ALGEBRA

Claudia Malvenuto
Canale A-L
Scheda esercizi n. 5

19 ottobre 2011

Rifugiamoci un po' nell'aritmetica:
dodici, ventiquattro, trentasei...
È un bell'aiuto quando si farnetica.
Ma ora non cosí come vorrei.
(Patrizia Valduga, 'Quartine, Seconda centuria')

1. Scrivere l'algoritmo di Euclide delle divisioni successive in pseudocodice. Scrivere anche lo pseudocodice di un algoritmo che presi in input due interi non entrambi nulli a e b, dia in output due interi s, t tali che $(a, b) = as + bt$ (identità di Bézout).

2. Trovare l'inverso di ogni elemento $\overline{a} \in \mathbb{Z}/29\mathbb{Z} \setminus \{\overline{0}\}$, tramite il piccolo teorema di Fermat (ovvero calcolando a^{27}...), oppure cercando i coefficienti s, t per l'identità di Bézout $1 = as + 29t$ relativa al massimo comune divisore $1 = (a, 29)$.

3. Per ognuna delle seguenti coppie di numeri $a, b \in \mathbb{N}$ trovare il massimo comune divisore (a, b) di a e b tramite l'*algoritmo di Euclide* ed esprimerlo nella forma $as + bt$ per opportuni $s, t \in \mathbb{Z}$ (identità di Bézout):

   (a) $a = 1705$ e $b = 625$

   (b) $a = 1625$ e $b = 858$

   (c) $a = 2094$ e $b = 12$

   (d) $a = 5307$ e $b = 9150$

Per gli interi a e b del punto d), trovare (a, b) anche con il metodo noto dalla scuola media della fattorizzazione in primi.

4. Se F_n è l'n–esimo numero di Fibonacci, quanto vale il massimo comune divisore (F_n, F_{n+1})? Dimostrarlo per induzione, usando l'algoritmo euclideo.

5. Indicato con $[a, b]$ il minimo comune multiplo tra due interi non entrambi nulli a e b, dimostrare che $[a, b] = \frac{a \cdot b}{(a,b)}$.

6. Utilizzando il teorema fondamentale dell'aritmetica dimostrare che se p è un numero primo in $\mathbb{Z}$, allora $\sqrt{p}$ è irrazionale.

7. Discutere la compatibilita e trovare eventuali soluzioni delle seguenti equazioni diofantee:

   (a) $6 = 15x + 21y$

   (b) $34 = 68x + 12y$.

8. Definire il massimo comun divisore d di n interi $a_1, a_2, \ldots, a_n$ e far vedere che esistono interi $z_1, z_2, \ldots, z_n$ tali che $d = a_1z_1 + a_2z_2 + \cdots + a_nz_n$ e che un intero m è combinazione lineare di $a_1, \ldots, a_n$ se e solo se d divide m.

9. Mostrare che se $n > 5$ ed n *non* è primo, allora

$$(n-1)! \equiv 0 (\text{mod } n).$$

10. (*Teorema di Wilson*) Mostrare che se n è primo allora

$$(n-1)! \equiv -1 (\text{mod } n).$$

11. Dimostrare che se x e y sono due interi dispari, allora $x^2 + y^2$ non è un quadrato.

12. Sia $a \in \mathbb{N}$ non nullo. Scriviamo a in forma decimale:

$$a = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0,$$

con $0 \leq a_i \leq 9$ per $0 \leq i \leq m$ e $a_m \neq 0$. Poniamo $S(a) = \sum_{i=0}^{m} a_i$ (somma delle cifre di a scritto in base 10). Dimostrare usando le congruenze (modulo 10) i ben noti criteri di divisibilità per 2, per 3 e per 9:

(a) $2|a \Leftrightarrow 2|a_0$;

(b) $3|a \Leftrightarrow 3|S(a)$;

(c) $9|a \Leftrightarrow 9|S(a)$.

13. (Criterio di divisibilità per 11). Un intero a è divisibile per 11 se e solo se 11 divide $A(a) = \sum_{i=0}^{m}(-1)^i a_i$ (la somma a segni alterni delle sue cifre, con le notazioni dell'esercizio precedente).

14. Per vedere se n è un numero primo, dimostrare che è sufficiente che esso non sia divisibile per alcun numero primo p tale che $p \leq \sqrt{n}$ (cfr: crivello o setaccio di Eratostene).

15. Si dice *palindrome* un numero $a \in \mathbb{N}$ tale che la successione delle sue cifre decimali sia la stessa se letta da sinistra verso destra o da destra verso sinistra (ad esempio 373 oppure 2002). Mostrare che se a è un palindrome con un numero pari di cifre, allora $11|a$.

16. Determinare gli elementi invertibili (e i loro inversi) di $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$.

17. Sia p un numero primo ed $a \in \mathbb{Z}$ tale che p non divide a. Mostrare, usando il piccolo Teorema di Fermat, che:

$$a^{p-1} \equiv 1 (\text{mod } p).$$

18. Quali e quanti sono gli elementi invertibili di $\mathbb{Z}/24\mathbb{Z}$? Trovare (anche empiricamente!) l'inverso di ognuno degli elementi invertibili.

19. Dimostrare che $n(n+1)(2n+1) \equiv 0 (\text{mod } 6)$

20. Dimostrare che $a^2 + b^2 \equiv 0 (\text{mod } 3)$ implica che $a \equiv 0 (\text{mod } 3)$ e $b \equiv 0 (\text{mod } 3)$.

21. In $\mathbb{Z}/72\mathbb{Z}$ denotiamo con a una delle classi di $5, 21, 34, 45$. Di ciascuna di esse si dica se è o meno invertibile in $\mathbb{Z}/72\mathbb{Z}$. Se lo è, si trovi una classe b tale che $ba = 1$, altrimenti si trovi una classe b tale che $ba = 0$.

22. Si definisca l'applicazione $g : \mathbb{Z}/13\mathbb{Z} \to \mathbb{Z}/13\mathbb{Z}$ tramite la $g(x) = x^5$. Dimostrare che g è biunivoca e determinarne l'inversa.

23. Sia p un primo dispari e $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ l'applicazione definita da $f(z) = z^6$. Dimostrare che essa non è suriettiva.

24. Risolvere, se possibile, la seguente congruenza: $6x \equiv 5 (\text{mod } 7)$.

25. Risolvere, se possibile, la seguente congruenza: $6x \equiv 4 (\text{mod } 10)$.

26. Studiare l'insieme quoziente di $\mathbb{Z}$ rispetto alla relazione di congruenza modulo m, per $m \geq 2$.

27. Costruire l'insieme quoziente di $\mathbb{Z}$ rispetto alla congruenza modulo 6 e studiarne le proprietà relative alle operazioni di addizione e moltiplicazione fra classi. Verificare se $\{\overline{0}, \overline{2}, \overline{4}\}$ è un sottoanello di $\mathbb{Z}/6\mathbb{Z}$.

28. Determinare gli elementi invertibili di $\mathbb{Z}/15\mathbb{Z}$ e verificare che il prodotto di due fra tali elementi è ancora invertibile.

29. Determinare l'opposto e l'inverso, se esiste, di $\overline{-29}$ in $\mathbb{Z}/7\mathbb{Z}$.

30. Risolvere, se possibile, in $\mathbb{Z}/5\mathbb{Z}$, l'equazione $x^2 - \overline{8} = \overline{0}$.

31. In $\mathbb{Z}/11\mathbb{Z}$ risolvere, se possibile, l'equazione $x^2 - \overline{2}x + \overline{3} = \overline{0}$.

32. Usando il teorema di Euler–Fermat, calcolare le ultime due cifre di $n = 81^{82}$.

33. Usando il teorema di Euler–Fermat, calcolare le ultime tre cifre del numero $n = 7^{827}$.