A5 Di tutto un po'

Simo_the_Wolf

Titolo nota 10/09/2008

(i) Trovare tutte le $f:\mathbb{R}\to\mathbb{R}$ tali che

$$f(x-f(y))=f(f(y))+xf(y)+f(x)-1 \qquad \forall x,y\in\mathbb{R}$$

(ii) Trovare tutte le $f:\mathbb{R}\to\mathbb{R}$ tali che

$$f(f(x)+y)=f(f(x)-y)+4f(x)y \qquad \forall x,y\in\mathbb{R}$$

(iii) Dire se esiste $f:\mathbb{Q}\to\{-1,1\}$ tale che

$$\text{se } x\neq y \wedge (x+y=1 \vee x+y=0 \vee xy=1) \Rightarrow f(x)f(y)=-1$$

n) $f(x - f(y)) = f(f(y)) + x f(y) + f(x) - 1$

- $x - f(y) = 0$ prendo $x := f(y)$

$$f(0) = f(f(y)) + f(y)^2 + f(f(y)) - 1$$

$$f(f(y)) = \frac{f(0) + 1 - f(y)^2}{2}$$

$$f(c) = \frac{f(0) + 1 - c^2}{2} \quad \text{se } c \in \mathrm{Im} f$$

Se la funz. fosse surjettiva ($\mathrm{Im} f = \mathbb{R}$) avremmo finito

NO!

$c = f(y)$

$$f(x-c) = f(c) + cx + f(x) - 1 \qquad \forall x \in \mathbb{R}, \; c \in Im f$$

in particolare vale $\forall \; x, c \in Im f$

$\Rightarrow$

$$f(x-c) = f(c) + cx + f(x) - 1 = f(c-x)$$

f è pari sui valori presi dalle differenze di numeri nell'immagine i.e. $k = f(x) - f(y)$

$\Rightarrow \quad f(k) = f(-k)$

Sappiamo che $c, x \in Im f \Rightarrow$ $f(x) = \dfrac{f(0)+1-x^2}{2}$

$f(c) = \dfrac{f(0)+1-c^2}{2}$

Sostituendo abbiamo

$$f(x-c) = \frac{f(0)+1-c^2}{2} + xc + \frac{f(0)+1-x^2}{2} - 1 =$$

$$= f(0) - \frac{(c-x)^2}{2}$$

Ora sappiamo che se $k = f(x) - f(y)$ per qualche $x, y \in \mathbb{R}$ $\Rightarrow$ $f(k) = f(0) - \frac{k^2}{2}$

Ponendo $y = 0$ abbiamo $f(x - f(0)) = f(f(0)) + f(0)x + f(x) - 1$

$f(x - f(0)) - f(x) = f(f(0)) + f(0)x - 1$

non è detto che ci vada bene ($f(0) \neq 0$)

Sfruttiamo il fatto che $f \equiv 0$ non funziona

$\Rightarrow \exists\ y_0$ t.c. $f(y_0) \neq 0$

$$f(x - f(y_0)) - f(x) = f(f(y_0)) + f(y_0)\,x - 1$$

$$f(x - a) - f(x) = bx + c \qquad \boxed{b \neq 0}$$

$\forall\ K \in \mathbb{R}$ cerchiamo trovare x, y t.c. $K = f(x) - f(y)$

A questo punto abbiamo quasi vinto

$$f(K) = f(0) - \frac{K^2}{2} \qquad \text{se } K \in \mathrm{Im} f \quad f(K) = \frac{f(0)+1-K^2}{2}$$

$\Rightarrow \quad f(0) = 1 \qquad \Rightarrow \qquad f(k) = 1 - \frac{k^2}{2} \qquad \forall\, k \in \mathbb{R}$

Verifica e poi ok.

$$f(f(x) + y) = f(f(x) - y) + 4 f(x)\, y \qquad \forall\, x, y \in \mathbb{R}$$

1° PASSO) $f(x) - y = 0$ (prendiamo $y = f(x)$)

$$f(2 f(x)) = 4 f(x)^2 + f(0) \Rightarrow f(c) = c^2 + f(0)$$

Se $c \in 2\,\mathrm{Im} f$

Se fosse $f(x)+y \in 2\,\mathrm{Im} f$

Avremmo che $f(0)+(f(x)+y)^2 = f(f(x)+y) = f(f(x)-y)+4yf(x)$

$$f(f(x)-y) = (f(x)-y)^2 + f(0)$$

Questa è vera se $f(x)+y \in 2\,\mathrm{Im} f$

$$\Rightarrow \quad f(x)+y = 2f(a) \qquad \Rightarrow \quad y = 2f(a) - f(x)$$

$$f(f(x) - 2f(a) + f(x)) = f(2(f(x) - f(a))) = (2f(x) - f(a))^2 + f(0)$$

$$f(c) = c^2 + f(0) \quad \text{se} \quad \exists\, x,y \text{ t.c. } c = 2(f(x) - f(y))$$

Un'altra volta se dimostriamo che $f(x)-f(y)$ copriamo tutto $\mathbb{R}$ al variare di $x,y \in \mathbb{R}$

$$f(f(x)+y)-f(f(x)-y)=4f(x)y$$

Dobbiamo prendere come prima x_0 t.c. $f(x_0)\neq 0$

Se $f\equiv 0$ va bene, funziona, si verifica

Altrimenti se $\exists$ almeno un valore per cui $f(x)\neq 0$ abbiamo che $f(x)=x^2+f(0)$

Si verifica che $f(x)=x^2+c$ va bene

$\forall\, c\in\mathbb{R}$.

IMO 2008/2

$xyz = 1$

$\Rightarrow$ (a) $\sum \frac{x^2}{(x-1)^2} \geq 1$

(b) esistono infinite terne $x, y, z \in \mathbb{Q}$ per cui vale l'uguaglianza

$x = \frac{1}{a} \quad y = \frac{1}{b} \quad z = \frac{1}{c}$

$abc = 1$

$$\frac{x^2}{(x-1)^2} = \frac{1}{(1-\frac{1}{x})^2} = \frac{1}{(1-a)^2}$$

$$\frac{1}{(1-a)^2} + \frac{1}{(1-b)^2} + \frac{1}{(1-c)^2} \geq 1$$

svolgiamo tutti i conti:

$$\sum (1-a)^2(1-b)^2 \geq (1-a)^2(1-b)^2(1-c)^2$$

$$\sum (1 - a - b + ab)^2 \geq (1 - a - b - c + ab + bc + ca - abc)^2$$

$$\sum (1 + a^2 + b^2 + ab)^2 + 2ab + 2ab - 2a - 2b - 2a^2b - 2ab^2) \geq$$

$$\geq (a+b+c)^2 + (ab + bc + ca)^2 - 2(ab+bc+ca)(a+b+c)$$

$$2\sum a^2 + 2\sum ab + \sum a^2b^2 - 2\sum_{\text{sym}} a^2b - 4\sum a + 3 \geq$$

$$\geq \cancel{\sum a^2} + \cancel{2\sum ab} + \cancel{\sum ab} + 2\sum a^2 b < -\cancel{2\sum_{Sym} a^2 b} - 6$$

$$\sum a^2 + 2\sum ab - 6\sum a + 9 \geq 0$$

$$(a+b+c)^2 - 6(a+b+c) + 9 \geq 0$$

$$(a+b+c-3)^2 \geq 0$$

La parte (*) è fatta

L'uguaglianza c'è (ovviamente) quando

$$\begin{cases} a+b+c=3 \\ abc=1 \end{cases}$$

Vogliamo trovare infinite terne $(a,b,c) \in \mathbb{Q}^3$ t.c. soddisfano questo sistema

Sostituendo la (1) nella (2) otteniamo

$$ab(3-a-b)=1$$

1° modo) Se per infiniti valori razionali di a $\Delta_p(b) \in \mathbb{Q}^2$ allora trovo infinite coppie

che soddisfano la mia relazione.

Qui il Vieta jumping NON FUNZIONA

$$-ab^2 + (3-a)a \cdot b - 1 = 0 \leftarrow$$

$$\Delta = ((3-a)\cdot a)^2 - 4a = 9a^2 - 6a^3 + a^4 - 4a =$$

$$= a(a^3 - 6a^2 + 9a - 4) =$$

$$= a(a-1)(a^2 - 5a + 4) =$$

$$= a(a-1)^2(a-4)$$

$$\Delta \in \mathbb{Q}^2 \iff a(a-4) \in \mathbb{Q}^2 \iff \frac{a(a-4)}{a^2} \in \mathbb{Q}^2$$

$$1 - \frac{4}{a} \in \mathbb{Q}^2$$

$$\underbrace{ab(3-a-b)-1=0}_{f(a,b)}$$

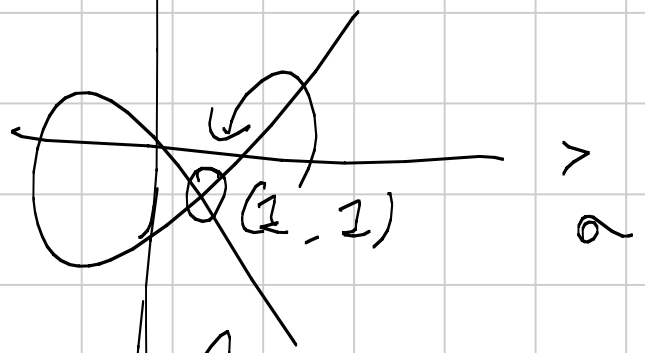
$(1,1)$

b

$$\frac{\partial f}{\partial a} \qquad \frac{\partial f}{\partial b}$$

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

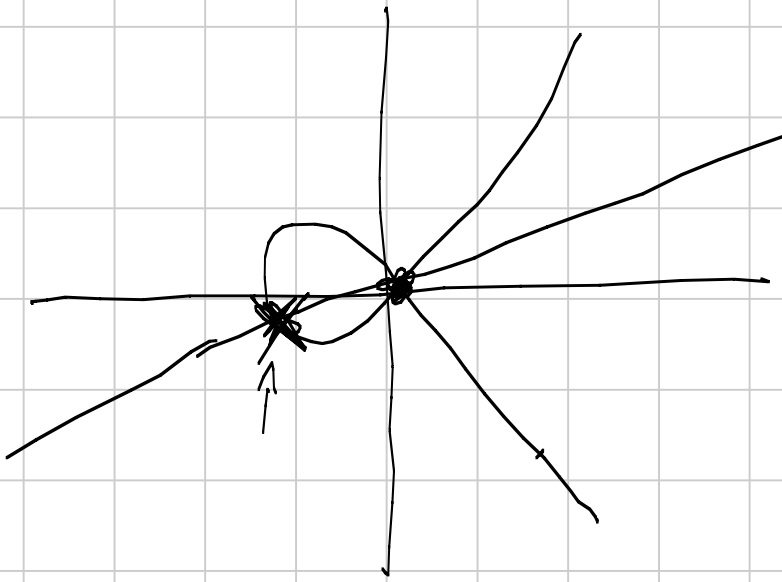
$$b(3-a-b)-ab$$



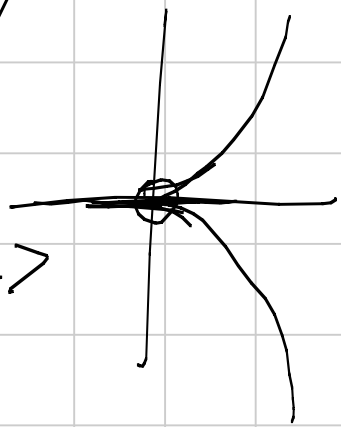
$(0,+)$

$y = tx$

$t \in \mathbb{Q}$



$(0,+)$



1.1

$$y = t(x-1)+1$$

$$a = t(b-1)+1$$

$$(t(b-1)+1)\,b\,(3 - t(b-1) - 1 - b) - 1 = 0$$

$$(tb - t + 1)\,b\,(3b - t^2b^2 + tb - b - b^2) - 1 = 0$$

$$b - 1 = \alpha$$

$$(t\alpha + 1)\,b\,(3 - t\alpha - 1 - b) - 1 = 0$$

$$1 - t\alpha - \alpha \quad (\alpha+1)$$

$$(t\alpha + 1 - t^2\alpha^2 - t\alpha - t\alpha^2 - \alpha)\,b - 1 = 0$$

$$- t^2\alpha^3 - t^2\alpha^2 - t\alpha^3 - t\alpha^2 - \alpha^2$$

$$-t^2\alpha - t^2 - t\alpha - t - 1 = 0$$

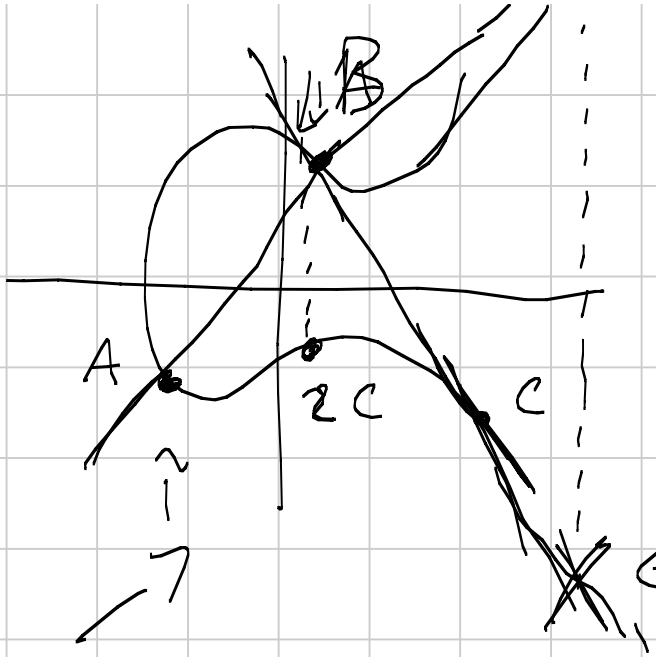
$$\alpha = -\frac{t^2+t+1}{t^2+t} \qquad b = \alpha + 1 = \frac{-1}{t^2+t}$$

$$a = t(b-1)+1 = \qquad t\alpha + 1 =$$

$$= \frac{-t^3 - t^2 - t + t^2 + t}{} \qquad a = \frac{-t^3}{t^2+1}$$

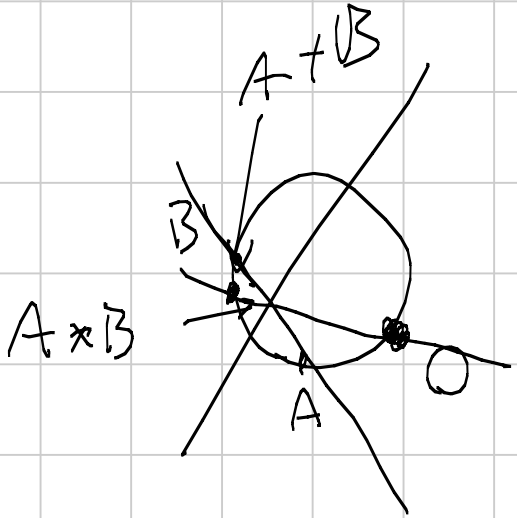
$$\left(-\frac{t^2}{t+1}, \frac{-1}{t^2+t}\right)$$

↘



$y^2 = f(x)$ ← polinomio di 3° grado senza radici multiple

$3x^3 + 4y^3 + 5z^3 = 0$



lui che ha inventato il VERTECH, lui non era una grande persona

$(G, \cdot)$ (i) $\forall a, b \quad ab \in G$

(ii) $\forall a \in G \quad \exists \; b \in G$ t.c. $ab = e = ba \quad (b = a^{-1})$

(iii) $\exists \; e \in G$ t.c. $ea = ae = a \quad \forall a \in G$

$|G| < +\infty$

$\forall a \in G \quad \exists \; k$ t.c. $a^k = e$ il minimo di questi k è tale che $k = \text{ord}(a) \mid |G|$

<u>Sottogruppo</u> $H \subseteq G$ è un sottogruppo se $(H, \cdot)$ è un gruppo $H \leq G$

$(\mathbb{Q}^*, \cdot)$ è un gruppo $((\mathbb{Q}^*)^2, \cdot)$ è un gruppo

Teo d. Lagrange $|H| \mid |G|$

$$H = \langle a \rangle = \{e, a, a^2, a^3, \dots, a^{ord(a)-1}\}$$

$$(a^k)^{-1} = a^{ord(a)-k}$$

$$|H| \mid |G| \Rightarrow ord(a) \mid |G|$$

Gruppo abeliano se $ab = ba \quad \forall a, b \in G$

$(123) \to (231)$

$(123) \to (213)$

$\{a_1, \dots, a_n\} = G$

$\{a a_1, a a_2, a a_3, \dots, a a_n\} = G$

Se $i \neq j$

$\Rightarrow a a_i \neq a a_j$ $\quad$ ~~a^{-1}~~ ~~a~~ $a_i = a_j$ $\quad$ $a_i = a_j$

$a_1 a_2 \cdots a_n = (a a_1)(a a_2) \cdots (a a_n)$

$A = (a_1 \cdots a_n) = a^n (a_1 \cdots a_n) = a^n A$

~~$A A^{-1}$~~ $= a^n$ ~~$A A^{-1}$~~ $\quad$ $a^n = e$ $\quad$ $n = |G|$

$\{ k \mid a^k = e \} = d\mathbb{Z}$ $\quad$ dove $d = ord(a)$

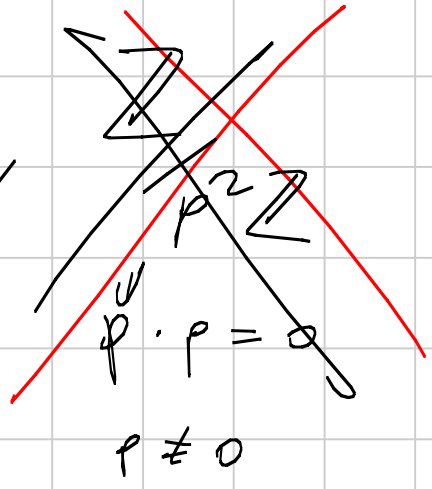
Campi Finiti:

$(\mathbb{K}, +, \cdot)$ è un campo se $(\mathbb{K}, +)$ è un gruppo abeliano (abeliano)

e $(\mathbb{K}^*, \cdot)$ è un gruppo abeliano ($\mathbb{K}^* = \mathbb{K} \setminus \{0\}$)

e vale la proprietà distributiva.

$\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{Z}/p\mathbb{Z}$ (p primo), $\mathbb{C}$,



$1, \quad 1+1, \quad 1+1+1, \quad \dots, \quad n \qquad |\mathbb{K}| < +\infty$

Poiché $\mathbb{K}$ ha un numero finito di elementi vuol dire che prima o poi dovrò avere $n_1 = n_2$ (in $\mathbb{K}$)

$n_1 - n_2 = 0 \quad \exists\, k \in \mathbb{N}$ t.c. $k = 0$

$\underbrace{1+1+1 \dots +1}_{n}$ $\qquad ord_+(1) = char(\mathbb{K}) = p$

$\boxed{a>0 \quad b>0}$

Se per assurdo $char \mathbb{K} = a \cdot b$ con $a<p$, $b<p$

$a \neq 0 \qquad b \neq 0 \qquad a \cdot b = 0$

$|K| = n$

Teo. Cauchy se p primo $p \mid |G| \Rightarrow \exists\ a \in G$ t.c. $a^p = e \Rightarrow ord(a) = p$

Supp. per assurdo che ci sia un altro primo q oltre a p che divide n.

$p \mid n$ $p = char K$ $q \mid n$ con $q \neq p$

per Cauchy $\exists\ a \in K^*$ t.c. $ord_+(a) = q$

$\underbrace{(a + a + a + \dots + a)}_{q} a^{-1} = 0 \cdot a^{-1}$

$\underbrace{1+1+1+\cdots+1}_{q} = 0$

$p \mid q \quad \Rightarrow \quad q = p$

Tutti gli elementi hanno lo stesso ordine additivo quindi $ord_+(a) = ord_+(1) = \text{char } \mathbb{K} = p$

$|\mathbb{K}| = p^n \qquad \mathbb{K} = \mathbb{F}_{p^n}$

$\mathbb{F}_{p^n} \supseteq \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, 3, \dots, p-1\}$

$a \in \mathbb{F}_{p^n} \quad a \neq 0 \quad a \in \mathbb{F}_{p^n}^* \quad ord.(a) \mid |\mathbb{F}_{p^n}^*|$

$a^{p^n-1} = 1 \quad \forall \; a \in \mathbb{F}_{p^n}^* \Rightarrow a$ è radice di x^{p^n-1}

tutte e sole le radici di $x^{p^n-1}-1$ sono gli elementi di $\mathbb{F}_{p^n}^*$

tutte " " " $x^{p^n}-x$ sono gli

" " $\mathbb{F}_{p^n}$.

$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n} \iff x^{p^d-1}-1 \mid x^{p^n-1}-1$

$\Uparrow \qquad\qquad\qquad\qquad \Uparrow$

$d \mid n \qquad\qquad p^d-1 \mid p^n-1 \iff d \mid n$

$p(x)$ irriducibile in $\mathbb{F}_p[x]$ $\qquad \frac{\mathbb{Z}}{p\mathbb{Z}}$

$$\frac{\mathbb{F}_p[x]}{(p(x))} \cong \mathbb{F}_{p^n}$$

↑

Qui dentro $p(x) = 0$ quindi se non fosse irriducibile avrei che $r(x)s(x) = 0$

$$\{1, x, x^2, \dots, x^{n-1}\}$$

$$a_1 + a_2 x + a_3 x^2 + \dots + a_n x^{n-1} \neq 0$$

$$x^n = p(x) - x^h$$

G gruppo è detto ciclico se $\langle x \rangle = G$

$$G = \{ e, x, x^2, \dots, x^{n-1} \} \cong \left(\mathbb{Z}_{n\mathbb{Z}}, + \right)$$
$$\{ 0, 1, 2, \dots, n-1 \}$$

$(\mathbb{F}_{p^n}^*, \cdot)$ è ciclico $\quad |G| = p^n - 1$

$a \in G$ è residuo quadratico $\iff a^{\frac{ord(G)}{2}} = 1$

$a = x^k$ k è pari $\Rightarrow x^{\frac{k \cdot ord(a)}{2}} = \left(x^{ord(a)} \right)^{\frac{k}{2}} = 1$

$a = x^d$ ma a non è residuo quadratico $\Rightarrow$ d è dispari

$2^n - 1$ è un numero primo $\iff 2^n - 1 \mid a_n$

dove $a_2 = 4$ $\quad a_{n+1} = a_n^2 - 2 = \left(\beta^2 + \frac{1}{\beta^2} + 2\right) - 2$

$\beta + \frac{1}{\beta}$

$a_2 = \alpha + \frac{1}{\alpha}$ $\quad a_3 = \alpha^2 + \frac{1}{\alpha^2}$ $\quad a_4 = \alpha^4 + \frac{1}{\alpha^4}$

$\ldots \quad a_n = \alpha^{2^{n-2}} + \frac{1}{\alpha^{2^{n-2}}}$

$\alpha = 2 + \sqrt{3}$ $\qquad p \mid a_n$

$\alpha^{2^{n-2}} + \frac{1}{\alpha^{2^{n-2}}} = 0$ $\qquad \alpha \in \mathbb{F}_{p^2} \cong \frac{\mathbb{F}_p[x]}{(x^2 - 3)}$

$$\alpha^{2^{n-1}} + 1 = 0 \iff 2^n = \mathrm{ord}_{\mathbb{F}_{p^2}}(\alpha)$$

Sto supponendo $p = 2^n - 1$ e spero che $p \mid a_n$. Finora ho dimostrato che

$$p \mid a_n \iff \mathrm{ord}_{\mathbb{F}_{p^2}}(\alpha) = 2^n \iff \alpha^{2^{n-1}} = -1$$

$$\iff (2+\sqrt{3})^{\frac{p+1}{2}} = -1$$

3 non è un res. qu. mod $2^n - 1$

$$(2+\sqrt{3})^{p+1} = (2+\sqrt{3})^p \cdot (2+\sqrt{3}) = (2^p + \sqrt{3}^p)\cdot(2+\sqrt{3}) =$$

$$= 2$$

$$\left(\frac{3}{2^n-1}\right)\left(\frac{2^n-1}{3}\right) = -1$$

n è dispari $\Rightarrow 2^n - 1 \equiv 1 \pmod 3$

$\Rightarrow \left(\frac{3}{2^n-1}\right) = -1$

$$3^{\frac{p-1}{2}} = -1 \qquad \alpha^2 = 3$$

$$\alpha^p = \alpha \cdot \alpha^{p-1} =$$
$$= \alpha \cdot (\alpha^2)^{\frac{p-1}{2}} =$$
$$= \alpha \cdot \underbrace{3^{\frac{p-1}{2}}}_{\equiv 1} = -\alpha$$

$$(2+\sqrt{3})^{p+1} = (2+\sqrt{3}^p)(2+\sqrt{3}) =$$
$$= (2-\sqrt{3})(2+\sqrt{3}) = 1$$

$$(2+\sqrt{3})^{2^n} = 1 \qquad \operatorname{ord}_{\mathbb{F}_{p^2}}(q) \mid 2^n$$

Se avessimo $\alpha = \beta^2$ dovremmo avere

$$\beta^{p+1} = -1 \qquad \beta^{2(p+1)} = 1$$

$$\beta^{\frac{p^2-1}{2}} = \beta^{p+1 \cdot \frac{p-1}{2}} = \left(\beta^{p+1}\right)^{\frac{p-1}{2}} = -1$$

$$\alpha = \beta^2 \neq \gamma^h \iff \operatorname{ord}_{\mathbb{F}_{p^2}}(\alpha) = 2^n$$

$$(1+\sqrt{3})^2 = 4 + 2\sqrt{3} = 2\alpha \qquad 2^n = 1$$

$$2^{n+1} = 2 \qquad 2^{\frac{n+1}{2}} = \sqrt{2}$$

$$\left(\frac{1+\sqrt{3}}{2^{\frac{n+1}{2}}}\right) = \beta$$

$$\beta^{p+1} \overset{?}{=} -1 \qquad \beta^{p+1} = \left(\frac{1+\sqrt{3}}{2^{\frac{n+1}{2}}}\right)^{p+1} = \frac{(1-\sqrt{3})\cdot(1+\sqrt{3})}{2^{\frac{n+1}{2}} \cdot 2^{\frac{n+1}{2}}} = \frac{-2}{2^{n+1}}$$

$\beta^{p+1} = -1 \iff \beta$ non è residuo quadratico

$\beta = \underbrace{(a+b\sqrt{3})^2}$ dove $a, b \in \mathbb{F}_p$

tutti e soli gli elementi di $\mathbb{F}_p$

$$(a+b\sqrt{3})(c+d\sqrt{3}) = (ac+3bd) + (ad+bc)\sqrt{3} \qquad -1$$

$2^n - 1$ es primo $\Rightarrow$ $2^n - 1 \mid a_n$

$p \mid 2^n - 1 \mid a_n \Rightarrow 2^n - 1$ es primo

$p \mid a_n \iff \mathrm{ord}_{\mathbb{F}_{p^2}}(\alpha) = 2^n$

$\iff \mathrm{ord}_{\mathbb{F}_{p^2}}(\beta) = 2^{n+1}$

$2^{n+1} \mid |\mathbb{F}_{p^2}^*| = p^2 - 1 = (p-1)(p+1)$

$p+1 \geq 2^n \Rightarrow p \geq 2^n - 1$

$\square$.