ALGEBRA 1 — Primo esame scritto
4 Luglio 2011
soluzioni

(1) Si trovino tutte le soluzioni intere del sistema di congruenze lineari

$$\begin{cases} x \equiv & 4 & \mod 5 \\ 2x \equiv & 5 & \mod 7 \\ 3x \equiv & 12345^{2448} & \mod 9 \end{cases}$$

Soluzione: L'inverso di 2 modulo 7 è 4. Moltiplicando per 4 la seconda congruenza si ottiene $x \equiv 6 \mod 7$. Per quanto riguarda la terza congruenza, $12345 \equiv 6 \mod 9$, e $12345^2 \equiv 36 \equiv 0 \mod 9$. Pertanto ogni potenza superiore di 12345 è congrua a 0, e la terza congruenza si riduce a $3x \equiv 0 \mod 9$ o, equivalentemente, $x \equiv 0 \mod 3$. Il sistema nella sua forma normale è quindi:

$$\begin{cases} x \equiv & 4 & \mod 5 \\ x \equiv & 6 & \mod 7 \\ x \equiv & 0 & \mod 3 \end{cases}$$

A questo punto, è facile trovarne le soluzioni. Ad esempio, -1 è soluzione delle prime due congruenze, che possono essere sostituite da $x \equiv -1 \mod 35$ per il teorema cinese del resto. E' ora sufficiente trovare un numero della forma $-1 + 35k$ che sia multiplo di 3, come ad esempio 69. Sempre per il teorema cinese del resto, sono allora soluzioni del sistema tutti gli interi $x \equiv 69 \mod 105$.

NB: il teorema di Eulero-Fermat permette di concludere che $a^{\phi(n)} \equiv 1 \mod n$ quando $\mathrm{MCD}(a, n) = 1$, e quindi NON IN QUESTO CASO! In effetti, $12345 \equiv 6 \mod 9$ e quindi $\mathrm{MCD}(12345, 9) = 3$.

(2) Determinare la cardinalità dei seguenti insiemi:

$$A = \{(x, y) \in \mathbb{R}^2 \mid x + y\sqrt{2} \in \mathbb{Q}\}$$
$$B = \{(x, y) \in \mathbb{R}^2 \mid \text{sia } x + y\sqrt{2} \text{ che } x - y\sqrt{2} \text{ appartengono a } \mathbb{Q}\}$$

Soluzione: Entrambi gli insiemi sono contenuti in $\mathbb{R}^2$, e la loro cardinalità è quindi al più quella del continuo. Per quanto riguarda A, l'applicazione $f : \mathbb{R} \to A$ definita da $f(a) = (-a\sqrt{2}, a)$ è iniettiva, e quindi $|A| \geq |\mathbb{R}|$. Di conseguenza, $|A| = |\mathbb{R}|$.

L'insieme B è invece molto più piccolo. Se $x \pm y\sqrt{2} \in \mathbb{Q}$, sommando e sottraendo si ottiene $2x, 2y\sqrt{2} \in \mathbb{Q}$, e quindi $x, y\sqrt{2} \in \mathbb{Q}$. Ma allora l'applicazione $g : \mathbb{Q} \times \mathbb{Q} \to B$ definita da $g(a, b) = (a, b/\sqrt{2})$ è suriettiva, mentre la sua iniettività è evidente. In altre parole, $|B| = |\mathbb{Q}^2|$ e quindi B è numerabile

(3) Verificare che il polinomio $x^4 + x - 1$ è irriducibile in $\mathbb{Q}[x]$.

Sia $\pi : \mathbb{Q}[x] \to \mathbb{Q}[x]/(x^4 + x - 1)$ la proiezione canonica. Spiegare per quale motivo l'elemento $\pi(x^2 + x - 1)$ possieda un inverso in $\mathbb{Q}[x]/(x^4 + x - 1)$, e determinare tale inverso.

Soluzione: Il modo più semplice per ottenere l'irriducibilità di $f(x) = x^4+x-1$ è osservare che la sua riduzione modulo 2 è irriducibile (abbiamo scritto a lezione l'elenco completo di tutti i polinomi irriducibili di quarto grado in $\mathbb{F}_2[x]$). Essendo $f(x)$ primitivo, è allora irriducibile in $\mathbb{Z}[x]$, e quindi anche in $\mathbb{Q}[x]$ per una delle tante forme del Lemma di Gauss.

Alternativamente, si vede che $f(x)$ non ha radici razionali (possono essere soltanto ± 1, che non soddisfano $f(x)$) e poi si mostra per forza bruta che $f(x)$ non si spezza nel prodotto di due polinomi di secondo grado.

Essendo $f(x)$ irriducibile, il quoziente $\mathbb{Q}[x]/(f(x))$ è un campo, e quindi ogni suo elemento non nullo – ad esempio $[x^2 + x - 1]$ – possiede un inverso. Il calcolo esplicito dell'inverso si può fare eseguendo l'algoritmo euclideo per il calcolo dell'identità di Bézout. Si ha:

$$x^4 + x - 1 = (x^2 - x + 2) \cdot (x^2 + x - 1) - (2x - 1)$$
$$x^2 + x - 1 = \left(\frac{1}{2}x + \frac{3}{4}\right) \cdot (2x - 1) - \frac{1}{4},$$

da cui

$$\begin{aligned}
1 &= 4 \cdot \frac{1}{4} \\
&= 4\left(\frac{1}{2}x + \frac{3}{4}\right) \cdot (2x - 1) - 4 \cdot (x^2 + x - 1) \\
&= (2x + 3) \cdot (2x - 1) - 4 \cdot (x^2 + x - 1) \\
&= (2x + 3) \cdot \big((x^2 - x + 2) \cdot (x^2 + x - 1) - (x^4 + x - 1)\big) - 4 \cdot (x^2 + x - 1) \\
&= \big((2x + 3)(x^2 - x + 2) - 4\big) \cdot (x^2 + x - 1) - (2x + 3)(x^4 + x - 1) \\
&= (2x^3 + x^2 + x + 2) \cdot (x^2 + x - 1) - (2x + 3)(x^4 + x - 1).
\end{aligned}$$

Concludiamo che $[2x^3 + x^2 + x + 2]$ è l'inverso di $[x^2 + x - 1]$.

(4) Dire se l'anello quoziente $\mathbb{Z}[i]/(7+i)$
- sia un campo;
- sia un dominio d'integrità;
- possieda elementi nilpotenti diversi da $[0]$.

Soluzione: La norma euclidea di $7+i$ è $50 = 2 \cdot 5^2$. Pertanto, nella fattorizzazione di $7+i$ in primi di $\mathbb{Z}[i]$ sono presenti due primi di norma 5 ed uno di norma 2. Provando a dividere $7+i$ per $2 \pm i$, si ottiene facilmente la fattorizzazione $7+i = (1-i)(2+i)^2$.

Le tre domande sono equivalenti a chiedere se $7+i$ sia irriducibile, primo, privo di fattori primi multipli; il quoziente $A = \mathbb{Z}[i]/(7+i)$ non è quindi né un campo, né un dominio d'integrità, e possiede nilpotenti non banali.

Più esplicitamente, $[1-i][(2+i)^2] = [0]$, e quindi A non è un dominio d'integrità. Di conseguenza, non può nemmeno essere un campo. L'elemento $[(1-i)(2+i)]$ è diverso da $[0]$, ma il suo quadrato $[(1-i) \cdot (1-i)(2+i)^2]$ è uguale a $[0]$.

(5) Sia $N \subset \mathbb{Z}^3$ lo $\mathbb{Z}$-sottomodulo generato dagli elementi $(4,2,2),(6,6,3),(5,5,5)$.
- Quanti elementi possiede N?
- Quanti elementi possiede $\mathbb{Z}^3/N$?

Soluzione: Applicando l'algoritmo di raddrizzamento al sottomodulo N, si ottiene:

$$\begin{pmatrix} 4 & 6 & 5 \\ 2 & 6 & 5 \\ 2 & 3 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 4 & 1 & 5 \\ 2 & 1 & 5 \\ 2 & -2 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 4 & 5 \\ 1 & 2 & 5 \\ -2 & 2 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 1 & -2 & 0 \\ -2 & 10 & 15 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 10 & 15 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & -5 & 15 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 5 & 15 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 15 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 15 \\ 0 & 2 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 15 \\ 0 & 0 & -30 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -30 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 30 \end{pmatrix}.$$

Esiste quindi un'applicazione $\mathbb{Z}$-lineare invertibile $f : \mathbb{Z}^3 \to \mathbb{Z}^3$ tale che $f(N) = (1) \oplus (1) \oplus (30)$. Si vede subito che N è infinito, mentre $M/N \simeq \mathbb{Z}/(30)$ possiede 30 elementi.