Prova scritta di Matematica Discreta

7 giugno 2016

Ci sono 10 esercizi.

1. Determinare le ultime tre cifre di 7^{8725}.

   Soluzione.

   Dobbiamo determinare la classe di congruenza modulo 1000 del numero dato.

   Osserviamo che $\phi(1000) = \phi(5^3 2^3) = (5^3 - 5^2)(2^3 - 2^2) = 400$ e quindi essendo $8725 = 400 \cdot 21 + 325$ il problema si riduce a calcolare le ultime cifre di 7^{325} per il Teorema di Eulero.

   Ora $7^3 = 343$ e dunque $7^{325} = (343)^{108}7 = 7 \cdot (343)^{108}$. Quadrando e via via riducendo abbiamo

$$7^{325} = (343)^{108}7 = 7 \cdot (649)^{54} \equiv 7 \cdot (201)^{27} \equiv 7 \cdot 201 \cdot (201)^{26} \equiv 7 \cdot 201 \cdot (401)^{13}$$

$$\equiv 7 \cdot 201 \cdot 401 \cdot (401)^{12} \equiv 7 \cdot 201 \cdot (401)(801)^6$$

$$\equiv 601^2 \cdot (601)(401)(201)7 \equiv (201)(601)(401)(201)7$$

$$\equiv (801)(401)(201)7 \equiv (201)(201)7 \equiv 401 \cdot 7 \equiv 807$$

2. Determinare la più piccola soluzione positiva del sistema di congruenze

$$\begin{cases} 1030x \equiv 5312066 \pmod{11} \\ 947x \equiv 532 \pmod{9} \\ 15x \equiv 31 \pmod{8} \end{cases}$$

   Soluzione.

   Semplifichiamo ciascuna congruenza usando criteri di divisibilità

$$1030 \equiv 0 - 3 + 0 - 1 = -4 \equiv 7 \pmod{11},$$

$$5312066 \equiv 6 - 6 + 0 - 2 + 1 - 3 + 5 = 1 \pmod{11}$$

$$947 \equiv 9 + 4 + 7 \equiv 2 \pmod{9},$$

$$532 \equiv 5 + 3 + 2 \equiv 1 \pmod{9}$$

$$15 \equiv 7 \pmod{8}$$

$$31 \equiv 7 \pmod{8}$$

Otteniamo

$$\begin{cases} 7x \equiv 1 \pmod{11} \\ 2x \equiv 1 \pmod{9} \\ 7x \equiv 7 \pmod{8} \end{cases}$$

Moltiplichiamo ciascuna congruenza per l'opportuno inverso moltiplicativo. Il sistema diventa

$$\begin{cases} x \equiv 8 \pmod{11} \\ x \equiv 5 \pmod{9} \\ x \equiv 1 \pmod{8} \end{cases}$$

Abbiamo $R = 8 \cdot 9 \cdot 11 = 792$ e le congruenze diventano

$$72x \equiv 8 \pmod{11}; \quad 88x \equiv 5 \pmod{9}; \quad 99x \equiv 1 \pmod{8}.$$

Risolviamo ciascuna separatamente.

$$\begin{array}{ccc} 72x \equiv 8 \pmod{11}; & 88x \equiv 5 \pmod{9}; & 99x \equiv 1 \pmod{8}; \\ 6x \equiv 8 \pmod{11}; & 7x \equiv 5 \pmod{9}; & 3x \equiv 1 \pmod{8}; \\ x \equiv 5 \pmod{11}. & x \equiv 2 \pmod{9}. & x \equiv 3 \pmod{8}. \end{array}$$

Ora prendiamo

$x = 72 \cdot 5 + 88 \cdot 2 + 99 \cdot 3 = 833 \equiv 41.$

3. Sia C_{30} il gruppo ciclico delle radici trentesime dell'unità e sia $\omega = e^{\frac{2\pi i}{30}}$.

   (a) Quante e quali sono le radici primitive? (i generatori del gruppo).

   (b) Scrivere gli elementi del sottogruppo generati da ω^6.

   (c) Scrivere gli elementi del sottogruppo di ordine 10.

   Soluzione.

   (a) $\phi(30) = \phi(2 \cdot 3 \cdot 5) = 1 \cdot 2 \cdot 4 = 8$ dunque abbiamo 8 generatori. Essi sono

   $$\omega, \omega^7, \omega^{11}, \omega^{13}, \omega^{17}, \omega^{19}, \omega^{23}, \omega^{29}.$$

   (b)

   $$\omega^6, \omega^{12}, \omega^{18}, \omega^{24}, 1$$

   (c)

   $$\omega^3, \omega^6, \omega^9, \omega^{12}, \omega^{15}, \omega^{18}, \omega^{21}, \omega^{24}, \omega^{27}, 1$$

4. Costruire un campo con 16 elementi. Illustrare con un esempio significativo come si calcola il prodotto di due elementi.

   Soluzione.

   Verifichiamo che x^4+x+1 è un polinomio irriducibile in $\mathbb{Z}_2[x]$. Si verifica subito che esso non ha radici in $\mathbb{Z}_2$. Proviamo a vedere se si fattorizza in due polinomi di secondo grado:

   $$x^4+x+1=(x^2+Ax+B)(x^2+Cx+D)$$

   Uguagliando i coefficienti abbiamo il sistema

   $$\begin{cases} A+C=0 \\ B+D+AC=0 \\ AD+BC=1 \\ BD=1 \end{cases}$$

   Dalla prima equazione ricaviamo che $A=C$, pertanto dalla terza: $A(D+B)=1$. Ne segue che A non è nullo e pertanto $A=1$ e per lo stesso motivo $D+B=1$. Dalla quarta tuttavia abbiamo che B e D sono non nulli e quindi uguali a 1. Ne consegue che $D+B=1+1=0$ contraddicendo il fatto che $D+B=0$. Questa contraddizione implica che il polinomio è irriducibile.

   Il campo in questione è quindi costituito da

   $$0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1,x^3,x^3+x^2,$$

   $$x^3+x,x^3+1,x^3+x^2+x,x^3+x^2+1,x^3+x^2+x,x^3+x^2+x+1$$

   Per esempio:

   $$x^2(x^4+x^3+x^2+x+1)=x^6+x^5+x^4+x^3+x^2$$

   Utilizziamo la relazione $x^4=x+1$ e otteniamo

   $$x^2(x+1)+x(x+1)+x+1+x^3+x^2$$

   $$x^3+x^2+x^2+x+x+1+x^3+x^2$$

   Questo si semplifica in

   $$x^2+1$$

5. Usando la parola chiave $\mathbf{k}=APPELLO$ criptare la frase A CAVAL DONATO NON SI GUARDA IN BOCCA (cifrario di Vigenère).

   Soluzione.

   Spezziamo la frase in blocchi da 7: ACAVALD ONATONO NSIGUAR DAINBOC CA

a	p	p	e	l	l	o	a	p	p	e	l	l	o
a	c	a	v	a	l	d	o	n	a	t	o	n	o
A	R	P	Z	L	W	R	O	C	P	X	Z	Y	C

a	p	p	e	l	l	o	a	p	p	e	l	l	o	a	p
n	s	i	g	u	a	r	d	a	i	n	b	o	c	c	a
N	H	A	K	F	L	F	D	P	X	R	M	Z	Q	C	P

Il messaggio crittato è

ARPZLWROCPXZYCNHAKFLFDPXRMZQCP

6. Enunciare e dimostrare il criterio di Eulero per l'esistenza di un circuito euleriano in un grafo.

   Soluzione. V. Teorema 8.6.2 degli Appunti.

7. Dimostrare che il grafo Q_3 del cubo tridimensionale è un grafo bipartito.

   Soluzione. V. §8.2.5 degli Appunti.

8. Dimostrare che non esiste un codice binario di tipo $(8, 30, 3)$. **Soluzione.** Un codice di tipo $(8, 30, 3)$ dovrebbe soddisfare la Disuguaglianza di Hamming: $n = 8, M = 30, t = 1, q = 2$ e dunque

$$30\{\binom{8}{0} + \binom{8}{1}\} \leq 2^8$$

   che vale $30\{9\} \leq 256$ ossia $270 \leq 256$ che non è vera. Il codice è impossibile.

9. Usare l'identità $(1 - x^2)^n = (1 - x)^n(1 + x)^n$ per dimostrare la formula

$$\binom{n}{0}^2 - \binom{n}{1}^2 + \binom{n}{2}^2 - \cdots + (-1)^n \binom{n}{n}^2 = \begin{cases} (-1)^{\frac{n}{2}} \binom{n}{\frac{n}{2}} & \text{se } n \text{ è pari} \\ 0 & \text{se } n \text{ è dispari} \end{cases}$$

   Ad esempio,

$$\binom{6}{0}^2 - \binom{6}{1}^2 + \binom{6}{2}^2 - \binom{6}{3}^2 + \binom{6}{4}^2 - \binom{6}{5}^2 + \binom{6}{6}^2 = -20 = -\binom{6}{3}$$

   (Suggerimento: Considerare il coefficiente di x^n in ambo i membri dell'identità).

   Soluzione. Consideriamo il coefficiente di x^n in ambo i membri dell'idntità. Nel secondo membro abbiamo

$$(1 - \binom{n}{1}x + \binom{n}{2}x^2 - \cdots + (-1)^n \binom{n}{n}x^n)(1 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n)$$

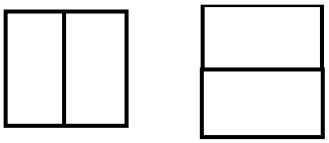
e il coefficiente di x^n è

$$\sum_{r+s=n}(-1)^r\binom{n}{r}\binom{n}{s}=\sum_{r=0}^{n}(-1)^r\binom{n}{r}\binom{n}{n-r}=\sum_{r=0}^{n}(-1)^r\binom{n}{r}^2$$

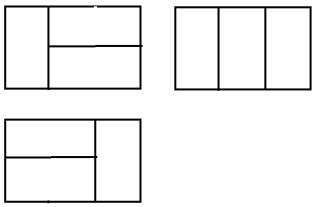
D'altra parte il coefficiente di x^n nel primo membro è 0 se n è dispari mentre è uguale a $(-1)^{\frac{n}{2}}\binom{n}{\frac{n}{2}}$ se n è pari. Otteniamo quindi la formula desiderata.

10. Una ditta deve pavimentare un marciapiede largo 2 metri e lungo n metri, n intero maggiore o uguale a 1, usando lastre di travertino rettangolari di 1 metro per 2 metri. In quanti modi diversi si possono disporre le lastre per pavimentare un marciapiede lungo n metri? (Suggerimento: chiamiamo p_n il numero di modi cercato, calcolare $p_1, p_2, \cdots$ per qualche n piccolo. Trovare una formula per p_n e dimostrarla.)

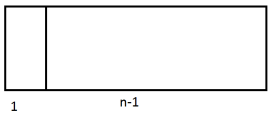
Soluzione. Se $n = 1$ c'è ovviamente un solo modo di disporre la lastra. Se $n = 2$ il marciapiede si può pavimentare in due modi



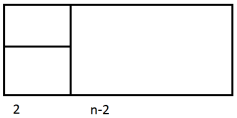
Mentre se $n = 3$ ci sono tre modi:



In generale, un marciapiede di n metri può essere pavimentato disponendo una lastra come in figura e poi tutte le maniere di pavimentare i restanti $n - 1$ metri:



oppure cominciando posizionando due lastre e poi pavimentando i rimanenti $n - 2$ metri di marciapiede:



Nel primo caso abbiamo p_{n-1} modi per completare l'opera, nel secondo caso abbiamo p_{n-2} modi. In totale quindi abbiamo

$$p_n = p_{n-1} + p_{n-2}$$

Si tratta quindi della successione di Fibonacci.