cdot x = 0$ $\operatorname{char} K =$
$= \min\{n \mid n\cdot x = 0\} \in \mathbb{N}$

Se $y \neq x$ $\quad y \neq 0$, $\quad y + y - - - + y = n \cdot y =$

$$= \left(\frac{y}{x}\right)(x + x - - - + x)$$

quindi o tutti sono t.c. $\underbrace{x + x - - - + x}_{n \cdot x} = 0$
o nessuno

Se il campo è finito, $\operatorname{char} K \neq 0$.

Ma $\operatorname{char} K$ è un numero primo:

$$h = p \cdot q \qquad h \cdot x = 0 \qquad p \cdot q - x = 0 =$$

$$= \underbrace{(1 + 1 - - - + 1)}_{p \text{ volte}} \cdot (q x) \quad \begin{cases} p \neq 0 & \exists \frac{1}{p} \Rightarrow \underline{q x = 0} \quad 0 < q < n \\ & \qquad\qquad \text{ass.} \\ p = 0 & \text{ass.} \end{cases}$$

Ma allora $K \supset \mathbb{F}_p = (0, 1, \dots, p-1)$

Ma se $K \supset L$ K è sp. vett. su $L \Rightarrow$ ha p^n el.

$\mathbb{F}_{27}$?

Oss. in $\mathbb{F}_p$ o $\mathbb{F}_{p^k}$ o char $K = p$

$$(a+b)^p = a^p + b^p$$

$\mathbb{F}_p$

$$Q(x) = x^{p^k} - x = x \cdot (x^{p^k - 1} - 1)$$

$$Q(x) = \prod_{i=1}^{N} q_i(x) \qquad q_i \text{ irr.}$$

Posso costruire $\dfrac{\mathbb{F}_p[x]}{(q_i(x))} \longrightarrow \mathbb{F}_p(\alpha)$ dove $q_i(\alpha)$ ha una radice.

in $\mathbb{F}_p(\alpha)[x]$, $Q(x) = \prod q_i^{\alpha}(x)$ $\qquad q_i^{\alpha}$ irr.

$\longrightarrow \dfrac{\mathbb{F}_p(\alpha)[x]}{(q_i^{\alpha}(x))} \longrightarrow \mathbb{F}_p(\alpha)(\beta) \longrightarrow$

$\longrightarrow \quad - \quad - \quad - \quad \mathbb{F}_p(\alpha)(\beta)\ldots\ldots(\omega)$ in cui

$\mathbb{Q}(\kappa)$ si spezza in fattori di grado 1

$$K \subset \mathbb{F}_p(\alpha)(\beta)(\gamma)\dots(\omega)$$

$$K = \{\lambda \in \mathbb{F}_p(\alpha)(\beta)(\gamma)\dots(\omega) \mid \lambda^{p^k} = \lambda\}$$

Oss. K è un campo!

$$(\lambda_1 + \lambda_2)^{p^k} = \lambda_1^{p^k} + \lambda_2^{p^k} = \lambda_1 + \lambda_2$$

$$(\lambda_1 \lambda_2)^{p^k} = \lambda_1^{p^k} \lambda_2^{p^k}$$

$$\lambda_1^{p^k} = 1 \qquad \left(\frac{1}{\lambda_1}\right)^{p^k} = \frac{1}{\lambda_1^{p^k}} = 1$$

Quanti el. ha K? Sono le radici di

$x^{p^k} - x$ in $\mathbb{F}_p(\alpha)(\beta)\ldots(\omega)$.

$\left(x^{p^k} - x\right)' = -1 \Rightarrow$ le radici sono distinte

e in $\mathbb{F}_p(\alpha)\ldots(\omega)$ c'erano tutte $\Rightarrow p^k$.

$\Rightarrow |K| = p^k$. e K è il <u>campo di spezzamento</u> di $\mathbb{Q}(x)$,

cioè il più piccolo campo $(\supset \mathbb{F}_p)$ dove $\mathbb{Q}(x)$ si spezza in fattori di grado 1.

THIS IS
THE END

grado di L su K $\doteq$ dim di L su K come sp. vett.

$[L:K]$

$\alpha^4 = \alpha + 1$

$\alpha^2+\alpha \in \mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ $\quad (\alpha^2+\alpha)^2 + (\alpha^2+\alpha) + 1 =$

$\cup$

$\mathbb{F}_4 = \mathbb{F}_2(\alpha^2+\alpha)$ $= \alpha^4 + \alpha^2 + \alpha^2 + \alpha + 1 =$

$= \alpha + 1 + \alpha^2 + \alpha^2 + \alpha + 1 = 0$!

(anche $\alpha^2+\alpha+1$ va bene)

$[\mathbb{F}_{16} : \mathbb{F}_2] = 4$ $\quad [\mathbb{F}_4 : \mathbb{F}_2] = 2$ $\quad [\mathbb{F}_{16} : \mathbb{F}_4] = ?$ ②

$K < L < E$

$$[E:K] = [E:L][L:K].$$

$$\mathbb{F}_{16} = \mathbb{F}_2(\alpha) = \mathbb{F}_4(\beta)$$

$\mathbb{F}_2(\gamma) \overset{\mathbb{F}_4}{=}$ $\gamma^2+\gamma+1=0$

$\hookrightarrow \mathbb{F}_{16}$ $\gamma \longrightarrow \alpha^2+\alpha$

in $\mathbb{F}_{16}$ $\alpha^2+\alpha=\gamma$

$\mathbb{F}_2(\gamma)[x]$

$\mathbb{F}_4[x]$ $x^2+x-\gamma$

è irr.!

$K < K(\alpha)$ $\quad [K(\alpha):K]$ è il grado del minimo polinomio soddisfatto da α.

$1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{k-1}$ sono indip.:

se $\alpha^k = \lambda_{k-1}\alpha^{k-1} + \cdots + \lambda_1\alpha + \lambda_0$

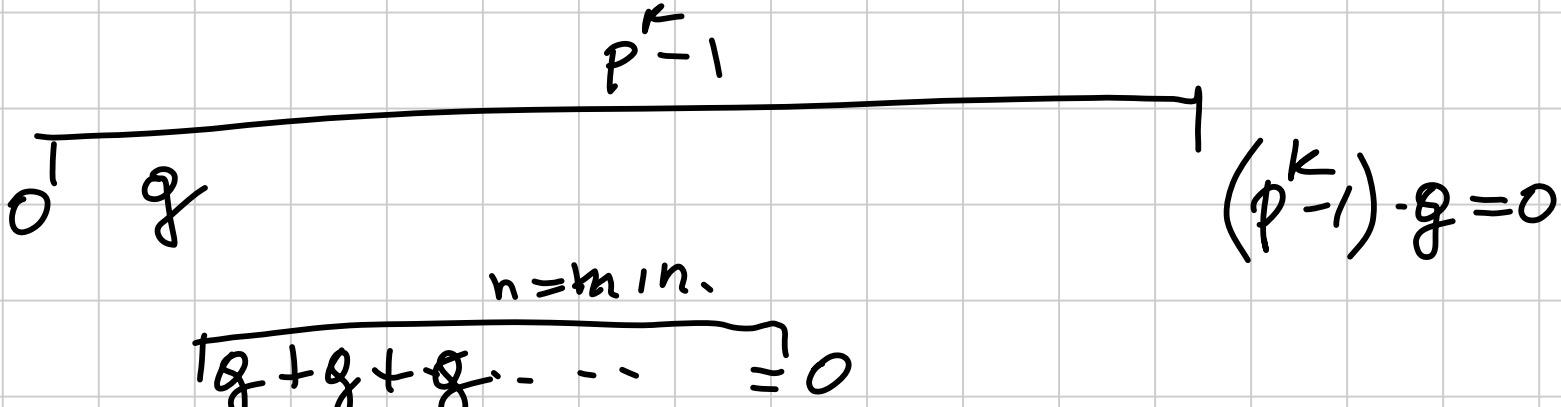
$\Rightarrow x^k - \lambda_{k-1}x^{k-1} - \cdots - \lambda_1 x - \lambda_0$ è il polinomio minimo di α su K

$x^4 + x + 1 = (x^2 + x - \gamma)(\cdots)$ in $\mathbb{F}_4[x]$

$|K| = p^k$ el., $K^* = K \setminus \{0\}$ è un gruppo molt.

di ordine $p^k - 1$. $\quad a^{p^k-1} = 1 \quad \forall a \in K$.

$\Rightarrow$ gli el. soddisfano $x^{p^k} = x$.



posso dividere i $p^k - 1$ el. in classi di equiv.

rispetto al multipli di $g \Rightarrow n \mid p^k - 1 \Rightarrow$

$\subseteq (p^k - 1) \cdot g = 0,$

$\Longrightarrow K =$ c. spezz. di $x^{p^k} - x.$

Di più: $\mathbb{F}_{p^k}^*$ è ciclico.

Dim. ha $p^k - 1$ elem. $\quad p^k - 1 = q_1^{\alpha_1} \cdot \ldots \cdot q_h^{\alpha_h}$

$x^{\frac{p^k-1}{q_i}} - 1$ ha al più $\frac{p^k-1}{q_i}$ radici in $\mathbb{F}_{p^k}^*$

$\Rightarrow \exists\, b_i$ non radice di

$\tilde{b}_i = b_i^{\frac{p^k-1}{q_i^{\alpha_i}-1}} \qquad \tilde{b}_1 \cdot \tilde{b}_2 \cdot \ldots \cdot \tilde{b}_h = g$

Dico che g è un generatore.

$g^{p^k-1}=1$ se $g^h=1$ h $h_{min.}$ $h<p^k-1 \Rightarrow h \mid p^k-1$

$\Rightarrow h \mid \frac{p^k-1}{q_i}$ per un certo i Ma allora

$b_j^{\frac{p^k-1}{q_i}}=1 \quad j \neq i$

$g^{\frac{p^k-1}{q_i}} = 1 \cdot b_i^{\frac{p^k-1}{q_i}} \cdot 1 \cdot 1 \cdots = b_i^{\frac{p^k-1}{q_i}} \neq 1$

□

$\mathbb{F}_{p^n}^* = \langle g \rangle$ <u>non è detto che $\#_{p^n} = \#_p(a)$, $g=a$</u>

$\mathbb{F}_9 \qquad x^2+1 \qquad \mathbb{F}_3(\alpha) \qquad \alpha^2+1=0 \qquad \mathbb{F}_9^* = \mathbb{Z}/8\mathbb{Z}$

$\#\mathbb{F}_9$

ma $\alpha^4 = (\alpha^2)^2 = (-1)^2 = 1$

$$Q(x) = x^{p^k} - x = \prod \{ q_i(x) \text{ (monici) irriducibili di grado } d \mid k \text{, tutti} \}$$

se $q_i(x)$ irr. $q_i(x) \mid Q(x)$ il campo di spezz. di $\prod_i q_i(x)$ è $\mathbb{F}_{p^k}$

$$[\mathbb{F}_{p^k} : L_i][L_i : \mathbb{F}_p] = k$$

ma $\deg q_i$ divide $[L_i : \mathbb{F}_p]$:

se α radice di q_i, $L_i \supset \mathbb{F}_p(\alpha) \supset \mathbb{F}_p$

$\deg q_i$

$\Rightarrow \deg q_i \mid k$.

$q_i(x)$ compaiono una volta sola perché

$\mathbb{Q}(x)$ non ha radici multiple.

α radice di $q(x)$ irriducibile su $\mathbb{F}_p$.

$$q(x) = \sum_{i=0}^{d} \lambda_i x^i \qquad \mathbb{F}_p(\alpha)$$

$$\sum \lambda_i \alpha^i = 0$$

$$\alpha \longmapsto \alpha^p$$

$$\sum \lambda_i (\alpha^p)^i = \sum \lambda_i (\alpha^i)^p = \sum^p \lambda_i (\alpha^i)^p =$$

$$= \left(\sum \lambda_i \alpha^i\right)^p = 0 \Rightarrow \alpha^p \text{ è ancora radice!}$$

Ma $\alpha^p = \alpha$? no se no sarebbe radice di $x^p - x$ che ha già p radici in $\mathbb{F}_p$

$\alpha \quad \alpha^p \quad (\alpha^p)^p \quad \dots \quad \alpha^{p^{d-1}}$ sono radici di q

$\alpha^{p^i} = \alpha^{p^j} \qquad \alpha^{p^{j-i}} = 1$

$\Phi : \alpha \longmapsto \alpha^p$ omomorfismo di Frobenius

$\mathrm{Fix}\,\Phi = \mathbb{F}_p \qquad \mathrm{Fix}\,\Phi^{(k)} = \mathbb{F}_{p^k}$

$p^k = \sum_{d \mid k} d \cdot N_d(p)$ $\#$ pol. irrid. grado d su $\mathbb{F}_p$

$$x^{p^n} - x = \prod q_i(x)$$

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = \prod_{i=1}^{k} p_i \\ 0 & p^2 \mid n \end{cases}$$

$$N_n = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d =$$

$$= \frac{1}{n} \sum_{d \mid n} \mu(d)\, p^{\frac{n}{d}}$$

$$f * g(n) = \sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right)$$

$$\mu * 1 = 1$$

mi pare...

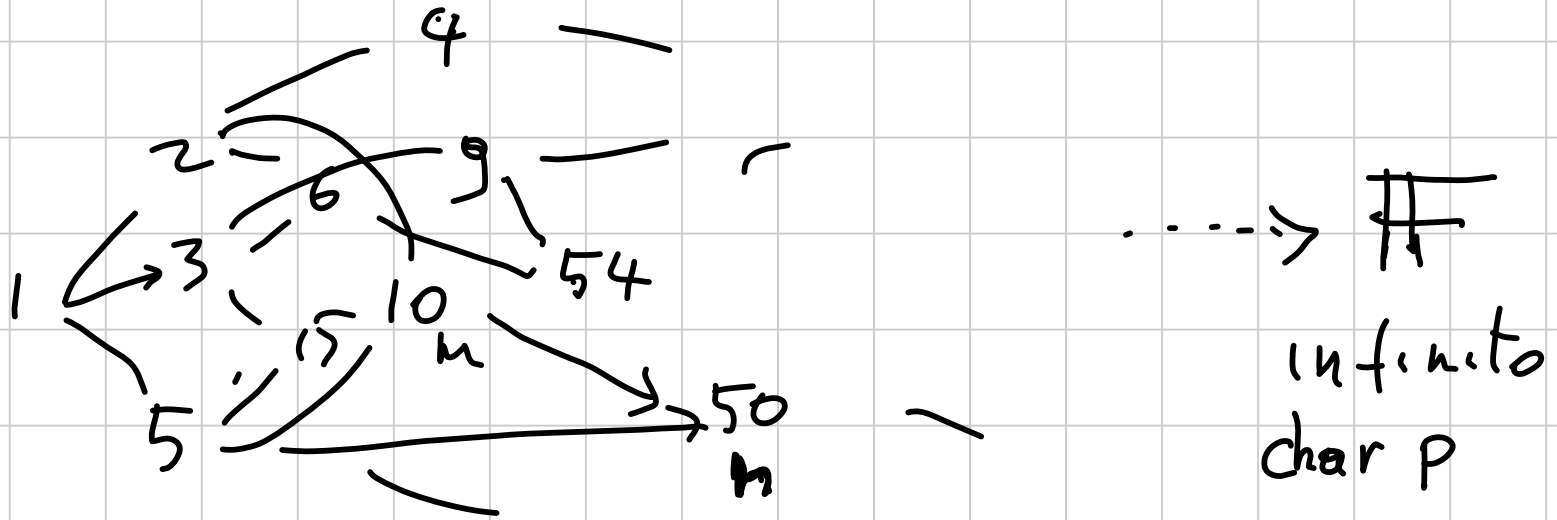
$d \mid k$
$\Rightarrow$
$\{x_{p^d} = x\}$
$\wedge$
$\{x_{p^k} = x\}$
$d \mid k$
$\Leftrightarrow$
d_1
d_2
$d_1 d_2$
k

$x^5 - 1$ en $\mathbb{F}_p$ $\quad p \neq 5$

1, 4 $\quad$ 2, 3 $\quad$ 2, 2, 1

$K = 12$

$x^{p^{12}} - x =$



$m \longrightarrow n$

$\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$

$\mathbb{F} = \text{“}\bigcup\text{”} \; \mathbb{F}_{p^k}$

$p(x)$ a coeff. in $\mathbb{F}$

$c_i \in \mathbb{F}_{p^{k_i}} \subset \mathbb{F}_{p[k_1 \dots k_n]}$ (m.c.m.)

$p(x)$ avrà radici in $\mathbb{F}_{(p^{k_1} \dots)^N} \subset \mathbb{F}$

p.es. N = m.c.m dei gradi dei fattori irrid. di p

$\mathbb{F}$ è algebricamente chiuso $\quad \Phi_{\mathbb{F}} : \mathbb{F} \to \mathbb{F}$

$\mathbb{F}_{p^k} = F_{ix}\left(\Phi_{\mathbb{F}}^{(k)}\right)$

INO 98/3

$d(n$

Trovare gli $m \in \mathbb{Z}$ per cui $\exists\, a \in \mathbb{N}$ t.c.

$$\frac{d(a^2)}{d(a)} = m.$$

$$a = \prod p_i^{\alpha_i}$$

$$m = \prod \frac{2\alpha_i + 1}{\alpha_i + 1} = \prod \left(2 - \frac{1}{\alpha_i + 1}\right)$$

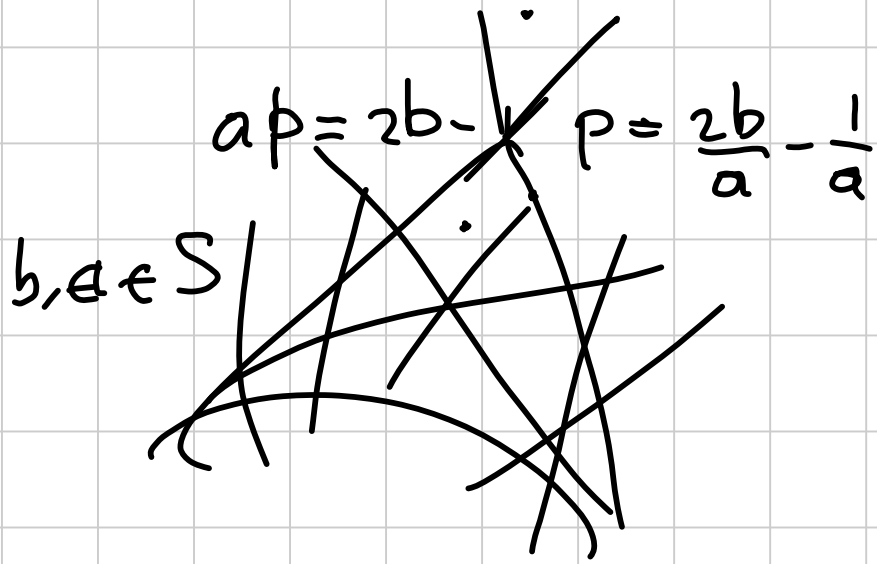
$\alpha_i + 1 = b_i$

$m = 1$ ok

$b_1 = 3,\ b_2 = 5 \rightarrow 3$

m_1, m_2 ok $\longrightarrow m_1 \cdot m_2$ ok

$$p = \frac{②p}{\frac{ap+1}{2}}$$



disp.

$m = 4k-1$ $\qquad \frac{12k-3}{6k-1} \cdot \frac{6k-1}{3k} \cdot k$

$m = 2^t k + 1$ $\qquad m \cdot (2^t - 1)$

$$m = \frac{2^t(2^t-1)k - (2^t-1)}{2^{t-1}(2^t-1)k - (2^{t-1}-1)} \cdots \frac{4(2^t-1)k-3}{2(2^t-1)k-1} \frac{2(2^t-1)k-1}{(2^t-1)k} \cdot k$$

2000 SL N6

$$\left|\left\{ n \in \mathbb{N} \mid n \text{ non è } \sum \text{ quadrati distinti} \right\}\right| \text{ è finito.}$$