Esercizi 16 novembre 2020

Eq. 1 $\quad ax^2+bx+c=0$ $\quad \frac{-b\pm\sqrt{b^2-4ac}}{2a}$ $\quad \mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$.

In $\mathbb{Z}_p[x]$ $\quad f=ax^2+bx+c$

$f=0$

Definiamo $\sqrt{\ }$ in $\mathbb{Z}_p$.

Sia $a\in\mathbb{Z}_p$ diciamo che $b\in\mathbb{Z}_p$ è radice quadrata di a se vale $b^2=a$.

Se esiste un tale numero, lo indichiamo $\sqrt{a}$

Osserviamo che se b è radice quadrata di a, anche $p-b$ $(=-b)$ è radice di a

$b^2=a$ $\quad (-b)^2=a$ $\quad (p-b)^2=p^2-2pb+b^2=a$.

In $\mathbb{Z}_p$ $\quad p>2$ $\quad 2\cdot a$ $(a\in\mathbb{Z}_p)$ $\quad a+a$

$2a\neq 0$ $\quad (2\cdot 1)\cdot a=0$ $\quad$ Esiste $(2a)^{-1}$

$ax^2+bx+c\in\mathbb{Z}_p[x]$

$(-b\pm\sqrt{b^2-4ac})(2a)^{-1}$.

$(x-2)(x-3)\in\mathbb{Z}_7[x]$

$x^2+2x+6\in\mathbb{Z}_7[x]$

$b^2 - 4ac = 4 - 4 \cdot 1 \cdot 6 = 4 - 24 = -20 = 1$.

$\sqrt{1}$? 2 numeri di $\mathbb{Z}_7$ al quadrato fanno 1

e sono 1 e -1 o 1 e 6. $\sqrt{b^2-4ac} = \begin{cases} 1 \\ 6 \end{cases}$

$(2 \cdot 1)^{-} = (2)^{-1} = 4$.

$\left(-2 + \begin{cases} 1 \\ 6 \end{cases}\right) \cdot 4 = \begin{cases} (-1) \cdot 4 = -4 = 3 \\ 16 = 2. \end{cases}$

$x^2 + 2x + 6$ ha due radici in $\mathbb{Z}_7[x]$

$x_1 = 3$, $x_2 = 2$.

$ax^2 + bx + c = 0 \quad / \cdot a$

$a^2x^2 + abx + ac = 0$

$a^2x^2 + abx + \frac{b^2}{4} - \frac{b^2}{4} + ac = 0$

$(ax + \frac{b}{2})^2 = \frac{b^2}{4} - ac$

$= \frac{b^2 - 4ac}{4}$ ---

$(ax + u)^2$

$a^2x^2 + 2axu + u^2$

4^{-1} vale in q.g. campo con $\mathrm{ch} \neq 2$

In $\mathbb{Z}_p$ ci possono essere elementi a per i quali esiste la radice quadrata

$b^2 = a$ $\mathbb{Z}_p$ finito

$\{0,1,2,\dots,p-1\} = \mathbb{Z}_p$

$\{k^2 \mid k \in \mathbb{Z}_p\}$ $\quad a \in \mathbb{Z}_p$ $\quad a = p-k$

$k \in \mathbb{Z}_p$ $\quad (-k) \in \mathbb{Z}_p$

non tutti gli elementi di $\mathbb{Z}_p$ hanno $\sqrt{}$.

$\mathbb{Z}_3[x]$ $\quad \{0,1,2\} = \mathbb{Z}_3$

X^2+1
X^2+2
X^2

$a_0 + a_1 x + a_2 x^2$ $\quad a_0, a_1, a_2 \in \mathbb{Z}_3$

$\{0,1,2\} + \{0,1,2\} + \{1,2\} x^2$ $\quad a_2 \neq 0$

18 pol. di grado 2 in $\mathbb{Z}_3[x]$

Se $f = a_0 + a_1 x + \dots + a_n x^n \in K[x]$ $\quad a_n \neq 0$

f irred $\iff$ $(a_n)^{-1} f$ è irred

monico

Monici di $\mathbb{Z}_3[x]$

$0 + 0x + x^2$
$0 + 1x + x^2$
$0 + 2x + x^2$

$1 + 0x + x^2$
$1 + 1x + x^2$
$1 + 2x + x^2$

$2 + 0x + x^2$
$2 + 1x + x^2$
$2 + 2x + x^2$

$f(x) \in K[x]$ $\quad$ t.c. $f(a) = 0$

$f(x) = (x-a)\, g(x)$

$1+x^2$ ha zeri in $\mathbb{Z}_3[x]$.

0 $f(0)=1$
1 $f(1)=2$
2 $f(2)=2$

f

$1+x^2$ è irriducibile in $\mathbb{Z}_3[x]$

Con Ruffini non possiamo dire niente a fattori lineari di pol. di $\mathbb{Z}_p[x]$?

Cerchiamo di capire quanti sono tutti i polinomi monici di grado 2 di $\mathbb{Z}_p[x]$.

p^2 $1+x^2+ax+b$

p^2 pol. di grado 2 monici in $\mathbb{Z}_p[x]$.

Quanti sono i pol. irriducibili monici di $\mathbb{Z}_p[x]$ di grado 2?

Quanti sono i pol riducibili monici di $\mathbb{Z}_p[x]$ di grado 2?

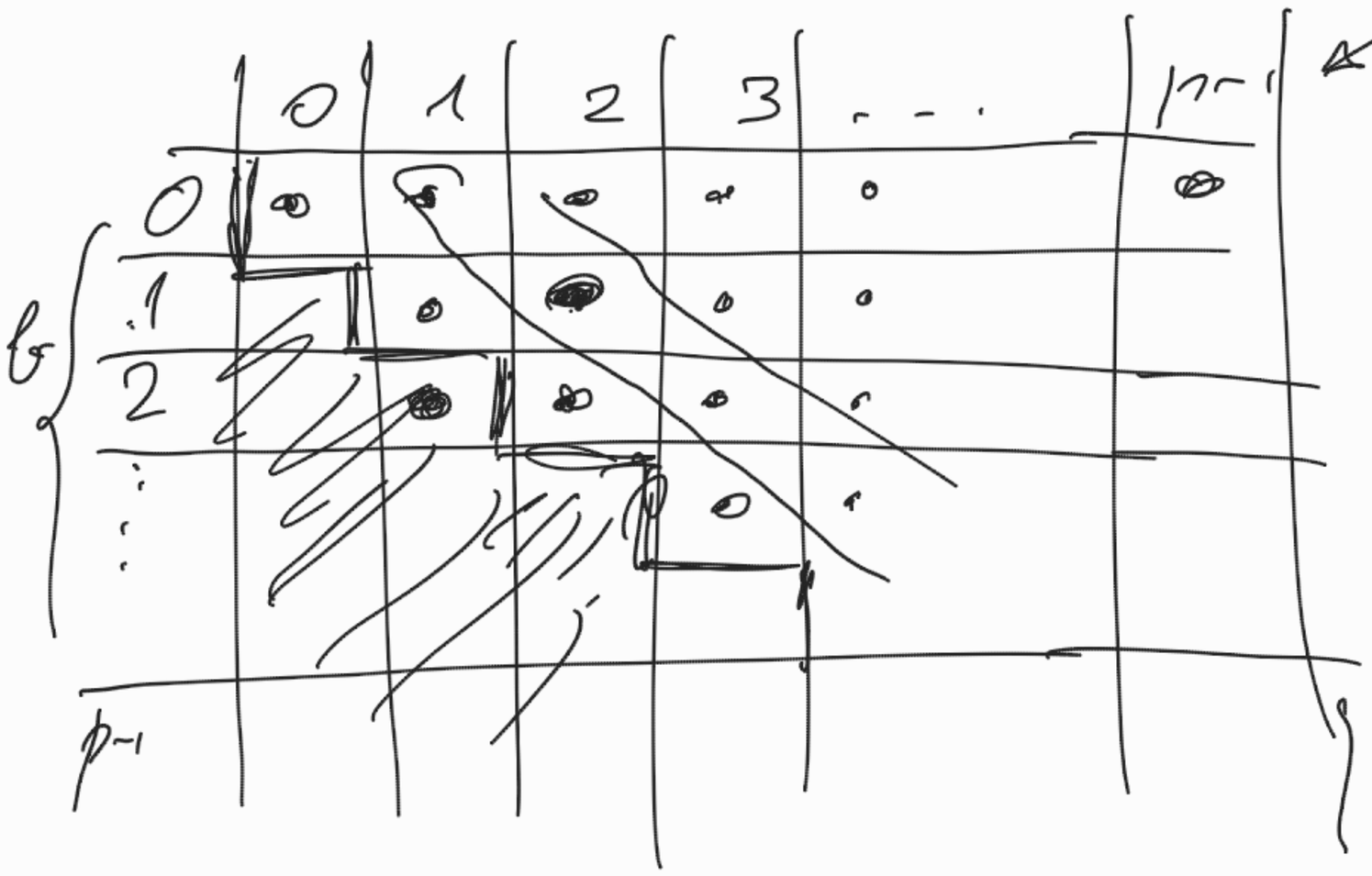
$(x-a)(x-b)$ questo è un pol ridotto di grado 2.

$a \in \mathbb{Z}_p$ $b \in \mathbb{Z}_p$ p^2

$(x-3)(x-2)$

$(x-a)(x-b)$

$(x-2)(x-3)$



$(x-1)(x-2)$

$p + (p-1) + (p-2) + \dots + 1$

$\frac{p(p+1)}{2}$

Pol. resol grado 2 en $\mathbb{Z}_p[x]$ hay $\frac{p(p-1)}{2}$. Hemos

Pol. irred grado 2 hemos de $\mathbb{Z}_p[x]$ hay:

$$p^2 - \frac{p(p-1)}{2} = \frac{2p^2 - p^2 + p}{2} = \boxed{\frac{p(p+1)}{2}}$$

Existe un método para contar todos los pol mónicos irred de $\mathbb{Z}_p[x]$ de grado n.

Problema de saber si un elem de $\mathbb{Z}_p$ es un residuo cuadrático

$\mathbb{Z}_m$. Resolver ecuaciones. Gauss.

Consideramos el siguiente omom de anillos:

$$\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}_p[x]$$

$$a \in \mathbb{Z} \longmapsto [a]$$

$$x \longmapsto x.$$

$$a_0 + a_1 x + \dots + a_n x^n \longmapsto [a_0] + [a_1]x + \dots + [a_n]x^n$$

$\mathbb{Z}[x]$

$f: A \longrightarrow B$ omom de anillos $b \in B$

$\exists!$ omom $F: A[x] \longrightarrow B$ t.q

$F(a) = f(a) \quad \forall a \in A \qquad F(x) = b.$

Prueba $b = x \in B[x]$.

Dado $f: A \to B$ omom ecuk ! omom

$F: A[x] \longrightarrow B[x] \qquad F(a) = f(a) \quad \forall a \in A$

$F(x) = x \in B[x]$.

Consideriamo $\pi : \mathbb{Z} \to \mathbb{Z}_p$ proiezione canonica

$\exists ! \varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ omom. anelli

che estende π e manda x in x.

Prendo un pol $f \in \mathbb{Z}[x]$

d'omom. φ mi può accadere a seconda di

f è riducibile o irriducibile in $\mathbb{Z}_p[x]$ o no in $\mathbb{Z}[x]$?

$\ker \varphi = ?$ $\ker \varphi = \{ p \cdot f \mid f \in \mathbb{Z}[x] \}$

$= (p) \subsetneq \mathbb{Z}[x]$.

Se f è primo primitivo $f \neq 0$ $f \notin \ker \varphi$

Consideriamo

$x^2 + 1 \in \mathbb{Z}[x]$ irriducibile $p = 2$

$\varphi(x^2+1) = (x+1)(x+1)$ in $\mathbb{Z}_2[x]$ riducibile.

$(px+1)(x-1) \in \mathbb{Z}[x]$

riducibile in $\mathbb{Z}[x]$ ma irriducibile in $\mathbb{Z}_p[x]$.

f $\deg f = 2$.

$\deg \varphi(f) = 1$

Sia $f \in \mathbb{Z}[x]$ t.c.

$$\boxed{\deg f = \deg \varphi(f)}$$

Se $\varphi(f)$ è irriducibile, allora f è irriducibile.

Dim Per assurdo:

Sia f riducibile in $\mathbb{Z}[x]$

Cioè: $\exists\ h, g \in \mathbb{Z}[x]$ non costanti, quindi

$\deg h \geq 1$ $\deg g \geq 1$ t.c. $f = hg$.

Consideriamo $\varphi(f)$

$$\varphi(f) = \varphi(h \cdot g) = \varphi(h) \cdot \varphi(g)$$

$\varphi(f)$ è irriducibile

allora o $\varphi(h)$ o $\varphi(g)$ devono essere invertibili

Per esempio $\varphi(h)$ è invertibile.

Che vuol dire invertibile in $\mathbb{Z}_p[x]$?

$\varphi(h)$ è costante $\neq 0$.

$\deg \varphi(h) = 0 \neq 0$

$\deg \varphi(f) = \deg \varphi(h) + \deg \varphi(g)$

$$\deg f \overset{!!}{=} \deg h + \deg g$$

$$\boxed{\deg \varphi(g) = \deg g + \deg h > \deg g}$$

$\boxed{\text{assurdo}}$, perché φ non può far crescere il grado.

Conseguenza Se $\deg \varphi(f) = \deg f$

$\varphi(f)$ irred $\Rightarrow$ f irred.

$x^3 + 2x + 1 \in \mathbb{Z}_3[x]$

$x=0$	1	Il pol. è irred. in $\mathbb{Z}_3[x]$.
$x=1$	1	
$x=2$	1	

Consideriamo il pol irred

$$x^3 + 61452x^2 + 32x + 13 \in \mathbb{Z}[x]$$

$\varphi(-) = x^3 + 2x + 1 \in \mathbb{Z}_3[x]$
