GIOVANNI CUTOLO — ESEMPI DI EQUAZIONI CONGRUENZIALI E LORO SOLUZIONI

1 $324x \equiv_{508} 127$ non ha soluzioni (2 divide 324 e 508, non 127)

2 $120x \equiv_{164} 128$ ha soluzioni: (4 è un MDC tra 120 e 164 e divide 128). Troviamole.

Dividiamo tutto per 4: l'equazione diventa $30x \equiv_{41} 32$ (equazione congruenziale ridotta: 30 e 41 sono coprimi). Eseguiamo l'algoritmo euclideo:

$$\begin{aligned} \underline{41} &= (1)\,\underline{30} + \underline{11} \\ \underline{30} &= (2)\,\underline{11} + \underline{8} \\ \underline{11} &= (1)\,\underline{8} + \underline{3} \\ \underline{8} &= (2)\,\underline{3} + \underline{2} \\ \underline{3} &= (1)\,\underline{2} + \underline{1} \\ \underline{2} &= (2)\,\underline{1} \quad \text{(non serve)} \end{aligned} \qquad \begin{aligned} \underline{11} &= (1)\,\underline{41} + (-1)\,\underline{30} \\ \underline{8} &= (1)\,\underline{30} + (-2)\,\underline{11} \\ \underline{3} &= (1)\,\underline{11} + (-1)\,\underline{8} \\ \underline{2} &= (1)\,\underline{8} + (-2)\,\underline{3} \\ \underline{1} &= (1)\,\underline{3} + (-1)\,\underline{2} \end{aligned}$$

Dalla seconda colonna ricaviamo:

$$\begin{aligned} 1 &= (1)\,\underline{3} + (-1)\,\underline{2} = (1)\,\underline{3} + (-1)(\underline{8} + (-2)\underline{3}) = (-1)\,\underline{8} + (1 + (-1)(-2))\,\underline{3} = (-1)\,\underline{8} + (3)\,\underline{3} \\ &= (-1)\,\underline{8} + (3)(\underline{11} + (-1)\,\underline{8}) = (3)\,\underline{11} + (-1 + (3)(-1))\,\underline{8} = (3)\,\underline{11} + (-4)\,\underline{8} \\ &= (3)\,\underline{11} + (-4)(\underline{30} + (-2)\,\underline{11}) = (-4)\,\underline{30} + (3 + (-4)(-2))\underline{11} = (-4)\,\underline{30} + (11)\underline{11} \\ &= (-4)\,\underline{30} + (11)(\underline{41} + (-1)\,\underline{30}) = (11)\underline{41} + (-4 + 11(-1))\underline{30} = (11)\underline{41} + (-15)\underline{30} \end{aligned}$$

Pertanto, $1 = (11)\underline{41} + (-15)\underline{30}$; abbiamo trovato una coppia soluzione dell'equazione diofantea $30x + 41y = 1$; più significativamente: abbiamo scoperto che vale $(-15)30 \equiv_{41} 1$, cioè abbiamo scoperto che l'inverso di $[30]_{41}$ in $\mathbb{Z}_{41}$ è $[-15]_{41}$. A questo punto, sappiamo che l'unica classe in $\mathbb{Z}_{41}$ che, moltiplicata per $[30]_{41}$, dia $[32]_{41}$ è $([30]_{41})^{-1}[32]_{41} = [-15]_{41}[32]_{41} = [(-15)32]_{41}$. Questa classe è l'insieme delle soluzioni, in $\mathbb{Z}$, dell'equazione congruenziale originaria, $120x \equiv_{164} 128$.

In alternativa: da $(-15)30 \equiv_{41} 1$, moltiplicando per 32, otteniamo $32(-15)30 \equiv_{41} 32$, dunque $32(-15)$ è una soluzione dell'equazione congruenziale e quindi (poiché 30 e 41 sono coprimi) $[(-15)32]_{41}$ è l'insieme di tutte le sue soluzioni in $\mathbb{Z}$.

Per gli appassionati: facendo qualche calcolo (lo verificheremo più avanti) si può osservare che vale $(-15)32 \equiv_{41} 12$, quindi l'insieme delle soluzioni si può anche descrivere come $[12]_{41}$.

Quello appena presentato NON È il modo più rapido di risolvere l'equazione congruenziale considerata. Vediamo qualche alternativa. Eseguendo l'algoritmo euclideo non necessariamente con le divisioni aritmetiche, ne abbiamo una versione più veloce:

$$\begin{aligned} \underline{41} &= (1)\,\underline{30} + \underline{11} \\ \underline{30} &= (3)\,\underline{11} + (\underline{-3}) \\ \underline{11} &= (-4)\,(\underline{-3}) + (\underline{-1}) \\ \underline{-3} &= (3)(\underline{-1}) \quad \text{(non serve)} \end{aligned} \qquad \begin{aligned} \underline{11} &= (1)\,\underline{41} + (-1)\,\underline{30} \\ (\underline{-3}) &= (1)\,\underline{30} + (-3)\,\underline{11} \\ (\underline{-1}) &= (1)\,\underline{11} + (4)\,(\underline{-3}) \\ \text{(ovvero } \underline{1} &= (-1)\,\underline{11} + (-4)(\underline{-3})\text{)} \end{aligned}$$

che richiede qualche passaggio in meno nella fase successiva:

$$\begin{aligned} 1 &= (-1)\,\underline{11} + (-4)(\underline{-3}) = (-1)\,\underline{11} + (-4)(\underline{30} + (-3)\underline{11}) = (-4)\,\underline{30} + ((-1) + (-4)(-3))\underline{11} = (-4)\,\underline{30} + (-11)\underline{11} \\ &= \ldots \text{(siamo già al terzo rigo del calcolo precedente)} \end{aligned}$$

Si può fare ancora meglio: 30 e 32 sono, evidentemente, congrui rispettivamente a -11 e -9 modulo 41, quindi la nostra equazione congruenziale si può riscrivere come $-11x \equiv_{41} -9$, ovvero (spostando termini tra destra e sinistra, oppure moltiplicando per -1, evidentemente invertibile modulo 41) come $11x \equiv_{41} 9$. Le divisioni si riducono ancora:

$$\begin{aligned} \underline{41} &= (4)\,\underline{11} + (\underline{-3}) \\ \underline{11} &= (-4)\,(\underline{-3}) + (\underline{-1}) \end{aligned} \qquad \begin{aligned} (\underline{-3}) &= (1)\,\underline{41} + (-4)\,\underline{11} \\ (\underline{-1}) &= (1)\,\underline{11} + (4)\,(\underline{-3}) \end{aligned}$$

ed abbiamo:

$$1 = (-1)\,\underline{11} + (-4)(\underline{-3}) = (-1)\,\underline{11} + (-4)(\underline{41} + (-4)\underline{11}) = (-4)\,\underline{41} + ((-1) + (-4)(-4))\underline{11} = (-4)\,\underline{41} + (15)\underline{11}$$

dunque $15 \cdot 11 \equiv_{41} 1$ e così l'insieme delle soluzioni dell'equazione è $[9 \cdot 15]_{41} = [135]_{41} = [12]_{41}$ (infatti $135 = 3 \cdot 41 + 12$).

3 $4x \equiv_{10} 8$ ha ovviamente 2 come soluzione in $\mathbb{Z}$. L'insieme di tutte le soluzioni non è $[2]_{10}$ ma $[2]_5$, perché in forma ridotta l'equazione diventa $2x \equiv_5 4$, notare: 2 e 5 sono coprimi. Si può osservare che, ad esempio, $7 \in [2]_5 \smallsetminus [2]_{10}$, quindi $[2]_5$ è strettamente contenuto in $[2]_{10}$; è facile anche verificare che $[2]_5$ è l'unione disgiunta di $[2]_{10}$ e $[7]_{10}$, quindi, l'equazione data, vista come equazione in $\mathbb{Z}_{10}$: $[4]_{10}X = [8]_{10}$ ha esattamente due soluzioni: $[2]_{10}$ e $[7]_{10}$.

4 L'equazione $45x \equiv_{47} 476$ si risolve immediatamente senza bisogno di calcoli: evidentemente $45 \equiv_{47} -2$ e $476 \equiv_{47} 6$, quindi l'equazione è equivalente a (nel senso che ha le stesse soluzioni di) $-2x \equiv_{47} 6$, ovvero (dividendo -2 e 6 per -2, che è invertibile modulo 47) a $x \equiv_{47} -3$, che è già risolta: l'insieme delle soluzioni è $[-3]_{47}$.

5 L'equazione $32x - 4 \equiv_{18} 8$ non è altro che un modo diverso di scrivere $32x \equiv_{18} 12$. Per semplificarla possiamo dividere tutto per 2 (MCD tra 32 e 18), ottenendo $16x \equiv_9 6$. Da questa, siccome 2 è coprimo con 9, quindi invertibile modulo 9, dividendo 16 e 6 per 2 ricaviamo l'equazione equivalente $8x \equiv_9 3$; ma $8 \equiv_9 -1$, quindi possiamo riscrivere questa come $-x \equiv_9 3$, ovvero $x \equiv_9 -3$, e l'equazione originaria è risolta. In alternativa: da $32x \equiv_{18} 12$ passiamo a $-4x \equiv_{18} 12$, perché $-4 \equiv_{18} 32$, quindi, dividendo tutto per 2, a $-2x \equiv_9 6$; possiamo ancora dividere -2 per 2, o direttamente per -2, perché, di nuovo, 2 e -2 sono invertibili modulo 9, per ottenere ancora $x \equiv_9 -3$ e così l'insieme $[-3]_9$ di tutte le soluzioni.

6 Un esempio simile: $14x \equiv_{111} 21$ ha le stesse soluzioni di $2x \equiv_{111} 3$; qui bisogna fare attenzione al fatto che 7, per il quale abbiamo diviso 14 e 21, e 111 sono coprimi. Come facciamo a saperlo? Be', $111 \equiv_7 111 - 70 = 40$, siccome 42 è multiplo di 7 certamente non lo è 40 (infatti $40 \equiv_7 -2$), quindi 7 non divide 111; poiché 7 è primo questo garantisce che 7 e 111 sono coprimi. A questo punto dobbiamo risolvere $2x \equiv_{111} 3$. Possiamo farlo usando l'algoritmo euclideo, oppure osservando che, siccome 3 è dispari come 111, allora $3 + 111$ è pari, ne ricaviamo l'intero $(3 + 111)/2 = 114/2 = 57$, allora $2 \cdot 57 = 3 + 111 \equiv_{57} 3$ e così vediamo che 57 è soluzione dell'equazione. Dal momento che l'equazione è ridotta (2 e 111 sono coprimi), l'insieme delle soluzioni è $[57]_{111}$.

7 Non sempre riusciamo ad identificare a prima vista il massimo comun divisore non negativo tra il modulo ed il coefficiente dell'incognita dell'equazione, o almeno a stabilire se questi sono coprimi. Possiamo utilizzare l'algoritmo anche in questi casi.

Ad esempio, consideriamo l'equazione congruenziale $238x \equiv_{323} 51$. Usiamo l'algoritmo euclideo (velocizzato) per la ricerca dei MDC tra 238 e 323:

$$\begin{aligned} \underline{323} &= (1)\,\underline{238} + \underline{85} \\ \underline{238} &= (3)\,\underline{85} + (\underline{-17}) \\ \underline{85} &= (-17)\,(5), \end{aligned}$$

vediamo così che -17 e quindi 17 sono i MCD cercati. Siccome 17 divide $51 = 3 \cdot 17$, l'equazione ha soluzioni. Per trovarne una, come fatto in precedenza, ricaviamo un'espressione di 17 come combinazione lineare di 238 e 323. Abbiamo $\underline{17} = (-1)\,\underline{238} + (3)\,\underline{85}$ e $\underline{85} = \underline{323} + (-1)\,\underline{238}$, quindi $\underline{17} = (-1)\,\underline{238} + (3)(\underline{323} + (-1)\,\underline{238}) = (3)\,\underline{323} + (-4)\underline{238}$.

Allora $238(-4) \equiv_{323} 17$. Moltiplicando per $51/17 = 3$ otteniamo $238(-12) \equiv_{323} 51$, dunque -12 è una soluzione della nostra equazione. Per ottenere l'insieme di tutte le soluzioni in $\mathbb{Z}$ dobbiamo dividere il modulo 323 per 17 (MCD tra 323 e 238) ottenendo $323/17 = 19$; l'insieme delle soluzioni è dunque $[-12]_{19}$.

8 Osservazione finale: e se volessimo risolvere $323x \equiv_{238} 51$ o, ad esempio, $323x \equiv_{238} 34$? Non dovremmo ripetere la procedura: l'uguaglianza $\underline{17} = (3)\,\underline{323} + (-4)\underline{238}$ che abbiamo ottenuto al punto precedente, infatti, mostra anche che vale $3 \cdot 323 \equiv_{238} 17$, quindi moltiplicando 3 per $3 = 51/17$ otteniamo una soluzione di $323x \equiv_{238} 51$, moltiplicando 3 per $2 = 34/17$ ne otteniamo una di $323x \equiv_{238} 34$. Gli insiemi di tutte le soluzioni in $\mathbb{Z}$ di queste due equazioni sono dunque $[9]_{14}$ e $[6]_{14}$, dal momento che $238/17 = 14$.

Questo non deve sorprendere, e discorso analogo si applica a tutti gli esempi precedenti. Risolvere un'equazione congruenziale $ax \equiv_m c$ è infatti sostanzialmente equivalente a risolvere l'equazione diofantea $ax + my = c$, che è anche equivalente a risolvere (a meno di scambiare i nomi delle variabili) l'equazione congruenziale $mx \equiv_a c$; il problema di determinare una soluzione di $ax \equiv_m c$ è quindi sostanzialmente equivalente a quello di determinarne una per $mx \equiv_a c$.