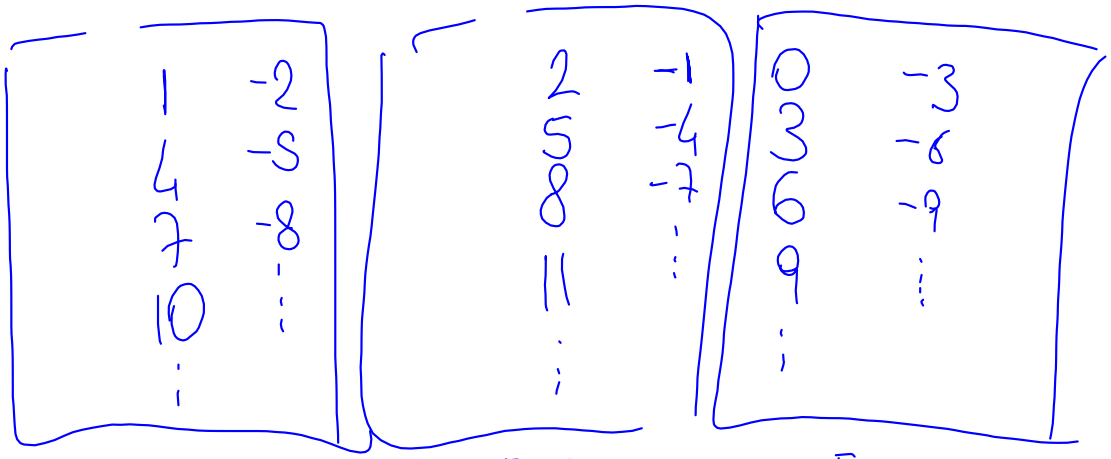
WWW.DI.UNIPI.IT/~FPOLONI

FPOLONI@DI.UNIPI.IT

WWW.DM.UNIPI.IT/~BERARDU

12/12 VEN POMERIGGIO 14-16 AULA D



$[1]$ $[2]$ $[0]$

$[2]\cdot[2]=[1]$

$[1]+[2]=[0]$ $[1]+[1]=[2]$

$1 + 2 \equiv 0 \pmod 3$

$+$: il solito

$\equiv$: definizione nuova

$[1] + [2] = [0]$

$+$: nuove definizioni

$=$: solito

insieme di $\{\ldots -2, 1, 4, \ldots\}$

universo composto da 3 elementi $[0], [1], [2]$

"$+$" va definito "$=$" solito

$\{[0],[1],[2]\} = \mathbb{Z}/(3)$ oppure $\mathbb{Z}/3\mathbb{Z}$ oppure $\mathbb{Z}_3$

$\mathbb{Z}_3$ ambigua

Ho definito somma e prodotto in $\mathbb{Z}/(3)$

$([1]+[1])[2] \stackrel{?}{=} [1]\cdot[2]+[1][2]$

Tutte le proprietà sono da riverificare

(Si verificano, solo noioso)

$\mathbb{Z}/(3)$ è un [anello]

cioè un insieme su cui sono definiti $+, \cdot$

e soddisfano le "proprietà solite"

$\exists\, 0$, e $a+0=a$ $\qquad a+b=b+a$

$\exists\, -a$, $\quad -a+a=0$

Funziona con ogni modulo, es. $\mathbb{Z}/(6)$

$$\frac{\mathbb{Z}}{(6)} = \{[0], [1], [2], [3], [4], [5]\}$$

"ring of integers modulo 6"

In un anello non valgono: $[1] \leq [2]$

- disuguaglianze

$1 \leq 2$

$4 \leq 2$???

Succedono cose strane $[1]+[1]+[1]+[1]+[1]+[1] = [0]$

$[1]\cdot[2]=[4]\cdot[2]$ (in $\mathbb{Z}/(6)$)

ma $[1]\neq[4]$

Perché? Semplificare $\Leftrightarrow$ moltiplicare per un inverso

$\frac{1}{3a}\,3a^2=3ab\,\frac{1}{3a} \Rightarrow a=b$

E in $\mathbb{Z}/(6)$ non tutti i numeri hanno inverso...

Quando possiamo semplificare? Quando il modulo è primo

Es mod 3

$$[2]^{-1}[1]\cdot[2]=[1]\cdot[2]\,[2]^{-1}$$

In $\mathbb{Z}/(3)$ posso fare somme, prodotti e divisioni (e inversi)

Un insieme su cui sono definite queste cose si chiama campo (ing. field)

"Tabelline"

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	1	2	3	4	5
[2]	[0]	2	4	0	2	4
[3]	[0]	3	0	3	0	3
[4]	[0]	4	2	0	4	2
[5]	[0]	5	4	3	2	1

$[0]$ $[1]$ $[2]$

---

in $\mathbb{Z}/(7)$ $\qquad \frac{[3]}{[4]} = [3]\cdot[4]^{-1} = [3]\cdot[2] = [6]$

$$(1-a^{n+1}) = (1-a)(1+a+a^2+\dots+a^n)$$

Vera anche in $\mathbb{Z}/(m)$

$$\frac{1-a^{n-1}}{1-a} = 1+a+\dots+a^n \quad \forall\, a \neq 0$$ ← vera in $\mathbb{Z}/(p)$

Quante soluzioni ha $[3]x-[2]=0$ in $\mathbb{Z}/(5)$?

$[2]\cdot[3]x=[2]\cdot[2] \iff x=[4]$

$[3]x-[2]=0$ ha una sola soluzione

cercheremo di vedere in futuro che un'equazione di grado d ha al più d soluzioni

uint16 è $\mathbb{Z}/(65536)$

```
uint16 a = 65534;
uint16 b = 2;
printf("%d", a+b)   ← scrive 0
```

Cifre di controllo sui codici a barre

$8\,7\,2\,1\,2\,0$

aggiungo in fondo

$[8]+[7]+[2]+[1]+[2]=[0]$

mod 10

$8\,7\,3\,1\,2\,0$

$8+7+3+1+2 \neq 0$

c'è stato un errore!

Aggiungendo un carattere, trovo tutti gli errori

Questo metodo trova qualche errore, non tutti

Es 871220 passa! $8+7+2+1+2 \equiv 0$

870320 passa!

Con questo metodo tutti gli errori su esattamente una cifra non possono inosservati

Dim:

$$a+b+c+d+e = a+b+c'+d+e$$
$$\Updownarrow$$
$$c = c'$$

4548718726752

significato — cifra di controllo

Proprietà: se sommo le cifre con coefficienti 1 e 3 alternativamente mod 10

$1\cdot 4 + 3\cdot 5 + 1\cdot 4 + 3\cdot 8 + 1\cdot 7 + 3\cdot 1 + 1\cdot 8 + 3\cdot 7 + 1\cdot 2 + 3\cdot 6 + 1\cdot 7 + 3\cdot 5 + 1\cdot 2 \equiv 0$

$\equiv 1(4+4+7+8+2+7+2) + 3(5+8+1+7+6+5) \equiv$

$\equiv 1\cdot 4 + 3\cdot 2 \equiv 0$

il risultato deve fare 0 mod 10 (*)

Quindi la cifra di controllo in fondo è scelta in modo che (*) valga

$$18+30+11+31+16+38+18+30+15+31+11+35+16 =$$

$$1\cdot(8+1+6+8+5+1+6)+3\cdot(0+1+8+0+1+5)=$$

$$= 1\cdot 5 + 3\cdot 5 \equiv 0 \pmod{10} \quad =)$$

---

lezione venerdì? Vi faccio sapere domattina su www.di.unipi.it/~fpoloni

$$p(x) = p_0 x^0 + p_1 \cdot x + p_2 \cdot x^2 + \dots + p_n x^n = \sum_{j=0}^{n} p_i x^i \qquad (x^0 = 1)$$

Dove vivono i p_i?

$p(x) = 1 \cdot x + 2 \cdot x^2 + 3$ coefficienti interi

$p(x) = -1.5 + 3x + \pi x^2$ coeff. reali

Basta che siano tutti elementi dello stesso anello

Posso fare polinomi a coeff. interi modulo 3:

$p(x) = [1]\cdot x + [2]$ $\quad q(x) = [1]\cdot x^2 + [0]\cdot x + [2]$

$p(x)\cdot q(x) = (x+[2])\cdot(x^2+[2]) = x^3 + [2]x^2 + [2]x + [1]$

↳ operazioni mod 3!

Def somma di polinomi, prodotto di polinomi

$p(x) = \sum_{i=0}^{n} p_i x^i$ $\quad q(x) = \sum_{i=0}^{m} q_i x^i$ (n, m diversi in gen.)

↳ posso "allungare" con zeri

$p_0 + p_1 x + p_2 x^2 + p_3 x^3$ $\quad q_0 + q_1 x + 0\cdot x^2 + 0\cdot x^3$

$$p(x)+q(x) \overset{\text{def}}{=} \sum_{i=0}^{\max(m,n)} (p_i+q_i)x^i$$

con la convenzione che i termini più alti che mancano sono zeri

$$p(x)q(x) = \sum_{i=0}^{m+n} \sum_{j=0}^{i} p_{i-j}q_j x^i$$

$$(p_0+p_1x+p_2x^2)(q_0+q_1x+q_2x^2) = p_0q_0 + (p_1q_0+p_0q_1)x + (p_2q_0+p_1q_1+p_0q_2)x^2 + \dots$$

struct polinomio { ..? }

Basta avere l'array dei coefficienti

Polinomio = array coefficienti + "+" e "*" definiti in modo strano

Proprietà "solite" di +, * discendono da quelle dei coefficienti

→ Anche i polinomi sono un anello

$\mathbb{Z}[x] = \{$ polinomi a coefficienti interi $\}$

$\mathbb{R}[x] = \{$ polinomi a coeff. reali $\}$

$\mathbb{Z}_{(3)}[x] = \{$ poly. a coeff. in $\mathbb{Z}_{(3)}\}$

---

grado di un polinomio: è

$$\deg p(x) := \max \{ i : p_i \neq 0 \}$$

$$\deg \left([1] + [2]x + [1]x^2 \right) = 2$$

$$\deg\left([1]+[2]\cdot x+[0]\cdot x^2\right)=1$$

$$\deg\left(p_0+p_1x+p_2x^2\right)=2 \quad \underline{\text{solo se}} \quad p_2\neq 0$$

Comportamento del grado rispetto a somme/prodotti:

$$\deg\left(p(x)+q(x)\right) \leqslant \max\left(\deg p(x), \deg q(x)\right)$$

↑ occhio

$$\deg\left(\left(1+2x+3x^2\right)+\left(-5+4x-3x^2\right)\right)=1$$

$$\deg\left(p(x)\cdot q(x)\right) \leq \deg p(x) + \deg q(x)$$

Occhio! Esempio:

$$\deg\left[\left(1+2x^3\right)\left(2+3x^5\right)\right] = 8$$

$\mathbb{Z}/(6)[x]$ $\quad \left(1+[2]x^3\right)\left([2]+[3]x^5\right) = \ldots \underbrace{[2][3]}_{\|}x^3\cdot x^5$

$[0]$

(In un campo, vale =)

Qual è $\deg(0)$?

Le proprietà di prima (somma, prodotto...) valgono se definiamo $\deg(0) = -\infty$ o $\deg(0) = 0$

In generale, fate attenzione a definizione precisa

Divisione tra polinomi

$4x^3+6x^2-8x+1 : 2x^2 = 2x+3$ con resto $-8x+1$

Come sugli interi, le divisioni non sono esatte, c'è resto

interi: Per ogni $a, b \neq 0$ $\exists$ q, r tali che

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|$$

polinomi: Per ogni $a(x), b(x) \neq 0$ $\exists$ $q(x), r(x)$

tali che $a(x) = b(x)q(x) + r(x)$

(oppure $r(x) = 0$) $\longrightarrow \deg r(x) < \deg(b(x))$