ALGEBRA 1 — Secondo esame scritto
soluzioni
18 Luglio 2011

(1) Risolvere il seguente sistema di congruenze lineari:

$$\begin{cases} 3x \equiv 15 \mod 21 \\ 44x \equiv 20 \mod 12 \\ 6x \equiv 6^{1000} \mod 15 \end{cases}$$

Soluzione: Richiedere la validità della congruenza $3x \equiv 15 \mod 21$ è equivalente ad affermare che $21 = 3 \cdot 7$ divide $3x - 15 = 3(x-5)$. Per il teorema di fattorizzazione unica, questo accade esattamente quando 7 divide $x - 5$. Possiamo quindi *semplificare* il fattore 3 in comune ed ottenere la congruenza equivalente $x \equiv 5 \mod 7$. Si può procedere nello stesso modo con la seconda congruenza, che diventa $11x \equiv 5 \mod 3$, cioè $2x \equiv 2 \mod 3$, da cui, cambiando segno, si ottiene $x \equiv 1 \mod 3$.

Prima di procedere con la terza congruenza, dobbiamo calcolare $6^{1000} \mod 15$ o trovare una maniera per renderne inutile il calcolo. Il calcolo di $6^{1000} \mod 15$ si può fare in molti modi: si può ad esempio notare che $6^2 = 36 \equiv 6 \mod 15$ e concludere – con una facile induzione che siete sicuramente in grado di scrivere – che $6^n \equiv 6 \mod 15$ per ogni $n \geq 1$. Alternativamente, si può calcolare 6^{1000} modulo 3 e 5, e poi ricomporre le informazioni modulo 15 con il Teorema cinese del resto. Ad ogni modo, il calcolo delle potenze di 6 modulo 3 e 5 è semplice, in quanto $6 \equiv 1 \mod 5$, $6 \equiv 0 \mod 3$. Si ottiene quindi $6^n \equiv 1 \mod 5$, $6^n \equiv 0 \mod 3$ per ogni $n \geq 1$, da cui ancora $6^n \equiv 6 \mod 15$.

In effetti, però, si può eliminare del tutto il calcolo delle potenze di 6: la terza delle congruenze proposte si può spezzare modulo 3 e modulo 5. Si ottengono $0 \cdot x \equiv 0 \mod 3$, che è sempre verificata e può essere eliminata, e $x \equiv 1 \mod 5$ che impone invece una condizione non banale. In qualunque modo si sia deciso di procedere, si giunge al sistema equivalente

$$\begin{cases} x \equiv 5 \mod 7 \\ x \equiv 1 \mod 3 \\ x \equiv 1 \mod 5 \end{cases}$$

che si risolve nei soliti modi. Si vede subito che $x = 61$ è una soluzione del sistema dato, che è unica modulo $105 = 3 \cdot 5 \cdot 7$, ancora per il Teorema cinese del resto.

(2) Si determini la cardinalità dei seguenti insiemi:
- $A = \{f(x) \in \mathbb{Q}[x] \mid f(\sqrt{2}) \text{ è irrazionale}\}$;
- $B = \{f(x) \in \mathbb{R}[x] \mid f(2) \text{ è razionale}\}$.

Soluzione:
- Abbiamo mostrato a lezione che l'insieme $\mathbb{Q}[x]$ è numerabile; essendone A un sottoinsieme, deve essere al più numerabile. Bisogna stabilire, adesso, se A è finito o infinito: in quest'ultimo caso è almeno numerabile, ed abbiamo quindi concluso.
  Si vede facilmente che tutti i polinomi della forma $x + q, q \in \mathbb{Q}$ sono a coefficienti razionali ed assumono in $\sqrt{2}$ valori irrazionali. Questo mostra che A è infinito, e quindi numerabile.
- Possiamo procedere come con $\mathbb{Q}[x]$ per mostrare come la cardinalità di $\mathbb{R}[x]$ coincida con quella di $\mathbb{R}$. In effetti, i polinomi a coefficienti in $\mathbb{R}$ di grado minore o uguale di d sono in corrispondenza biunivoca (leggendone i coefficienti) con $\mathbb{R}^{d+1}$, che possiede la stessa cardinalità di $\mathbb{R}$; l'insieme $\mathbb{R}[x]$ è allora unione numerabile di insiemi che hanno tutti cardinalità $\mathbb{R}$, e possiede quindi anch'esso la stessa cardinalità di $\mathbb{R}$. Essendone B un sottoinsieme, otteniamo subito $|B| \leq |\mathbb{R}|$.
  Mostriamo adesso che $|B| \geq |\mathbb{R}|$. L'applicazione $\mathbb{R} \ni a \mapsto a(x-2) \in \mathbb{R}[x]$ associa a ciascun numero reale un polinomio a coefficienti reali che, calcolato in 2, produce il numero razionale 0. Abbiamo pertanto costruito un'applicazione (iniettiva) $\mathbb{R} \to B$, e quindi $|\mathbb{R}| \leq |B|$. In conclusione, $|\mathbb{R}| \leq |B| \leq |\mathbb{R}|$ e quindi $|B| = |\mathbb{R}|$.

(3) Determinare per quali valori di $a \in \mathbb{Z}_p$, il polinomio $x^2 - 3x + a$ sia riducibile in $\mathbb{Z}_p[x]$, nei casi $p = 3, 7, 11$.

Soluzione: In tutti e tre i casi, dobbiamo stabilire l'irriducibilità di polinomi di grado 2 a coefficienti in un campo. Si tratta pertanto di stabilire se i polinomi in questione abbiano o meno fattori di primo grado, il che equivale a stabilire se possiedano radici nel campo. Vediamo i tre casi in dettaglio.

- $p = 3$. Il polinomio $x^2 - 3x + a$ assume su $\mathbb{Z}/(3)$ i valori $a, a + 1, a + 1$ e quindi è riducibile non appena uno di tali valori sia zero, cioè quando $a \equiv 0, 2 \mod 3$.
- $p = 7$. Il polinomio $x^2 - 3x + a$ assume su $\mathbb{Z}/(7)$ i valori $a, a-2, a-2, a, a-3, a-4, a-4$, ed è quindi riducibile quando $a \equiv 0, 2, 3, 4 \mod 7$.
- $p = 11$. I valori assunti da $x^2 - 3x + a$ su $\mathbb{Z}/(11)$ sono $a, a-2, a-2, a, a-7, a-1, a-4, a-5, a-4, a-1, a-7$. Si ha riducibilità quando $a \equiv 0, 1, 2, 4, 5, 7 \mod 11$.

(4) Vero o Falso (con dettagliate spiegazioni):
(a1) 7981 è un MCD di $3x+1$ e $5x$ in $\mathbb{Z}[X]$
(a2) 7981 è un MCD di $3x+1$ e $5x$ in $\mathbb{Q}[X]$
(b1) $3x$ è un MCD di $13x^2$ e x in $\mathbb{Z}[X]$
(b2) $3x$ è un MCD di $13x^2$ e x in $\mathbb{Q}[X]$
(c1) $x-2$ è un MCD di x^3+2x^2-x-2 e x^3-8 in $\mathbb{Z}[X]$
(c2) $x-2$ è un MCD di x^3+2x^2-x-2 e x^3-8 in $\mathbb{Q}[X]$.

Soluzione: Nell'esercizio si parla di *un* massimo comun divisore, e non del massimo comun divisore, poiché, in un dominio d'integrità, il massimo comun divisore di due elementi dati, quando esiste, è unico a meno di moltiplicazione per un elemento invertibile. Ricordiamo che gli invertibili dell'anello $\mathbb{Q}[x]$ sono tutte e sole le costanti non nulle, mentre gli unici invertibili di $\mathbb{Z}[x]$ sono ± 1.

(a1) Si vede subito che 7981 non divide né $3x+1$, né $5x$, altrimenti ne dividerebbe i coefficienti. Non può esserne, pertanto, massimo comun divisore.

(a2) I polinomi $3x+1$ e $5x$ sono entrambi irriducibili in $\mathbb{Q}[x]$. Non essendo associati, si ha $\mathrm{MCD}(3x+1,5x)=1$. Essendo 7891 e 1 associati, anche 7981 è un loro massimo comun divisore.

(b1) $3x$ non divide x, e non può quindi essere un massimo comun divisore di x e $13x^2$.

(b2) Un massimo comun divisore di x e $13x^2$ si può calcolare con l'algoritmo euclideo, oppure ricavare dalle (ovvie) fattorizzazioni in irriducibili dei due polinomi. Si ha $\mathrm{MCD}(x,13x^2)=x$ e quindi anche $3x$, che si ottiene da x moltiplicandolo per l'invertibile 3, è un massimo comun divisore.

(c1) E' facile calcolare le fattorizzazioni esplicite dei due polinomi in irriducibili di $\mathbb{Z}[x]$. Si ha: $x^3-8=(x-2)(x^2+2x+4), x^3+2x^2-x-2=x^2(x+2)-(x+2)=(x^2-1)(x+2)=(x-1)(x+1)(x+2)$. Si vede subito che le due fattorizzazioni non hanno primi (o loro associati) in comune, e quindi il massimo comun divisore tra i due polinomi in $\mathbb{Z}[x]$ è 1, che non è associato ad $x-2$.

(c2) Si può procedere come nel punto precedente, oppure con l'algoritmo euclideo, che permette di calcolare il massimo comun divisore. Alternativamente, si può osservare come $x-2$ non divida x^3+2x^2-x-2, e quindi non possa essere un divisore comune.

(5) Nell'anello $\mathbb{Q}[x]$ si consideri l'ideale I generato da $x^7 - x^5 - x^4 + x$ e $x^5 - x$. Dire se $\mathbb{Q}[x]/I$ sia o meno un campo.

Soluzione: L'anello $\mathbb{Q}[x]$ è un dominio a ideali principali. L'ideale $I = (x^7 - x^5 - x^4 + x, x^5 - x)$ è quindi generato dal massimo comun divisore tra i due polinomi, che si trova rapidamente con l'algoritmo euclideo. Si ottiene $\mathrm{MCD}(x^7 - x^5 - x^4 + x, x^5 - x) = x^2 - x$.

Il quoziente $\mathbb{Q}[x]/I$ è un campo se e solo se l'ideale I è massimale. Poiché $\mathbb{Q}[x]$ è un dominio a ideali principali, la massimalità di I è equivalente all'irriducibilità di un (qualsiasi) suo generatore. Ad ogni modo, $x^2 - x = x(x-1)$ è riducibile a vista, e quindi $\mathbb{Q}[x]/I$ non è un campo.