Esercizi Matematica 2 per Matematici Ottobre 2005 - III settimana

1) Calcolare il MCD tra le seguenti coppie di interi, e i coefficienti della loro combinazione che lo calcolano:
(a) 300 e 325;
(b) 198 e 288;
(c) 576 e 840.
(d) 630 e 132;
(e) 285 e 126.

2) Se $a = qb + r$ è la divisione con resto di a per b con a, b positivi, scrivere quoziente e resto delle divisioni di a per $-b$, di $-a$ per b e di $-a$ per $-b$.

3) Mostrare che $\mathrm{MCD}(ac, bc) = c\mathrm{MCD}(a, b)$.

4) Mostrare che $\mathrm{MCD}(a, b + za) = \mathrm{MCD}(a, b)$ se $z \in \mathbf{Z}$. Usare questo risultato per giustificare l'algoritmo di Euclide di calcolo del massimo comun divisore.

5) Dimostrare che $\mathrm{MCD}(a, bc)$ divide, ma in generale non coincide, con il prodotto di $\mathrm{MCD}(a, b)$ e di $\mathrm{MCD}(a, c)$. Mostrare che $\mathrm{MCD}(a, bc) = \mathrm{MCD}(a, b)\mathrm{MCD}(a, c)$ se $\mathrm{MCD}(b, c) = 1$ (cioè se b e c sono coprimi).

6) Siano $a = qb + r$ e $a' = q'b + r'$ le divisioni con resto di a e a' per b. Cosa possiamo dire delle divisioni con resto di aa', $a + a'$, $a - a'$ per b?

7) Siano $a = qb + r$ e $b = q'c + r$ le divisioni con resto di a per b e di b per c. Cosa possiamo dire della divisione con resto di a per c?

8) Date le due divisioni con resto $a = qb + r$ di a per b e $b = q'a + r'$ di b per a, che relazioni vi sono tra q, q', r, r'?

9) Scrivere le tavole di somma e moltiplicazione di $\mathbf{Z}/n\mathbf{Z}$ per $n = 2, 3, 4, 5, 6, 7, 8, 9$. Trovare i divisori di zero, i nilpotenti, gli unipotenti, gli invertibili.
È vero che in $\mathbf{Z}/n\mathbf{Z}$ un elemento è o invertibile o divisore di zero?

10) Studiare iniettività e suriettività della funzione che manda x in x^2 come funzione di $\mathbf{Z}$ in sé e come funzione di $\mathbf{Z}/n\mathbf{Z}$ in sé per $n = 2, 3, 4, 5, 6$.

11) Idem per la funzione che manda x in x^3.

12) Dati $a, b \in \mathbf{N}$, si studi la funzione $f_{(a,b)}\colon \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ definita da $f_{(a,b)}(x, y) = ax + by$.

13) *Rappresentazione posizionale in base qualsiasi.* Sia b un qualunque numero intero maggiore di 1. Dato un numero intero, esso si può rappresentare come sequenza di cifre comprese tra 0 e $b - 1$ nel modo seguente: la sequenza $a_n a_{n-1} \cdots a_2 a_1 a_0$ rappresenta il numero $a_n b^n + a_{n-1} b^{n-1} + \cdots + a_2 b^2 + a_1 b + a_0$ (se $b = 10$, allora si tratta della rappresentazione posizionale in base 10). Dato un numero naturale, come trovare la sua rappresentazione posizionale in base b? [Scrivere un algoritmo, usando ripetutamente la divisione euclidea con resto, per trovare successivamente le cifre a_0, a_1, …, a_n].
Di solito per indicare che una sequenza $a_n a_{n-1} \cdots a_1 a_0$ di cifre rappresenta un numero in base b, si scrive la base al pedice del numero: $(a_n a_{n-1} \cdots a_1 a_0)_b$

14) Scrivere nelle basi 2, 3, 4, 8, 16 i seguenti numeri scritti in base 10: 2, 4, 8, 16, 32, 64, 256, 3, 9, 27, 81, 243 (per le basi $b > 10$ si usano come cifre successive a 9 le lettere maiuscole dell'alfabeto nell'ordine alfabetico; per es. in base 16 le cifre sono $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$).

15) Esprimere in base 10 i seguenti numeri naturali espressi nella base indicata a pedice: 101010_2, 100_8, 101_8, 115_8, 100_{16}, 101_{16}, $11A_{16}$, $A1A_{16}$, $A2C_{16}$, FAC_{16}.

16) Dare dei criteri per decidere se un numero intero scritto in base 10 è divisibile per 2, 3, 4, 5, 6, 7, 8, 9, 11, 13.

17) Ricordare la "regola del 9" per il controllo delle moltiplicazioni (e delle somme), e giustificarla in termini di congruenza modulo 9.

18) Sia p un fissato numero primo. Per ogni numero intero non nullo n, definiamo l'ordine in p nel modo seguente: $\mathrm{ord}_p(n) = a$ se p^a divide n, e p^{a+1} non divide n (dunque è il massimo esponente a tale che p^a divide n). Abbiamo allora una funzione $\mathrm{ord}_p\colon \mathbf{Z}\setminus\{0\} \to \mathbf{N}$; mostrare che soddisfa alle seguenti proprietà:

(a) $\mathrm{ord}_p(n) = 0$ se e solo se p non divide n;
(b) $\mathrm{ord}_p(nm) = \mathrm{ord}_p(n) + \mathrm{ord}_p(m)$ (moltiplicatività);
(c) $\mathrm{ord}_p(n+m) \geq \min(\mathrm{ord}_p(n), \mathrm{ord}_p(m))$ (quando vale l'uguaglianza? quando la disuguaglianza stretta?);
(d) se m divide n allora $\mathrm{ord}_p(m) \leq \mathrm{ord}_p(n)$ (vale il viceversa?).

ord_p è funzione suriettiva? iniettiva?

19) Calcolare ord_3 e ord_5 dei seguenti interi: 15, 16, 27, 69, 125, 330.

20) Sia p un fissato numero primo. Per un intero positivo n, calcolare $\mathrm{ord}_p(p^n)$, $\mathrm{ord}_p(p!)$,$\mathrm{ord}_p(p^n!)$, $\mathrm{ord}_p(n!)$ [usare le cifre in base p], $\mathrm{ord}_p(\binom{p}{n})$.

21) Mostrare che per ogni coppia di numeri interi x e y abbiamo che $(x+y)^p \equiv x^p + y^p \pmod{p}$ (si osservi che i coefficienti binomiali $\binom{p}{i}$ sono divisibili per p se p è primo e $i \neq 0, p$).
Dedurne per induzione il piccolo teorema di Fermat: per ogni intero a, abbiamo che $a^p \equiv a \pmod{p}$.

22) Dire se esistono, ed eventualmente trovarli, interi x, y, z tali che $6x + 28y + 15z = 1$.

23) Risolvere la congruenza $16x \equiv 1000 \pmod{27}$.

24) Discutere il seguente sistema di congruenze: $\begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{6} \end{cases}$

25) Discutere il seguente sistema di congruenze: $\begin{cases} x \equiv 5 \pmod{28} \\ 10x \equiv 35 \pmod{125} \end{cases}$

26) Disponendo di francobolli da 36 e da 45 centesimi, è possibile affrancare un pacco per 2 euro e 34 centesimi? Eventualmente come approssimarlo con la perdita minore? E per un pacco di 3 euro e 51 centesimi?