Esame di Matematica Discreta

Laurea Triennale in Informatica e Comunicazione Digitale

10/2/2006

1. Risolvere la congruenza

$$5x \equiv (54321)^{33} \bmod 11.$$

Risulta $54321 \equiv_{11} 1 - 2 + 3 - 4 + 5 \equiv_{11} 3$ per cui la congruenza può riscriversi

$$5x \equiv 3^{33} \bmod 11.$$

Inoltre, applicando il Piccolo Teorema di Fermat, essendo $33 \equiv 3 \bmod 10$, si ha

$$3^{33} \equiv 3^3 \bmod 11$$

e quindi la congruenza si semplifica in

$$5x \equiv 27 \bmod 11$$

ovvero

$$5x \equiv 5 \bmod 11.$$

Utilizzando la legge di cancellazione, si ottiene

$$x \equiv 1 \bmod 11$$

per cui le soluzioni sono tutti e soli gli interi del tipo $1 + 11k$, $k \in \mathbb{Z}$.

2. Si consideri la relazione $\mathcal{R}$ su $\mathbb{Z}$ definita da

$$x\mathcal{R}\, y \iff 7|(8x + 13y).$$

a) Verificare che $\mathcal{R}$ è una relazione di equivalenza;

b) Determinare tutti gli elementi della classe $[-1]_{\mathcal{R}}$.

a) PRIMO METODO: Si verifica che $\mathcal{R}$ è riflessiva, simmetrica e transitiva.

Riflessività: per ogni $x \in \mathbb{Z}$ è vero che $x\mathcal{R}x$ in quanto $8x + 13x = 21x$ è divisibile per 7.

Simmetria: Siano $x, y \in \mathbb{Z}$ tali che $x\mathcal{R}y$. Si deve provare che è anche $y\mathcal{R}x$. Per ipotesi $8x + 13y$ è multiplo di 7. Ovvero

$$8x + 13y = 7k \tag{$*$}$$

per un opportuno $k \in \mathbb{Z}$. Occorre mostrare che anche $8y + 13x$ è multiplo di 7. A questo scopo ricaviamo x in funzione di y dalla (*): possiamo riscrivere $(*)$ come segue

$$x + 7x + 13y = 7k$$

da cui

$$x = -13y + 7(k - x) = -13y + 7s$$

dove si è posto $s = k - x$. Utilizzando questa relazione ricaviamo

$$13x + 8y = 13(-13y + 7s) + 8y = -161y + 7 \cdot 13s.$$

Poichè 161 è multiplo di 7, concludiamo che $13x + 8y$ è anch'esso multiplo di 7.

Transitività: Siano $x, y, z \in \mathbb{Z}$ tali che $x\mathcal{R}y$ e $y\mathcal{R}z$. Bisogna provare che $x\mathcal{R}z$.

Per ipotesi

$$8x + 13y = 7k,\ \ 8y + 13z = 7h$$

per opportuni $h, k \in \mathbb{Z}$. Sommando membro a membro queste relazioni otteniamo

$$8x + 13z + 21y = 7(h + k)$$

ovvero

$$8x + 13z = 7(h + k - 3y).$$

Quindi 7 divide $8x + 13z$ il che garantisce che $x\mathcal{R}z$ in base alla definizione di $\mathcal{R}$.

SECONDO METODO: La definizione della relazione $\mathcal{R}$ è equivalente a

$$8x + 13y \equiv 0 \bmod 7$$

ovvero, riducendo 8 e 13 modulo 7:

$$x + 6 \equiv 0 \bmod 7$$

che può ancora riscriversi

$$x \equiv -6 \bmod 7$$

Esame di Matematica Discreta
Laurea Triennale in Informatica e Comunicazione Digitale
23/1/2006

1. Si consideri la struttura algebrica $(\mathbb{Q} \times \mathbb{Q}, *)$ la cui operazione $*$ è definita nel modo seguente

$$(a, b) * (x, y) := (ax, ay + b).$$

Verificare che $(\mathbb{Q} \times \mathbb{Q}, *)$ è un monoide.

Si tratta di verificare che l'operazione $*$ è associativa e dotata di elemento neutro.

Riguardo l'associatività, dati tre elementi arbitrari $(a, b), (x, y), (u, v)$ di $\mathbb{Q} \times \mathbb{Q}$ risulta

$$((a, b) * (x, y)) * (u, v) = (ax, ay + b) * (u, v) = (axu, axv + ay + b)$$

e d'altra parte

$$\begin{aligned}&(a, b) * ((x, y) * (u, v)) = (a, b) * (xu, xv + y) = \\ &(axu, a(xv + y) + b) = (axu, axv + ay + b)\end{aligned}$$

il che implica che $*$ è associativa.

Per determinare se $*$ ha l'elemento neutro, occore stabilire l'esistenza di un elemento (x, y) di $\mathbb{Q} \times \mathbb{Q}$ tale che, per ogni $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ risulti

$$(a, b) * (x, y) = (a, b) = (x, y) * (a, b).$$

Dalla prima di queste uguaglianze seguono

$$ax = a, \quad ay + b = b$$

ovvero

$$ax = a, \quad ay = 0$$

che devono essere verificate per ogni $a \in \mathbb{Q}$. Scegliendo $a \neq 0$ (ad es. $a = 1$), segue che $x = 1$ ed $y = 0$. Dunque, se esiste l'elemento neutro per $*$, esso è necessariamente dato da $(1, 0)$. Resta da verificare che per ogni (a, b) si ha $(1, 0) * (a, b) = (a, b)$; infatti

$$(1, 0) * (a, b) = (1 \cdot a, 1 \cdot b + 0) = (a, b).$$

Resta provato che $(\mathbb{Q} \times \mathbb{Q}, *)$ è un monoide.

2. Risolvere il sistema di congruenze lineari

$$\begin{cases} x \equiv 15 \mod 81 \\ x \equiv 0 \mod 7 \end{cases}$$

Determinare inoltre una soluzione pari x_o e una soluzione dispari x_1.

Il sistema ha soluzioni per il Teorema cinese del resto in quanto $MCD(81, 7) = 1$. Dalla seconda congruenza si trae

$$x = 7k, \quad k \in \mathbb{Z}$$

e sostituendo nella prima si perviene alla congruenza

$$7k \equiv 15 \mod 81$$

nell'incognita k. La generica soluzione (ottenibile ad esempio mediante l'algoritmo di Euclide) di questa congruenza risulta

$$k = 60 + 81t, \quad t \in \mathbb{Z}.$$

Dunque tutte le soluzioni del sistema sono gli interi

$$x = 7(60 + 81t) = 420 + 567t, \quad t \in \mathbb{Z}.$$

Una soluzione pari è dunque 420, mentre una soluzione dispari è $420+567 = 987$.

3. Si consideri la permutazione

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 4 & 7 & 6 & 5 & 8 \end{pmatrix}.$$

a) Calcolare f^{27}.

b) Determinare, se esistono, i sottogruppi di $< f >$ di ordine 2, 3 e 4.

a) Decomponendo f in cicli disgiunti si ottiene

$$f = (132) \circ (57)$$

ovvero, essendo $-6 \equiv_7 1$,

$$x \equiv y \bmod 7.$$

Dunque la relazione $\mathcal{R}$ altri non è che la relazione di congruenza modulo 7, che è ben noto essere una relazione di equivalenza.

b) Per definizione

$$[-1]_{\mathcal{R}} = \{x \in \mathbb{Z} \mid -1\mathcal{R}x\} = \{x \in \mathbb{Z} \mid \ 7|(-8+13x)\}.$$

Dunque gli elementi di $[-1]$ sono tutte e sole le soluzioni $x \in \mathbb{Z}$ della congruenza

$$-8 + 13x \equiv 0 \bmod 7$$

ovvero

$$13x \equiv 8 \mathrm{mod}\, 7.$$

Poichè $-1\mathcal{R}-1$ in forza della riflessività di $\mathcal{R}$, necessariamente -1 appartiene alla classe $[-1]_{\mathcal{R}}$, per cui una soluzione è già nota ed è necessariamente $x_o = -1$. Inoltre la nostra congruenza ha *una sola soluzione modulo 7*, essendo $MCD(13, 7) = 1$. La generica soluzione è pertanto

$$-1 + 7k \quad k \in \mathbb{Z}.$$

Conclusione:

$$[-1]_{\mathcal{R}} = \{-1 + 7k \mid \ k \in \mathbb{Z}\}.$$

Si osservi che, svolgendo la parte a) dell'esercizio col secondo metodo, la risposta a b) è invece immediata:

$$[-1]_{\mathcal{R}} = [-1]_7 = \{-1 + 7k \mid \ k \in \mathbb{Z}\}.$$

3. Si considerino le permutazioni di S_8:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 2 & 4 & 7 & 6 & 5 & 8 \end{pmatrix} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 3 & 6 & 5 & 4 & 7 & 1 \end{pmatrix}$$

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 2 & 6 & 7 & 4 & 5 & 1 \end{pmatrix}.$$

a) Verificare che $H = \{Id, f, g, h\}$ è un sottogruppo di S_8.

b) Stabilire se H è un gruppo ciclico.

a) Per stabilire se un sottoinsieme H di un gruppo $(G, \cdot)$ è un sottogruppo, è sufficiente applicare il seguente criterio: *dati due elementi qualsiasi x, y di H, si ha $x \cdot y^{-1} \in H$.*

Nel caso in esame $f = (23)(75)$, per cui $o(f) = 2$ e quindi $f^2 = Id$; ciò significa che f^{-1} concide con f. Analogamente $g = (18)(46)$, per cui $o(g) = 2$ e $g^{-1} = g$ ed infine $h = (18)(23)(46)(57)$ e quindi è anche $o(h) = 2$ con $h^{-1} = h$.

Ora, abbiamo la seguente tabella

∘	Id	f	g	h
Id	Id	f	g	h
f	f	Id	h	g
g	g	h	Id	f
h	h	g	f	Id

che mostra che il criterio di cui sopra è soddisfatto; concludiamo che H è sottogruppo di S_8.

b) H non è cilico perchè tutti i suoi elementi diversi dall'elemento neutro Id hanno periodo $2 \neq 4 = |H|$ per cui nessuno di essi può esserne generatore.

N.B: Il gruppo H è isomorfo al gruppo di Klein.

4. a) Determinare tutti i sottogruppi di $\mathbb{Z}_{15}$;

b) Determinare l'omomorfismo $f : \mathbb{Z} \to \mathbb{Z}_{15}$ tale che

$$f(7) = [6]_{15}$$

e stabilire se è surgettivo.

a) I divisori non banali di 15 sono 3 e 5; quindi $\mathbb{Z}_{15}$ ha, oltre ai sottogruppi $\{0\}$ e $\mathbb{Z}_{15}$, altri due sottogruppi K_1 e K_2 con $|K_1| = 3$ e $|K_2| = 5$. Entrambi sono ciclici. Risulta

$$K_1 =< [5] >= \{0, [5], [10]\}, \; K_2 =< [3] >= \{0, [3], [6], [9], [12]\}.$$

b) Un omomorfismo $f : \mathbb{Z} \to \mathbb{Z}_{15}$ è completamente determinato dal valore che assume in 1; posto

$$f(1) = [y]_{15}$$

con $0 \leq y \leq 14$, risulta quindi

$$f(7) = 7[y]_{15} = [7y]_{15}.$$

Pertanto f verifica la condizione richiesta se e solo se

$$[7y]_{15} = [6]_{15}$$

ovvero se y è soluzione della congruenza

$$7y \equiv 6 \bmod 15.$$

Risolvendo, si ricava $y = 3$. Quindi f è dato dalla seguente formula

$$f(n) = [3n]_{15}, \quad n \in \mathbb{Z}.$$

Ricordando che la surgettività significa che $Im(f) = \mathbb{Z}_{15}$ e che $Im(f) =< f(1) >$, abbiamo che f non è surgettivo in quanto $f(1) = [3]$ *non* è generatore di $\mathbb{Z}_{15}$, avendosi $MCD(3, 15) = 3 \neq 1$.

5. Calcolare l'inverso di [17] nel campo $\mathbb{Z}_{19}$.

Sapendo inoltre che [2] è un elemento primitivo, dire, giustificando la risposta, quali dei seguenti sono elementi primitivi di $\mathbb{Z}_{19}$:

$$a = [8], b = [2^5], c = [2^9].$$

Si tratta di risolvere la congruenza

$$17x \equiv 1 \bmod 19$$

Si ottiene che $[17]^{-1} = [9]$.

Il gruppo $(\mathbb{Z}_{19}^*, \cdot)$ ha ordine 18; per cui, oltre a [2], tutti i suoi generatori (elementi primitivi del campo) sono le potenze $[2]^s = [2^s]$ con $MCD(s, 18) = 1$. Pertanto b è elemento primitivo, mentre a e c non lo sono.

6. Si consideri il campo $\mathbb{K} = \mathbb{Z}_2[x]/(x^2 + x + 1)$.

a) Dire quanti elementi ha $\mathbb{K}$ ed elencarli;

b) Scrivere la tabella dell'addizione e della moltiplicazione di $\mathbb{K}$.

a) Il campo $\mathbb{K}$ ha quattro elementi, dati dalle seguenti classi di congruenza modulo il polinomio di secondo grado $q = x^2 + x + 1$:

$$[0], [1], [x], [x + 1].$$

Esse sono infatti tutte le classi di congruenza distinte determinate da polinomi di grado < 2.

b) Tenendo conto che $x^2 \equiv x+1 \bmod q$ e che $x^2+x \equiv 1 \bmod q$, le tabelle delle operazioni sono le seguenti:

+	[0]	[x]	[x+1]	[1]
[0]	[0]	[x]	[x+1]	[1]
[x]	[x]	[0]	[1]	[x+1]
[x+1]	[x+1]	[1]	[0]	[x]
[1]	[1]	[1+x]	[x]	[0]

·	[0]	[x]	[x+1]	[1]
[0]	[0]	[0]	[0]	[0]
[x]	[0]	[x+1]	[1]	[x]
[x+1]	[0]	[1]	[x]	[x+1]
[1]	[0]	[x]	[x+1]	[1]

Esame di Matematica Discreta
Laurea Triennale in Informatica e Comunicazione Digitale-Taranto
9/1/2005
Soluzioni

1. 1) X non è sottomoide, perchè non è chiuso per la moltiplicazione:
ad esempio, risulta $\frac{3}{2}, 2 \in X$, ma $\frac{3}{2} \cdot 2 = \frac{1}{2} \notin X$.

2) f è ingettiva, ma non surgettiva. Infatti, il numero $\frac{1}{2} \in \mathbb{Q}$ **non** ha alcuna preimmagine $x \in X$. A ciò si perviene esaminando l'equazione

$$f(x) = y$$

nell'incognita $x \in X$, con dato $y \in \mathbb{Q}$. Tale equazione è

$$(1-2y)x = 5 - y$$

che non ha soluzione se $1 - 2y = 0$, ovvero $y = \frac{1}{2}$.

2. L'insieme delle soluzioni del sistema è $[2]_{15} = \{2 + 15h \mid h \in \mathbb{Z}\}$.
Pertanto, ad esempio, $x_0 = 2$ è una soluzione pari, mentre $x_1 = 17$ è una soluzione dispari.

3. 1) La decomposizione di f in cicli disgiunti è

$$f = (135)(24)$$

per cui $o(f) = m.c.m.(3, 2) = 6$. La decomposizione di $f \circ g$ in cicli disgiunti è

$$f \circ g = (264)$$

per cui $o(f \circ g) = 3$.

2) I generatori di H sono tutte le potenze f^k con $0 \leq k \leq 5$ primo con 6. Quindi sono f e $f^5 = (135)^5(24)^5 = (135)^2(24) = (153)(24)$.

3) Poichè $Im(F) =< F(1) >$, $F(1)$ dev'essere un elemento di H di periodo 3. Gli elementi di $H = \{Id, f, \ldots, f^5\}$ di periodo 3 sono f^2 e f^4 perchè 2 e 4 sono i soli interi positivi, minori di 6, tali che $MCD(k, 6) = 2$. Pertanto vi sono esattamente due omomorfismi $F_1, F_2 : \mathbb{Z} \to H$ tali che $|Im(F)| = 3$ e sono determinati dalle condizioni

$$F_1(1) = f^2,\ F_2(1) = f^4.$$

Segue che

$$F_1(2) = (f^2)^2 = f^4,\ F_2(2) = (f^4)^2 = f^8 = f^2.$$

Poichè

$$f^4 = (135)\ f^2 = (153)$$

segue che l'omomorfismo richiesto esiste e concide con F_2.

4. Risulta $MCD(p,q) = x + 1$.

5. 1) Abbiamo $< 5 >= \{5k \mid k = 0, \dots, 5\}$ in quanto 5 è un elemento di periodo 6 in $(\mathbb{Z}_{30}, +)$. (Qui e nel seguto si è semplificata la notazione: 5 va naturalmente inteso come $[5]_{30}$).

Esaminado la tabella della moltiplicazione per S si può osservare che 25 è l'elemento neutro.

Volendo determinare più rapidamente l'el. neutro $u = 5x$ con $x = 0, \dots, 5$, si tratta di imporre che per ogni $k = 0, \dots, 5$ risulti

$$5x \cdot 5k \equiv 5k \mod 30.$$

Da qui ricaviamo

$$5xk \equiv k \mod 6.$$

In particolare, per $k = 1$

$$5x \equiv 1 \mod 6$$

da cui si ricava $x = 5$. Pertanto necessariamente $u = 25$. Occorre però fare la verifica:

$$25 \cdot 5k \equiv_{30} 125k \equiv_{30} 5k.$$

Quindi l'elemento neutro è effettivamente 25.

2) Sebbene $(S, +, \cdot)$ sia un anello, esso **non** è un campo in base al Teorema di classificazione dei campi finiti: 6 non è potenza di un primo.

6. L'albero in questione ha 6-1=5 lati, per cui necessariamente $x = 1$, in quanto tutti i vertici di grado x sono adiacenti a quello di grado 5. Ciò può ricavarsi anche dalla formula

$$10 = 5 + 5x$$

che lega il numero dei lati ed i gradi dei vertici.

Esame di Matematica Discreta
Laurea Triennale in Informatica e Comunicazione Digitale
17/1/2007
Soluzioni degli esercizi proposti

1. Si ponga $X = \{1, 2, 3, 4, 5, 6\}$ e $Y = \{a, b, c, d\}$. Calcolare il numero delle applicazioni surgettive $f : X \to Y$ verificanti la condizione seguente:

$$f(1) = f(2) = a.$$

La generica funzione surgettiva $f : X \to Y$ si costruisce a partire da una partizione di X con 4 blocchi ed assegnando un'etichetta a ciascun blocco scelta tra uno degli elementi di Y. La condizione richiesta implica che gli elementi $1, 2$ devono appartenere allo stesso blocco, etichettato con "a". Osserviamo che tale blocco può essere $\{1, 2\}$ o al massimo contenere un altro elemento di X diverso da 1 e 2. Per ciascuna partizione ammissibile vi sono 3! funzioni surgettive verificanti la condizione in esame. Quindi il totale delle funzioni in questione è dato da:

$$S(4, 3)3! + 4S(3, 3)3! = 6 \cdot 6 + 4 \cdot 6 = 36 + 24 = 60.$$

2. Risolvere il sistema di congruenze lineari:

$$\begin{cases} 19x \equiv 1 & \mod 7 \\ 12x \equiv 1 & \mod 11 \end{cases}$$

Si osservi che il sistema può riscriversi come

$$\begin{cases} 5x \equiv 1 & \mod 7 \\ x \equiv 1 & \mod 11 \end{cases}$$

La seconda congruenza è quindi risolta da

$$x = 1 + 11k.$$

Sostituendo nella prima si ottiene la congruenza in k:

$$6k \equiv 3 \mod 7$$

da cui

$$k = 4 + 7h.$$

In conclusione le soluzioni sono date da

$$x = 1 + 11(4 + 7h) = 45 + 7h$$

al variare di $h \in \mathbb{Z}$.

3. Si consideri il campo $\mathbb{K} = \mathbb{Z}_2[x]/(x^3 + x + 1)$.

a) Elencare tutti gli elementi di $\mathbb{K}$.

b) Stabilire quali delle seguenti uguaglianze sono vere:

$$[x + 1][x + 1] = [x^2 + 1], \ \ [x^2 + 1][x^2] = 0, \ \ [x^2 + 1]^{-1} = [x].$$

a) Gli elementi di $\mathbb{K}$ sono $2^3 = 8$ e corrispondono alle classi di equivalenza distinte $[p]$ modulo il polinomio $q = x^3 + x + 1$, che sono tante quanti sono i polinomi a coefficienti in $\mathbb{Z}_2$ di grado ≤ 2. Dunque:

$$\mathbb{K} = \{0, [1], [x], [x + 1], [x^2], [x^2 + 1], [x^2 + x], [x^2 + x + 1]\}.$$

b) Poichè $\mathbb{K}$ è una campo, e quindi privo di divisori dello zero, certamente la seconda uguaglianza è falsa. La prima uguaglianza è vera: infatti, modulo q risulta:

$$(x + 1)(x + 1) \equiv x^2 + 2x + 1 \equiv x^2 + 1.$$

Riguardo la terza, si tratta di verificare se $[x^2 + 1][x] = 1$. Anche questa identità è vera: infatti abbiamo $q = x^3 + x + 1 \equiv 0$ da cui

$$x^3 + x \equiv -1 \equiv 1.$$

4. Stabilire se il polinomio

$$p = x^5 + x + \underline{1}$$

di $\mathbb{Z}_2[x]$ è irriducibile.

Si verifica subito che p non ha radici in $\mathbb{Z}_2[x]$:

$$p(0) = \underline{1}, \ p(\underline{1}) = \underline{1}.$$

Quindi, per il Ter. di Ruffini p non ha divisori di grado 1. Essendo $gr(p) = 5$, p risulterà riducibile se e solo ammette un divisore irriducibile q grado 2. L'unico q possibile è $q = x^2 + x + 1$. Effettuando la divisione di p per q si verifica che in effetti $q|p$. Si conclude che p è riducibile.

5. a) Determinare il sottogruppo K di $\mathbb{Z}_{40}$ di ordine 10 e tutti i generatori di K.

b) Dire, giustificando la risposta, se esiste un omomorfismo

$F : \mathbb{Z}_{40} \to \mathbb{Z}_{30}$ tale che

$$F([1]_{40}) = [7]_{30}.$$

a) Per un noto Teorema, il sottogruppo richiesto K è ciclico. Un generatore $g = [k]$ di K dev'essere un elemento di periodo 10; poichè $o(g) = 40/MCD(40, k)$, dev'essere $MCD(40, k) = 4$. Una possibilità è $k = 4$ ovvero $g = [4]$.

Gli altri generatori di K sono i multipli ng con $MCD(n, 10) = 1$, ovvero $[12], [20], [28]$.

b) F non esiste in quanto $o([7]_{30}) = 30$ e 30 non divide l'ordine di $\mathbb{Z}_{40}$.

6. Stabilire se $a = [3]$ è elemento primitivo del campo $\mathbb{Z}_{11}$ e determinarne l'inverso a^{-1}. Quanti sono gli elementi primitivi?

Si tratta di verificare se a è generatore del gruppo $\mathbb{Z}_{11}^*$, ovvero se $o(a) = 10$ in tale gruppo. Calcoliamo a questo scopo le potenze di 3 modulo 11. Notiamo che $o(a)$ può essere solo 2, 5 o 10. Poichè

$$3^2 \equiv 9$$

senz'altro $o(a) \neq 2$. È sufficiente quindi controllare se $3^5 \equiv 1$. Risulta:

$$3^3 = 27 \equiv 5$$

da cui

$$3^5 \equiv 9 \cdot 5 \equiv 45 \equiv 1.$$

Concusione: $o(a) = 5$ e quindi a non è primitivo. L'inverso di a coincide con a^4 e quindi è dato da $[4]$. Alternativamente, l'inverso di a si ottiene risolvendo la congruenza $3x \equiv 1 \mathrm{mod} 11$. Infine il numero degli elementi primitivi di $\mathbb{Z}_{11}$ è dato da $\varphi(10) = \varphi(2)\varphi(5) = 1 \cdot 4 = 4$.