Prova scritta di Matematica Discreta

6 giugno 2017

Ci sono 10 esercizi.

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

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

$$\begin{cases} 1030x \equiv 5315066 \pmod{11} \\ 947x \equiv 532 \pmod{9} \\ 15x \equiv 31 \pmod{8} \end{cases}$$

Soluzione.

Semplifichiamo ciascuna congruenza usando criteri di divisibilità

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

$$5312066 \equiv 6 - 6 + 0 - 5 + 1 - 3 + 5 \equiv 9 \pmod{11}$$

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

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

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

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

Otteniamo

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

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

$$\begin{cases} x \equiv 6 \pmod{11} \\ x \equiv 5 \pmod{9} \\ x \equiv 1 \pmod{8} \end{cases}$$

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

$$72x \equiv 6 \pmod{11}; \quad 88x \equiv 5 \pmod{9}; \quad 99x \equiv 1 \pmod{8}.$$

Risolviamo ciascuna separatamente.

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

Ora prendiamo

$x = 72 \cdot 1 + 88 \cdot 2 + 99 \cdot 3 = 1193 \equiv 545.$

2. Costruire un campo con 25 elementi. Calcolare il prodotto $(3x+2)(x+1)$.

Soluzione.

Verifichiamo che $x^2 + x + 1$ è un polinomio irriducibile in $\mathbb{Z}_5[x]$. Si verifica subito che esso non ha radici in $\mathbb{Z}_5$ ed essendo di grado 2 ciò è sufficiente a concludere che è irriducibile.

Il campo in questione è quindi costituito da

$$0, 1, 2, 3, 4, x, x+1, x+2, x+3, x+4, 2x, 3x, \ldots$$

In general,

$$ax + b, \quad a, b \in \mathbb{Z}_5$$

Per esempio:

$(3x+2)(x+1) = 3x^2+5x+2 \equiv 3x^2+2 \equiv 3(-x-1)+2 = -3x-1 \equiv 2x+4$

3. Usando la parola chiave $\mathbf{k} = CHIAVE$ criptare la frase IL DIAVOLO FA LE PENTOLE MA NON I COPERCHI (cifrario di Vigenère).

Soluzione.

Spezziamo la frase in blocchi da 6 (finché è possibile): ILDIAV OLOFAL EPENTO LEMANO NICOPE RCHI

c	h	i	a	v	e	c	h	i	a	v	e	c	h
i	l	d	i	a	v	o	l	o	f	a	l	e	p
K	S	L	I	V	Z	Q	S	W	F	V	P	G	W

i	a	v	e	c	h	i	a	v	e	c	h	i	a	v	e
e	n	t	o	l	e	m	a	n	o	n	i	c	o	p	e
M	N	O	S	N	L	U	A	I	S	P	P	K	O	K	I

c	h	i	a	v	e
r	c	h	i		
T	J	P	I		

Il messaggio crittato è

KSLIVZQSWFVPGWMNOSNLUAISPPKOKITJPI

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

   Soluzione. V. §8.2.5 degli Appunti.

5. 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.

6. Esprimere $\frac{1361}{47}$ come frazione continua

   Soluzione.

$$\begin{aligned}
\frac{1361}{47} &= 28,\overline{957446808510638297872340425531914893617021276 5} \\
\frac{1}{0,\overline{957446808510638297872340425531914893617021276 5}} &= 1,0\overline{4} \\
\frac{1}{0,0\overline{4}} &= 22,5 \\
\frac{1}{0,5} &= 2
\end{aligned}$$

   da cui si ricava

$$[28; 1, 22, 2]$$

7. Se $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, \ldots$ è la classica successione di Fibonacci, dimostrare che $F_n \equiv 0 \pmod 4$ se e solo se $n \equiv 0 \pmod 6$.

   Soluzione. Per induzione: $F_6 = 8 \equiv 0 \pmod 4$. Supponiamo che $F_{6n} \equiv 0 \pmod 4$ allora consideriamo $F_{6(n+1)}$. Possiamo scrivere

$$\begin{aligned}
F_{6n+6} = F_{6n+5} + F_{6n+4} &= 2F_{6n+4} + F_{6n+3} \\
= 2(F_{6n+3} + F_{6n+2}) + F_{6n+3} &= 3F_{6n+3} + 2F_{6n+2} \\
= 5(F_{6n+2} + 3F_{6n+1}) &= 5(F_{6n+1} + F_{6n}) + 3F_{6n+1} \\
&= 8F_{6n+1} + 5F_{6n} \equiv 0 \pmod 4
\end{aligned}$$

   per ipotesi induttiva. Questo dimostra che se $n \equiv 0 \pmod 6$ allora $F_n \equiv 0 \pmod 4$.

Viceversa, se $F_n \equiv 0 \pmod 4$ allora con un ragionamento analogo a quello fatto sopra si vede che $F_n = 8F_{n-5} + 5F_{n-6}$ e che quindi necessariamente anche $F_{n-4} \equiv 0 \pmod 3$. Tuttavia F_1, F_2, F_3, F_4, F_5 non sono congrui a 0 modulo 4.

8. Risolvere la ricorrenza $h_n = 3h_{n-1} - 4h_{n-3}, n \geq 3$ con $h_0 = 1, h_1 = 0, h_2 = 0$. Quanto vale h_{10}? (Attenzione alle radici multiple).

   Soluzione. L'equazione caratteristica è $x^3 - 3x^2 + 4 = 0$ che ha soluzioni $2, 2, -1$. Avendo una radice doppia la soluzione generale è

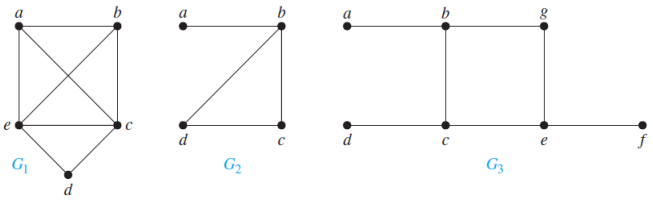
   $$a2^n + bn2^n + c(-1)^n$$

   con condizioni iniziali

   $$\begin{cases} a + b = 1 \\ 2a + 2b - c = 0 \\ 4a + 8b + c = 0 \end{cases}$$

   da cui $a = \frac{5}{9}$, $b = -\frac{1}{3}$, $c = \frac{4}{9}$. Infine, $h_{10} = -2844$.

9. Trovare, se possibile, un circuito hamiltoniano oppure un cammino hamiltoniano sui seguente grafi



   Soluzione.

   G_1 ha un circuito di Hamilton: a, b, c, d, e, a. G_2 non ha un circuito di Hamilton ma ha un cammino di Hamilton : a, b, c, d. G_3 non ha né un cammino né un circuito di Hamilton.

10. Dimostrare che se $N = a_k a_{k-1} \dots a_1 a_0 = a_0 + 10b$ è un numero scritto in cifre decimali allora $N \equiv a_0 + 3b \pmod 7$. Sfruttare questo risultato per verificare che il numero 123456789 è congruo a 1 modulo 7.

    Soluzione. Se $N = a_0 + 10b$ moltiplichiamo per l'inverso di 10 (mod 7), cioè -2. Infatti $-2 \times 10 \equiv 5 \times 10 = 50 \equiv 1 \pmod 7$. Otteniamo

    $$-2N = -2a_0 + (-2)(10)b$$

    $$-2N \equiv -2a_0 + b$$

    Ora, l'inverso di $-2 \pmod 7$ è 3 e dunque moltiplicando per 3 si ha

    $$3(-2N) \equiv 3(-2a_0) + 3b$$

ossia

$$N \equiv a_0 + 3b$$

Applichiamo ripetutamente adesso questa osservazione al numero N dato.

$$\begin{aligned}
123456789 \\
9 + 3(12345678) &= 3703704 \\
3 + 3(3703704) &= 11111115 \\
5 + 3(1111111) &= 3333338 \\
8 + 3(333333) &= 1000007 \\
7 + 3(100000) &= 300007 \\
7 + 3(30000) &= 90007 \\
7 + 3(9000) &= 27007 \\
7 + 3(2700) &= 8107 \\
7 + 3(810) &= 2437 \\
7 + 3(243) &= 736 \\
6 + 3(73) &= 225 \\
5 + 3(22) &= 71
\end{aligned}$$

da cui chiaramente, $N \equiv 1 \pmod 7$.