Esercizi Algebra, Informatica, corso A

Massimo Caboara

Lezione del 24 Febbraio 2005

Equazioni Polinomiali in $\mathbb{Z}_p$

1. Quante soluzioni ha l'equazione $x^5 + 1 = 0$ in $\mathbb{Z}_2$?.
   Usando il piccolo teorema di Fermat, abbiamo che $x^2 = x$ come funzioni su $\mathbb{Z}_2$. Quindi $x^5 + 1 = x + 1$ come funzioni su $\mathbb{Z}_2$ e la soluzione è 1.
   Altro ragionamento: $x^5 + 1 = (x + 1)^5$ e quindi 1 è soluzione quintupla.
   Allora la soluzione è semplice o quintupla?

2. Risolvere un eqazione di secondo grado in $\mathbb{Z}_2$.
   La forma generale è $x^2 + bx + c = 0$. Dato che $\mathbb{Z}_2 = \{0, 1\}$ come insieme, ci sono soltanto quattro equazioni

   (a) $x^2 = 0$ che ha come soluzione 0, doppia.
   (b) $x^2 + x = 0 \Rightarrow x(x + 1) = 0$ che ha come soluzioni $0, 1$.
   (c) $x^2 + 1 = (x + 1)^2$ che ha come soluzione $-1 = 1$, doppia.
   (d) $f(x) = x^2 + x + 1 = 0$ che non ha soluzioni in $\mathbb{Z}_2$. Per vederlo base controllare che $f(1) = f(0) = 1 \neq 0$.

   Altro metodo: Usando il piccolo teorema di Fermat, abbiamo che $x^2 = x$ copme funzione $\mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$. Quindi da $x^2 + bx + c = 0$ si ha $x(b+1) + c = 0$ la cui soluzione è

   - $-\dfrac{c}{b+1}$ se $b + 1 \neq 0 \Leftrightarrow b \neq 1$

   Se $b = 1$, ci riduciamo all'identità $c = 0$, che è soddisfatta solo da $c = 0$. Controllare che le soluzioni cosí ottenute sono equivalenti alle soluzioni trovate col primo metodo, a meno della molteplicità, ovviamente.

3. Risolvere l'eqazione $x^2 + 5x - 3 = 0$ in $\mathbb{Z}_{11}$.
   Usiamo la formula. Le soluzioni sono

$$\frac{-5 + \sqrt{25 + 4 * 3}}{2} = \frac{-5 + \sqrt{37}}{2}$$

Sappiamo che, in $\mathbb{Z}_{11}$, $-5 = 6$, $\frac{1}{2} = 6$ e $\sqrt{37} = \sqrt{4} = \{-2, +2\}$. Quindi le soluzioni sono $\frac{6+2}{2} = 4 = 8 * 6$ e $\frac{6-2}{2} = 2 = 4 * 6$.

4. Calcolare l' inverso di a in $\mathbb{Z}_p$.
   Se $a = 0$ l'inverso non esiste, se $a = 1$ l'inverso è banale 1. Per gli altri casi stiamo cercando $x \in \mathbb{Z}_p$ tale che $ax = 1$. L'esistemza di tale x è garantita dal fatto che $\mathbb{Z}_p$ è un campo.

   (a) Primo metodo: calcoliamo $a * x$ per ogni $x \in \mathbb{Z}_p$. Quando abbiamo trovato x tale che $ax = 1$, abbiamo provato che x è l'inverso di a.

   (b) Secondo metodo: trovare $x \in \mathbb{Z}_p$ tale che $ax = 1$ in $\mathbb{Z}_p$ equivale a trovare un $x \in \mathbb{Z}$ tale che esista $y \in \mathbb{Z}$ per cui si abbia $ax - py = 1$. Questa equazione diofantea ha sempre soluzioni in quanto $(a, p) = 1$.

   (c) Terzo metodo: Usiamo il fatto che $a^{p-1} = 1$ per il piccolo teorema di Fermat. Quindi $aa^{-2} = 1$ da cui $a^{-1} = a^{p-2}$. Rimane il problema di calcolare efficacemente a^{p-2} per alti valori di p, a. Una possibile soluzione è la seguente:
   Esempio: calcolo dell inverso di 5 in $\mathbb{Z}_{11}$. $5^{-1} = 5^9 = 5^2 \cdot 5^2 \cdot 5^2 \cdot 5^2 \cdot 5 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 = 81 \cdot 5 = 4 \cdot 5 = 20 = 9$
   Scrivere formalmente l'algoritmo per il terzo metodo.
   Implementare i tre metodi e controllare la complessità pratica su un certo numero di esempi
   Scrivere la complessità dei tre esempi.

5. Un equazione di secondo grado in $\mathbb{Z}_p$ ha zero o due soluzioni contate con la loro molteplicità.
   Sia $f(x) = 0$ la nostra equazione generica. Dato che $\mathbb{Z}_2$ è un campo, $f(x) = 0$ ha al piú due soluzioni. Supponiamo che abbia una soluzione, cioè che esita $a \in \mathbb{Z}_p$ tale che $f(a) = 0$. Allora per l'algoritmo euclideo $(x - a) \mid f(x)$, il che equivale a dire che $\exists\ g(x) \in ZZ_p$ tale che $f(x) = (x - a)g(x)$. Ma il grado di $g(x)$ è forzatamente 1, e tutte le equazioini di primo grado su un campo hanno un unica soluzione. Quindi esiste $b \in \mathbb{Z}_p$ tale che $g(b) = 0$. Ma allora $f(b) = (b - a)g(b) = 0$ e quindi b è soluzione anche di $f(x)$. Quindi se $f(x)$ non può avere una sola soluzione *contata con la propria molteplicità*. Puó infatti succedere che $a = b$ nel ragionamento precedente.

6. Trovare le radici di $x^2 = 0$ in $\mathbb{Z}_{36}$
   Dimostriamo che gli elementi dell'insieme $\{6k \mid k : 0 \ldots 5\}$ sono soluzioni. Infatti $(6k)^2 = 36k^2 = 0$.
   Provare che sono le uniche soluzioni.

Numeri complessi

7. Calcolare l'inverso di $3+2i$
   Dato che $(3+2i)(3-2i) = (9+4) = 13$ abbiamo che
$$\frac{(3+2i)(3-2i)}{13} = \frac{13}{13} = 1$$
   da cui si ricava
$$(3+2i)^{-1} = \frac{3-2i}{13}$$

8. Calcolare l'inverso di $a+ib$, $a, b \in \mathbb{R}$.

9. Calcolare $| \, 5+4i \, |$.

10. Calcolare $(3-i)(1+2i), (3-i)+(4-2i), \dfrac{1+i}{i-i}$.

11. Calcolare $(1+i\sqrt{3})^{2005}$.
    Portiamo in nostro numero complesso dalla forma $a+ib$ alla forma $\rho e^{i\theta} = \rho(\cos\theta + i\sin\theta)$. Usando le formule

    - $\rho = \sqrt{a^2+b^2}$
    - $\begin{cases} \rho\sin\theta = b \\ \rho\cos\theta = a \end{cases} \Rightarrow \theta = \arctan\frac{b}{a}$

    ricaviamo $\rho = 2$, $\theta = \frac{\pi}{3}$. Allora $(1+i\sqrt{3})^{2005} = (2e^{i\frac{\pi}{3}})^{2005} = 2^{2005}e^{i\frac{2005\pi}{3}} = 2^{2005}e^{i668\pi}e^{\frac{\pi}{3}} = 2^{2005}e^{0}e^{\frac{\pi}{3}} = 2^{2005}e^{\frac{\pi}{3}}$
    Volendo ritrasformare quest'ultimo numero in forma cartesiana, notiamo che $e^{\frac{\pi}{3}} = (1+i\sqrt{3})$. Quindi $(1+i\sqrt{3})^{2005} = 2^{2005} + i2^{2005}\sqrt{3}$. Notare che esponenziando $1+i\sqrt{3}$ per 2005 il modulo cambia ma l'argomento rimane invariato.

12. Calcolare $\sqrt[4]{1}$ in $\mathbb{C}$.
    Dato che le radici quarte di 1 in $\mathbb{C}$ sono tutte e sole le soluzioni dell'equazione $x^4 = 1$, per il teorema fondamentale dell'algebra sappiamo che $\sqrt[4]{1}$ ha quattro elementi. La formula per il calcolo delle radici complesse è
$$\sqrt[n]{\rho e^{i\theta}} = \{ \sqrt[n]{\rho} e^{\frac{\theta+2k\pi}{n}} \mid k \in 0 \dots n-1\}$$
    Abbiamo quindi
$$\sqrt[4]{1e^{i0}} = \{1 \cdot e^{\frac{0+2k\pi}{4}} \mid k \in 0 \dots 3\}$$
    Le quattro soluzioni sono quindi e^0, $e^{\frac{\pi}{2}}$, e^{π}, $e^{\frac{3\pi}{2}}$, vale a dire 1, i, -1, $-i$. Notare che sul piano cartesiano questi numeri formano un quadrato.

- Altri esercizi sui numeri complessi si possono trovare sull Abate o in qualunque testo elementare di Geometria e Analisi.

Comunicare ogni errore a `caboara@dm.unipi.it`