TDN 2 ADVANCED

darkcrystal

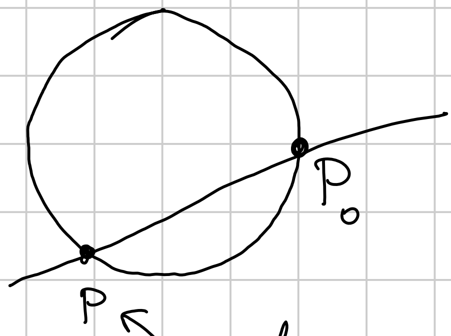
Titolo nota 06/09/2018

Parametrizzazioni (delle cubiche singolari)

(x, y) razionali su $x^2+y^2=1$

$P_0 = (1, 0)$

$$\begin{cases} x^2+y^2=1 \\ y = m(x-1) \end{cases}$$



coord raz

$y = m(x-1)$ con $m \in \mathbb{Q}$

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

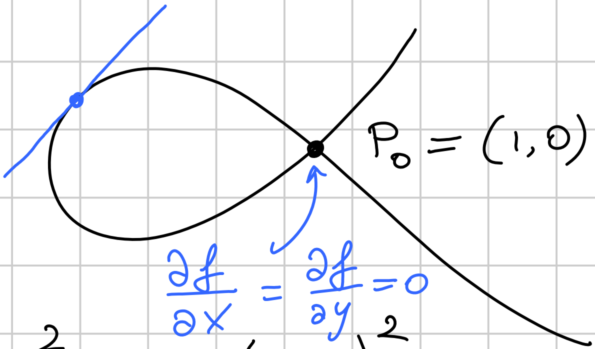
$$x_1 = 1 \qquad x_2 = \frac{m^2-1}{m^2+1} \rightsquigarrow y = \frac{-2m}{m^2+1}$$

$$(x,y) = \left(\frac{1-m^2}{1+m^2}, \frac{2m}{m^2+1}\right)$$

Terne pitagoriche: $a^2+b^2=c^2$

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$$

Cubica singolare:



$$f(x,y) = y^2 - x(x-1)^2$$

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

$$(1,0) + t(a,b) \leftarrow$$ posso supporre (a,b) interi coprimi

$$y = tb \qquad x = 1+ta$$

$$t^2 b^2 = (1+ta)\, t^2 a^2$$

$$\Downarrow$$

$$t = 0 \quad \text{oppure} \quad \left(\frac{b^2}{a^2} - 1\right) \cdot \frac{1}{a} = t$$

Parametrizz: $$(1,0) + \left(\frac{b^2 - a^2}{a^3}\right)(a,b)$$

IMO SL 2014 N2

$$\sqrt[3]{7x^2 - 13xy + 7y^2} = |x-y| + 1$$

Wlog $x > y$.

$$0 = \overbrace{7x^2 - 13xy + 7y^2 - \left(1 + 3(x-y) + 3(x-y)^2 + (x-y)^3\right)}^{f(x,y)}$$

Deriviamo!
$$\begin{cases} 0 = 14x - 13y - \left(3 + 6(x-y) + 3(x-y)^2\right) \\ 0 = -13x + 14y - \left(-3 + 6(x-y)(-1) - 3(x-y)^2\right) \\ f(x,y) = 0 \end{cases}$$

$$\begin{cases} 0 = x+y \\ 0 = 14x + 13x - \left(3 + 12x + 12x^2\right) \\ 0 = 7x^2 + 13x^2 + 7x^2 - \left(1 + 6x + 12x^2 + 8x^3\right) \end{cases}$$

$$\begin{cases} y = -x \\ 0 = -12x^2 + 15x - 3 \\ 0 = -8x^3 + 15x^2 - 6x - 1 \end{cases} \qquad \left\{ \underset{\text{OK}}{x=1}, \ \underset{\text{NO}}{\pm 1/4} \right.$$

Punto bello: $(1, -1)$

$$\begin{cases} x = 1 + at \\ y = -1 + bt \end{cases} \qquad \text{con } a, b \text{ interi coprimi}$$

$$7(1+at)^2 - 13(1+at)(-1+bt) + 7(-1+bt)^2 =$$

$$= 1 + \left(2 + t(a-b)\right)^3 + 3\left(2 + t(a-b)\right)^2 + 3\left(2 + t(a-b)\right)$$

$$7a^2t^2 - 13abt^2 + 7b^2t^2 = t^3(a-b)^3 + 3 \cdot 2 \cdot t^2(a-b)^2$$
$$+ 3t^2(a-b)^2$$

$$t = \frac{-2a^2 + 5ab - 2b^2}{(a-b)^3}$$

Tutte le soluz. raz: $\begin{cases} 1 + a\,\dfrac{-2a^2+5ab-2b^2}{(a-b)^3} \\[2ex] -1 + b\,\dfrac{-2a^2+5ab-2b^2}{(a-b)^3} \end{cases}$

Se $p \mid a-b$, $\quad p \nmid a$ $\qquad -2a^2+5ab-2b^2$

$$\equiv -2a^2+5a^2-2a^2$$

$$\equiv a^2 \mod p$$

$$\not\equiv 0$$

Soluzioni intere : $a = b \pm 1$

Seconda applicazione

Numero delle coppie (x,y) t.c.

$$x^2+y^2 \equiv 1 \pmod p$$

$(x_0, y_0) = (1,0)$ funziona

Sia (x,y) una qualunque soluz. con $x \neq 1$

Allora definisco $m = \dfrac{y}{x-1} \in \mathbb{Z}/p\mathbb{Z}$

e (x,y) è soluzione di $\begin{cases} x^2+y^2 \equiv 1 \ (p) \\ y \equiv m(x-1) \ (p) \end{cases}$

$$\begin{cases} x^2 + m^2(x-1)^2 \equiv 1 \ (p) \\ y \equiv m(x-1) \end{cases}$$

$$\Rightarrow \begin{cases} x+1 + m^2(x-1) \equiv 0 \ (p) \\ y \equiv m(x-1) \pmod p \end{cases}$$

$$\begin{cases} x \equiv \dfrac{m^2-1}{m^2+1} \mod p \\ y \equiv m(x-1) \mod p \end{cases}$$

Caso 1: $p \equiv 3 \mod 4$. La param. funziona per ogni m, quindi trovo p soluzioni $+ 1$ trovata all'inizio

Caso 2: $p \equiv 1 \ (4)$. Ci sono 2 valori "proibiti" per $m \rightsquigarrow p-1$ soluzioni

Sollevamento di Hensel

Macchinario per passare da congruenze mod p a congruenze mod p^n

Lemma Sia $f(x) \in \mathbb{Z}[x]$ e $a \in \mathbb{Z}$.

Supponiamo: $\begin{cases} f(a) \equiv 0 \mod p \\ f'(a) \not\equiv 0 \mod p \end{cases}$

Allora $\forall n$ esiste una soluzione della congr.

$$f(x) \equiv 0 \mod p^n$$

Dim $\boxed{p \to p^2}$ $\qquad f(x) = f(a) + (x-a)\, q(x)$

Scelgo $x = a + pK$

$$f(a+pK) = f(a) + pK\, q(a+pK)$$

Scrivo $f(a) = pm$: voglio risolvere

$$0 \equiv pm + pK\, q(a+pK) \mod p^2$$

$$0 \equiv m + K\, q(a) \mod p$$

Si risolve $\Leftarrow$ $q(a) \not\equiv 0 \mod p \iff f'(a) \not\equiv 0\ (p)$

D'altro canto, se derivo $f(x) = f(a) + (x-a)\, q(x)$

trovo $f'(x) = q(x) + (x-a)\, q'(x)$

$\Rightarrow f'(a) = q(a)$ $\square$

Conseguenza $a \overset{\not\equiv 0\,(p)}{}$ è residuo quadr. mod p^n

$(n \geq 1,\ p$ dispari$)$ $\Leftrightarrow$ lo è mod p

$f(x) = x^2 - a \qquad f'(x) = 2x$

Ipotesi: $x^2 - a \equiv 0 \ (p)$ abbia una soluzione

Se $b^2 \equiv a \pmod p \Rightarrow f'(b) = 2b \not\equiv 0\ (p)$

Esercizio $y^2 = p^3 + 10p^2 - 6p + 1$

Mod $p \longrightarrow y^2 \equiv \pm 1 \bmod p \xrightarrow{\text{"wlog"}} y \equiv 1\ (p)$

Mod p^2: $y = 1 + kp$

$$1 + 2kp \equiv -6p + 1 \bmod p^2$$

$$2k \equiv -6 \bmod p \quad \begin{cases} p = 2, & \text{NO} \\ k \equiv -3\ (p) \end{cases}$$

$\Rightarrow y \equiv 1 - 3p \bmod p^2$

$y = 1 - 3p + kp^2 \Rightarrow 1 + 9p^2 - 6p + 2kp^2 \equiv 1 - 6p + 10p^2$ mod p^3

$$2Kp^2 \equiv p^2 \mod p^3$$

$$2K \equiv 1 \mod p$$

$$\Rightarrow \quad y = 1 - 3p + \frac{p+1}{2} p^2 + \underset{jp^3}{\text{multiplo di } p^3}$$

Supponiamo $j < 0 \Rightarrow y \leq 1 - 3p + \frac{p+1}{2} p^2 - p^3$

$$\leq -p^3/2 + p^2/2 - 3p + 1$$

$$\leq -p^3/2 + p^2/2$$

$$\begin{array}{l} y^2 \geq \frac{1}{4}(p^3 - p^2)^2 \geq \frac{1}{4} p^4 (p-1)^2 \geq p^4 \\ \text{\rotatebox{90}{$=$}} \\ p^3 + 10p^2 - 6p + 1 \leq p^3 + 10p^2 \end{array}$$

$$p^2 \leq p + 10$$

$$\Rightarrow p \leq 3$$

e similmente per $j \geq 0$

Uniche sol: $p = 3, y = \pm 10$

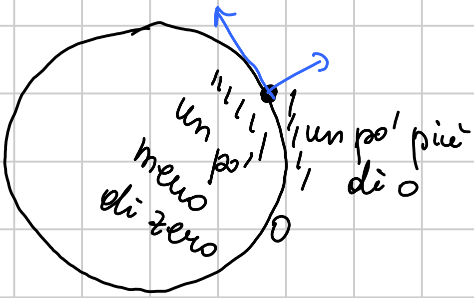
Soluzioni di $a^2+b^2=2c^2 \iff \left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=2$

Come prima! $a=b=c=1$ $\qquad x^2+y^2=2$

$x=1+at$
$y=1+bt$ $\qquad$ sviluppo, faccio il conto, viene

Fatto (difficile) Per le equaz. di 2° grado in 2 variabili razionali: c'è una soluz razionale se e solo se ci sono soluz mod p^n $\forall p\ \forall n$

$\boxed{\text{Tangenti}}$ $\qquad f(x,y)=0 \qquad (x_0,y_0)$ t.c. $f(x_0,y_0)=0$



x^2+y^2-1

La direzione di max crescita è

$$\begin{pmatrix} \frac{\partial f}{\partial x}(x_0,y_0) \\ \frac{\partial f}{\partial y}(x_0,y_0) \end{pmatrix}$$

$$f(x,y) = f(x_0,y_0) + \frac{\partial f}{\partial x}\cdot(x-x_0) + \frac{\partial f}{\partial y}(y-y_0) + \dots$$

$$= \begin{pmatrix} \partial f/\partial x \\ \partial f/\partial y \end{pmatrix} \cdot \begin{pmatrix} x-x_0 \\ y-y_0 \end{pmatrix} + \text{cose piccole}$$

Morale: la tg è perpendicolare a $\begin{pmatrix} \partial f/\partial x \\ \partial f/\partial y \end{pmatrix}$

Esempio $f(x,y) = x^2+y^2-1$

$$\partial f/\partial x = 2x \qquad \partial f/\partial y = 2y$$

Prendiamo $(x,y) = (1/\sqrt{2}, 1/\sqrt{2})$

Direzione max crescita : $/\!/ \begin{pmatrix} \sqrt{2} \\ \sqrt{2} \end{pmatrix} /\!/ \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$$\text{tg} \ /\!/ \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Hensel in 2 variabili

$f(x,y) \in \mathbb{Z}[x,y]$; $f(a,b) \equiv 0 \mod p$

Se $\frac{\partial f}{\partial x}(a,b) \not\equiv 0$ OPPURE $\frac{\partial f}{\partial y}(a,b) \not\equiv 0 \ (p)$

allora trovo soluzioni modulo p^n

Contare soluzioni mod p

$$x^2+y^2 \equiv 1 \pmod p$$

$$\sum_{a+b=1} N(x^2 \equiv a) \cdot N(y^2 \equiv b) =$$

$$= \sum_{a+b=1} \left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{b}{p}\right)\right) =$$

$$= \underbrace{\sum_{a+b=1} 1}_{p} + \underbrace{\sum_{a+b=1} \left(\frac{a}{p}\right)}_{0} + \underbrace{\sum_{a+b=1} \left(\frac{b}{p}\right)}_{0} + \sum_{a+b=1} \left(\frac{ab}{p}\right)$$

$$= p + \sum_{\substack{a+b=1 \\ b \neq 0}} \left(\frac{a/b}{p}\right) = p + \sum_{a \neq 1} \left(\frac{a/(1-a)}{p}\right)$$

$$\frac{a}{1-a} = c \iff a = c - ac \iff a(c+1) = c$$

$$\iff a = \frac{c}{c+1}$$

$$\sum_{a \neq 1} \left(\frac{a/(1-a)}{p}\right) = \sum_{c \neq -1} \left(\frac{c}{p}\right) = -\left(\frac{-1}{p}\right)$$

$$\#\{(x,y) \mid x^2+y^2 \equiv 1 \ (p)\} = p - \left(\frac{-1}{p}\right)$$

CARATTERI

Un carattere è una funzione

$$\chi : \mathbb{F}_p^* \longrightarrow \{1, \zeta_{p-1}, \dots, \zeta_{p-1}^{p-2}\}$$

tale che $\chi(ab) = \chi(a)\chi(b)$

[in soldoni: $\chi(g) = \zeta_{p-1}^{a}$

$\chi(g^i) = \zeta_{p-1}^{ai}$]

NON NECESSARIAMENTE $(a, p-1) = 1$

Esempio $\chi(n) = \left(\frac{n}{p}\right)$

Per comodità: $\chi(0) = 0$

Domanda Quanti caratteri ci sono? $p-1$

Uno di questi è il carattere che fa sempre 1

Per questo carattere χ_0 si pone $\chi_0(0) = 1$

Fissiamo χ carattere. Quanto fa $\sum_{a\in\mathbb{F}_p} \chi(a) = 0$?

(se $\chi \neq \chi_0$)

$$\sum_{a\in\mathbb{F}_p} \chi(a) = \sum_{a\neq 0} \chi(a) = \sum \chi(g^i)$$

$$= \sum_{i=0}^{p-2} \zeta_{p-1}^{bi} = 0$$

Viceversa: $\sum_{\chi} \chi(a) = \sum_{b=0}^{p-2} \zeta_{p-1}^{bi} = 0$

$a = g^i$

Def. χ e' di ordine $n \mid p-1$ se la sua immagine ha ordine n

Ex $\left(\frac{\cdot}{p}\right)$ ha ordine 2

Lemma Sia χ un carattere di ordine $n \mid p-1$

Allora $N(x^n \equiv a \mod p) = \sum_{i=0}^{n-1} \chi(a)^i$

Dim. Se c'e' una soluz. ce ne sono n.

$N(x^n \equiv 1 \ (p)) = n \qquad g^{\frac{p-1}{n}}, g^{2\frac{p-1}{n}}, \ldots$

Soluzioni $\Leftrightarrow$ $a \equiv g^{nk}$

$$\sum_{i=0}^{n-1} \chi(a)^i = \sum_{i=0}^{n-1} 1^i = n$$

No soluz $\Leftrightarrow$ $a \equiv g^r$ con $n \nmid r$

$\Leftrightarrow \chi(a) = \zeta_n^r$

$$\sum_{i=0}^{n-1} \zeta_n^r = 0 \quad \text{se } n \nmid r$$

$\square$

Supponiamo ora di volere contare

$$N\left(x^5 + y^2 - 1 \equiv 0 \ (p)\right) = \begin{cases} p, & \text{se } p \not\equiv 1 \ (5) \\ ?? & \text{se } p \equiv 1 \ (5) \end{cases}$$

Fissiamo χ carattere di ordine 5

$$\sum_{a+b=1} N\left(x^5 \equiv a \ (p)\right) N\left(y^2 \equiv b \ (p)\right)$$

$$= \sum_{a+b=1} \left(1 + \chi(a) + \dots + \chi(a)^4\right)\left(1 + \left(\frac{b}{p}\right)\right)$$

$$= p + \underset{\sum \chi}{0} + \underset{\sum \chi^2}{0} + \underset{\sum \chi^3}{0} + \underset{\sum \chi^4}{0} + \underset{\sum \left(\frac{b}{p}\right)}{0}$$

$$+ \underbrace{\sum_{a+b=1} \chi(a) \left(\frac{b}{p}\right)}_{\sim \sqrt{p}} + \dots$$

SOMME DI GAUSS

$$g_a(\chi) = \sum_{t \in \mathbb{Z}/p\mathbb{Z}} \chi(t)\, \zeta_p^{at}$$

1 $$g_a(\chi) = \sum_t \chi(t)\, \zeta_p^{at} = \frac{1}{\chi(a)} \sum_t \chi(at)\, \zeta_p^{at}$$

$$= 1/\chi(a) \sum_t \chi(t)\, \zeta_p^{t} = \chi(a^{-1})\, g_1(\chi)$$

② $$\sum_a g_a(\chi)\overline{g_a(\chi)} =$$

$$\sum_a \|g(\chi)\|^2 \chi(a^{-1})\overline{\chi(a^{-1})} = \|g(\chi)\|^2\cdot(p-1)$$

Ma è anche $= \displaystyle\sum_a\sum_{t_1}\chi(t_1)\zeta_p^{at_1}\overline{\left(\sum_{t_2}\chi(t_2)\zeta_p^{at_2}\right)}$

$$= \sum_{a,t_1,t_2}\zeta_p^{a(t_1-t_2)}\chi(t_1)\chi(t_2)^{-1}$$

$$= \sum_{t_1=t_2}(p-1)\chi(t_1)\chi(t_2^{-1})$$

$$= \sum_{t_1}(p-1)\chi(t_1\cdot t_1^{-1}) = p(p-1)$$

Conseguenza: $\|g(\chi)\| = \sqrt{p}$

Corollario: $\displaystyle\sum_t \underbrace{\chi(t)}_{\text{Legendre}}\zeta_p^t = \sum_{t=\square}\zeta_p^t - \sum_{t\neq\square}\zeta_p^t$

ha valore assoluto $\sqrt{p}$; in realtà è

proprio $\pm\sqrt{\pm p}$

$$\zeta_5 + \zeta_5^4 - \zeta_5^2 - \zeta_5^3 = \sqrt{5}$$

Teorema Se χ_1, χ_2 sono caratteri con $\chi_1 \neq 1$, $\chi_2 \neq 1$, $\chi_1\chi_2 \neq 1$ allora

$$\sum_{a+b=1} \chi_1(a)\chi_2(b) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$$

In particolare $\left|\sum_{a+b=1} \chi_1(a)\chi_2(b)\right| = \sqrt{p}$

Tornando al conto di prima:

$$N(y^2+x^5 \equiv 1 \ (p)) = \sum_{a+b=1} \left(1+\chi(a)+\dots+\chi(a)^4\right)\left(1+\left(\frac{b}{p}\right)\right)$$

$$= p + 4 \text{ termini di ordine } \sqrt{p}$$

$$N(ay^2+bx^3 \equiv c \ (p)) =$$

$$= \sum_{u+v=c} N(ay^2=u)\,N(bx^3=v)$$

$$= \sum_{u+v=c} N(y^2=a^{-1}u)\,N(x^3=b^{-1}v)$$

$$= \sum_{u+v=c} \left(1+\left(\frac{a^{-1}u}{p}\right)\right)\left(1+\chi(b^{-1}v)+\chi(b^{-1}v)^2\right)$$

$$= p + \sum_{u+v=c} \left(\frac{a^{-1}u}{p}\right) \chi(b^{-1}v) + \dots$$

$$= p + \left(\frac{a^{-1}}{p}\right) \chi(b^{-1}) \sum_{\substack{u+v=c \\ cu'+cv'=c}} \left(\frac{u}{p}\right) \chi(v) + \dots$$

$$= p + \left(\frac{a^{-1}}{p}\right) \chi(b^{-1}) \left(\frac{c}{p}\right) \chi(c) \underbrace{\sum_{u'+v'=1} \left(\frac{u'}{p}\right) \chi(v')}_{\text{la sappiamo!}}$$

$\boxed{\text{Morale}}$ Numero di soluz è p + errore che è $\leq K\sqrt{p}$, $K = \prod(\text{esponenti} - 1)$

Ha senso controllare mod p solo per p "piccolo" (cioè $p - K\sqrt{p} < 0$)

E di solito (Hensel) andare mod p^n non serve a niente

Cosa fare quando tutto fallisce?

$$2y^2 = x^4 - 17$$

1 ✓ Dim che ci sono soluz mod p^n $\forall p$ $\forall n$

2 • Dim che non ci sono soluzioni intere

Moduli: ≤ 7, oppure 17

2 • Idea: combinare informazioni modulo primi diversi con la reciprocità quadratica

Unici primi che ha senso guardare: quelli modulo i quali ci sono solo 2 termini.

Guardiamo modulo un divisore p di y

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

$$= \begin{cases} \left(\frac{q}{p}\right) & \text{se } p \equiv 1\ (4) \text{ o } q \equiv 1\ (4) \\ -\left(\frac{q}{p}\right) & \text{se } p \equiv q \equiv 3\ (4) \end{cases}$$

Sia $p \mid y$. Allora $0 \equiv x^4 - 17 \mod p$

$$\Rightarrow \left(\frac{17}{p}\right) = +1 \overset{RQ}{\Rightarrow} \left(\frac{p}{17}\right) = +1$$

e' se $p=2$?

Quindi $y \equiv z^2 \mod 17$

$$2z^4 \equiv x^4 \quad (\mod 17)$$

Siccome $z \not\equiv 0 \ (17) \Rightarrow 2 \equiv (x/z)^4 \mod 17$

$$\Rightarrow 2^4 \equiv (x/z)^{16} \equiv 1 \quad (17)$$

NON E' VERO! :)

Due equazioni della stessa razza:

$$y^2 = x^3 - x^2 + 8$$

$$y^2 = x^3 + 7$$

Vediamo che la seconda ha soluzione mod p $\forall p$

$$\sum_{x \in \mathbb{F}_p} 1 + \left(\frac{x^3+7}{p}\right) \equiv \sum_{x \in \mathbb{F}_p} (x^3+7)^{\frac{p-1}{2}}$$

$$\equiv \sum_{x} \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} x^{3j} \, 7^{\frac{p-1}{2}-j} \qquad (p)$$

$$\equiv \sum_{j=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{j} 7^{\frac{p-1}{2}-j} \sum_{x \in \mathbb{F}_p} x^{3j} \qquad (p)$$

$$\overset{p \equiv 1 (3)}{\equiv} - \binom{\frac{p-1}{2}}{\frac{p-1}{3}} 7^{\frac{p-1}{6}} \pmod{p}$$

Congruenza + bound di prima $\Rightarrow$ numero esatto!