Esempio. Per risolvere il sistema delle congruenze

$$x \equiv 1 \pmod 6 \qquad x \equiv 5 \pmod 7$$

si scrive $1+6y \equiv 5 \pmod 7$, quindi $6y \equiv 4 \pmod 7$. Si trovano ad esempio per x,y i valori particolari 19 e 3 e dunque la soluzione generale

$$x = 19 + 42\ z.$$

11.10. *Per ogni $x,y \in \mathbf{Z}$ e per ogni primo p, $(x+y)^p \equiv x^p + y^p \pmod p$.*

Per il teorema del binomio (cfr. 6.5.) sappiamo che

$$(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k}y^k + y^p.$$

Perciò è sufficiente dimostrare che la sommatoria è divisibile per p. Ma dalla definizione di $\binom{p}{k}$ si vede che p divide $\binom{p}{k}$ per $1 \leqslant k \leqslant p-1$ e quindi p divide anche $\sum_{k=1}^{p-1} \binom{k}{p} x^{p-k}y^k$.

11.11. Teorema di Fermat: *Se a è un intero e p un primo, allora*

$$a^p \equiv a \pmod p.$$

Dimostrazione: supponiamo anzitutto $a \geqslant 0$ e usiamo l'induzione. Se $a = 0$ il risultato è banale. Sia vero l'asserto per un certo intero a: $a^p \equiv a \pmod p$. Allora per 11.10. $(a+1)^p \equiv a^p + 1^p$; ma $1^p \equiv 1$ e $a^p \equiv a$ comportano $(a+1)^p \equiv a+1$, cioè l'asserto è vero per $a+1$. Per il principio di induzione il teorema è provato per ogni $a \geqslant 0$. Consideriamo adesso il caso $a < 0$. Allora risulta $0 \equiv 0^p \equiv [a+(-a)]^p \equiv a^p + (-a)^p \pmod p$. Ora $-a > 0$, e quindi $(-a)^p \equiv -a$ per il risultato precedente. Si conclude $0 \equiv a^p - a$ come si voleva. Ad esempio $2 \equiv 2^5 = 32 \pmod 5$; $3 \equiv 3^5 = 243 \pmod 5$.

11.12. Applichiamo il teorema cinese del resto per dimostrare la seguente relazione per la funzione di Eulero: $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$ se $(r,s) = 1$, relazione che abbiamo anticipata al numero 9.5.

Sia $U = \{u_1, u_2, \ldots, u_{\varphi(r)}\}$ l'insieme dei numeri interi x tali che $1 \leqslant x \leqslant r$, $(x,r) = 1$. Siano $V = \{v_1, v_2, \ldots, v_{\varphi(s)}\}$ e $W = \{w_1, w_2, \ldots, w_{\varphi(rs)}\}$ gli analoghi insiemi, relativi a s ed rs. Ci proponiamo di definire una biiezione $f: U \times V \to W$, e dunque di provare che W possiede $\varphi(r)\varphi(s)$ elementi.

Sia $(u,v) \in U \times V$; il teorema di 11.10. afferma allora che le congruenze $z \equiv u \pmod r$, $z \equiv v \pmod s$ hanno una soluzione comune, e anzi che ne esiste una (sola) che soddisfa all'ulteriore condizione $1 \leqslant z \leqslant rs$. Chiamiamo w questa soluzione; w è primo con r (perché lo è u, che è congruo a $w \pmod r$); w è primo con s (perché lo è v); dunque w è primo con rs (perché r,s sono coprimi) e in definitiva $w \in W$. Ponendo allora $f(u,v) = w$ si definisce un'applicazione $f: U \times V \to W$. f è iniettiva: se infatti risulta $f(u,v) = w = f(u',v')$, allora $u = w = u' \pmod r$, $v = w = v' \pmod s$ e dunque $u = u'$, $v = v'$. Infine f è suriettiva: partendo infatti da un qualunque $w \in W$ se lo si divide per r si ottiene un resto u che è primo con r (perché lo è w); analogamente, il resto v della divisione di w per s è il primo con s. Ma allora $(u,v) \in U \times V$, $w \equiv u \pmod r$, $w \equiv v \pmod s$, e dunque $f(u,v) = w$.

Esercizi

1) Si dimostrino le familiari *prove del* 9 per la verifica delle addizioni e moltiplicazioni negli interi (si usi la scrittura decimale e si osservi che $10^n \equiv 1 \pmod 9$ per ogni $n > 0$).
2) Si generalizzi il teorema cinese del resto, provando che: se $m_1, m_2, \ldots, m_r$ sono interi a due a due coprimi (cioè $(m_i, m_j) = 1$ se $i \neq j$), allora esiste una soluzione comune delle congruenze $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, $\ldots$, $x \equiv a_r \pmod{m_r}$.

§ 12. Numeri razionali

12.1. Denoteremo con il simbolo $\mathbf{Q}$ l'insieme dei *numeri razionali*. Sono definite in $\mathbf{Q}$ due operazioni: l'addizione e la moltiplicazione; tra le proprietà di queste operazioni, ricordiamo le seguenti:

A 1 ASSOCIATIVITÀ DELL'ADDIZIONE:
per ogni $x,y,w \in \mathbf{Q}$, $(x+y)+w = x+(y+w)$;

A 2 ELEMENTO NEUTRO ADDITIVO: *esiste un unico elemento* 0 (leggi *zero*) *di* $\mathbf{Q}$, *tale che* $0+x = x = x+0$ *per ogni* $x \in \mathbf{Q}$;

A 3 OPPOSTO: *per ogni $x \in \mathbf{Q}$ esiste un unico elemento $-x$ di* $\mathbf{Q}$ (che si dice *opposto* di x) *tale che* $x+(-x) = 0 = (-x)+x$;

A 4 COMMUTATIVITÀ DELL'ADDIZIONE: *per ogni $x,y \in \mathbf{Q}$, $x+y = y+x$;*