due interi x,y sono congrui modulo m ($\neq 0$) se e solo se, divisi per m, danno luogo al medesimo resto. Sia infatti $x = mq_1 + r_1$, $y = mq_2 + r_2$, $0 \leqslant r_1, r_2 < m$. Se $r_1 = r_2$ allora $x - y = m(q_1 - q_2)$ cioè $x \equiv y \pmod m$. Viceversa da $x \equiv y \pmod m$ segue per qualche $z \in \mathbf{Z}$,

$$y = x + mz \quad \text{quindi} \quad y = mq_1 + r_1 + mz = m(q_1 + z) + r_1.$$

Per l'unicità del (quoziente e del) resto nella divisione euclidea, si conclude $q_1 + z = q_2$ e $r_2 = r_1$.

11.3 Per la congruenza, modulo un prefissato intero m, valgono proprietà che richiamano quelle delle uguaglianze: ad esempio, per ogni $x,y,z \in \mathbf{Z}$

a) $x \equiv x$, RIFLESSIVITÀ

b) *se* $x \equiv y$ *allora* $y \equiv x$, SIMMETRIA

c) *se* $x \equiv y$ *e* $y \equiv z$ *allora* $x \equiv z$, TRANSITIVITÀ

d) *se* $x \equiv y$ *allora* $x + z \equiv y + z$,

e) *se* $x \equiv y$ *allora* $xz \equiv yz$.

Tutte queste proprietà sono facili conseguenze della definizione: ad esempio, la transitività si prova osservando che se $m \mid (x - y)$ e se $m \mid (y - z)$ allora m divide $x - z = (x - y) + (y - z)$.

11.4 È bene osservare che l'ultima proprietà di 11.3 non si inverte. Ad esempio $7 \cdot 2 \equiv 1 \cdot 2 \pmod{12}$ non comporta $7 \equiv 1 \pmod{12}$. Questo avviene perchè il fattore 2, che si vorrebbe *cancellare* in entrambi i membri, è un divisore del modulo. Vale però la seguente proprietà: se z è primo con m, allora da $xz \equiv yz \pmod m$ segue $x \equiv y \pmod m$. Infatti per ipotesi m divide $xz - yz = (x - y)z$ ed $(m,z) = 1$. Ma allora, come si è visto in 8.4, $m \mid (x - y)$ come si voleva.

11.5 PROBLEMA: *assegnati $m,b,c \in \mathbf{Z}$ esiste un intero x tale che risulti $cx \equiv b \pmod m$*? Proveremo che *una soluzione x* di questa congruenza *esiste se e solo se $(m,c) \mid b$*.

Dimostrazione: necessità. Se questa congruenza ha soluzione, allora, per qualche $y \in \mathbf{Z}$ si ha $cx - b = my$, e quindi $b = cx - my$ è un multiplo di (m,c) (cfr. 8.1.). *Sufficienza.* Viceversa supponiamo che (m,c) sia un divisore di b; poichè (cfr. 8.1.) (m,c) si scrive nella forma $ct + ms$ (per opportune scelte di $t,s \in \mathbf{Z}$) allora, per qualche $z \in \mathbf{Z}$, si ha $b = (m,c)z = (ct + ms)z$, da cui risulta $c(tz) - b = -m(sz)$ e $c(tz) \equiv b \pmod m$. Ma allora tz è una soluzione.

11.6. Ad esempio, la congruenza $6x \equiv 5 \pmod 4$ non ha soluzioni perchè $2 = (4,6) \nmid 5$. Invece la congruenza $12x \equiv 15 \pmod{39}$ ha soluzioni perchè $3 = (39,12) \mid 15$. Per determinare una soluzione si può seguire la dimostrazione di 11.5. (applicando l'algoritmo di Euclide). Si trova:

$$3 = 1 \cdot 39 + (-3) \cdot 12, \qquad 15 = 5 \cdot 3 = 5 \cdot 39 + (-15) \cdot 12,$$

da cui si ottiene $12 \cdot (-15) \equiv 15 \pmod{39}$, cioè -15 è una soluzione.

11.7. Se x è una soluzione della congruenza $cx \equiv b \pmod m$ allora è una soluzione anche $x + zm/(m,c)$ per ogni scelta di $z \in \mathbf{Z}$. Infatti risulta $c[x + zm/(m,c)] = cx \pm z[m,c] = b + my \pm z[m,c]$ ove si è sfruttata la eguaglianza $[m,c] \cdot (m,c) = |mc|$ (cfr. 8.5.). Ora $z[m,c]$ è multiplo di m, e quindi $c[x + zm/(m,c)] \equiv b \pmod m$ come si voleva. Viceversa, se x,x' sono due soluzioni, allora $cx = b + my$ e $cx' = b + my'$ con $y,y' \in \mathbf{Z}$, quindi risulta $c(x - x') = m(y - y')$ e, infine, $[c/(m,c)](x - x') = [m/(m,c)](y - y')$. Ora $c/(m,c)$ e $m/(m,c)$ sono primi fra loro e quindi $m/(m,c) \mid (x - x')$. In altre parole $x' = x + zm/(m,c)$ per qualche $z \in \mathbf{Z}$. Si conclude che, *una volta determinata una soluzione particolare, tutte le altre si ottengono da essa aggiungendole un arbitrario multiplo di $m/(m,c)$*. Nell'esempio di 11.6 la *soluzione generale* è dunque

$$x = -15 + z \cdot 13, \qquad \text{con } z \in \mathbf{Z}.$$

11.8. Un importante corollario è il seguente. *Sia p un numero primo e sia c un intero non divisibile per p. Allora la congruenza $cx \equiv b \pmod p$ ammette soluzione; tutte le soluzioni differiscono per multipli di p.* (Si usa dire perciò che la soluzione è *unica modulo p*). Se, ad esempio, $p = 7$, $b = 1$, allora si trovano le congruenze:

$$1 \cdot 1 \equiv 1 \qquad 2 \cdot 4 \equiv 1 \qquad 3 \cdot 5 \equiv 1 \qquad 6 \cdot 6 \equiv 1 \qquad (\text{mod } 7)$$

11.9 TEOREMA CINESE DEL RESTO: *Siano r,s interi primi tra loro. Allora le congruenze $x \equiv a \pmod r$, $x \equiv b \pmod s$ hanno una soluzione comune.* La soluzione generale si ottiene aggiungendo ad una soluzione particolare un arbitrario multiplo di rs.

Infatti, per ogni $y \in \mathbf{Z}$, $x = a + yr$ è una soluzione della prima congruenza. Tale x è soluzione anche della seconda se e solo se $a + yr \equiv b \pmod s$, cioè $yr \equiv b - a \pmod s$. Come si è visto in 11.5, un tale y esiste, perchè per ipotesi $(r,s) = 1$. Infine, se anche x^* è soluzione delle due congruenze iniziali, allora $x - x^* \equiv 0 \pmod r$ e $x - x^* \equiv 0 \pmod s$. Ma allora $x - x^*$ è multiplo di r e di s, quindi anche di $[r,s] = rs$. Viceversa è chiaro che se x è soluzione, anche $x + rsz$ lo è per ogni $z \in \mathbf{Z}$.