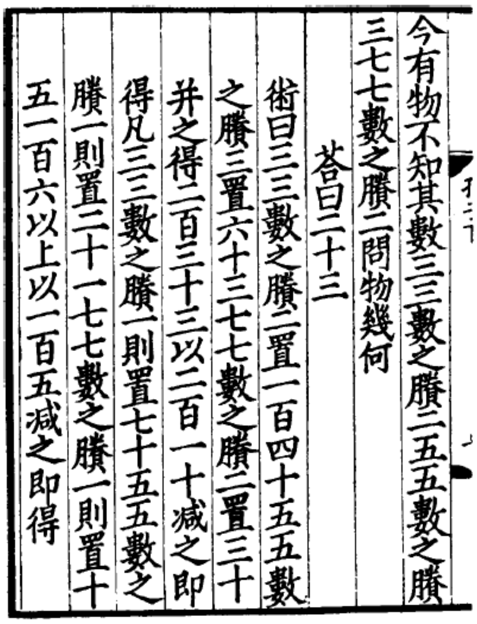
Il Teorema Cinese del Resto – Le origini

La prima fonte conosciuta è il trattato cinese 孙子算经 (*Canone aritmetico del maestro Sun*), che si ritiene sia stato composto tra il III e il V secolo.

Vi compare il seguente problema:



今有物不知其數三三數之賸二五五數之賸
三七七數之賸二問物幾何
荅曰二十三
術曰三三數之賸二置一百四十五五數
之賸三置六十三七七數之賸二置三十
幷之得二百三十三以二百一十减之即
得凡三三數之賸一則置七十五五數之
賸一則置二十一七七數之賸一則置十
五一百六以上以一百五减之即得

Prima di darne la traduzione, premettiamo che il procedimento risolutivo, presentato nella stessa opera nel caso particolare proposto, e poi generalizzato da altri autori nei secoli successivi, nella lingua cinese prende il nome di *Dà yăn shù* ("metodo della grande espansione"): 大衍術. Il termine è tratto dalla tecnica oracolare dello *Yì jīng* (易经, *Classico dei mutamenti*), che ha una forte componente aritmetica. Il nome si riferisce all'operazione di sostituire le congruenze assegnate con altre, in cui intervengono prodotti dei moduli (le cosiddette *espansioni*): sono quelli che noi abbiamo indicato con N_i. Ricordiamo che questi sono divisori del numero N, che è anche loro minimo comune multiplo (oltre che prodotto di tutti i moduli del sistema di congruenze). Per questo motivo N viene detto *yăn mŭ* ("la madre dell'espansione"): 衍母.

Veniamo ora alla traduzione. Il testo si legge per colonne, dall'alto verso il basso e da destra a sinistra.

今 Ora (supponiamo di)
有 avere
物 delle cose
不 e non
知 sapere
其 il loro
數 numero.

(Se)
三、tre
三 a tre,
數之 le contiamo
賸 il resto
二; è due;
五、cinque
五 a cinque,
數之 le contiamo,
賸 il resto
三; è tre;
七、sette
七 a sette
數之 le contiamo,
賸 il resto
二。è due.
問 Si chiede
物 le cose
幾何 quante siano.

Il sistema di congruenze è:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Questo è l'enunciato. Segue la soluzione:

答曰：二十三。
La risposta dice: 23.

術曰:
Il metodo dice:

三、三數之，賸二，
Tre a tre contatele, il resto è 2,

置一百四十;
poni 140;

五、五數之，賸三，
Cinque a cinque contatele, il resto è 3,

置六十三;
poni 63;

七、七數之，賸二，
Sette a sette contatele, il resto è 2,

置三十。
poni 30.

并之，
Somma questi,

得二百三十三。
il risultato è 233.

In questo modo l'autore ottiene una soluzione particolare. Il calcolo effettuato è sostanzialmente equivalente a quello che conosciamo dal corso. Per trovare la nostra c, noi considereremmo interi c_1, c_2, c_3 tali che si abbia

$$\begin{cases} N_1 c_1 & \equiv & b_1 & (\bmod n_1) \\ N_2 c_2 & \equiv & b_2 & (\bmod n_2) \\ N_3 c_3 & \equiv & b_3 & (\bmod n_3) \end{cases}$$

E quindi formeremmo la somma $N_1c_1 + N_2c_2 + N_3c_3$. Si noti che l'i-esimo addendo si può descrivere come un multiplo di N_i che sia congruo a b_i modulo n_i. Questo può essere ottenuto trovando prima un multiplo di N_i che sia congruo a 1 modulo n_i, e poi moltiplicandolo per b_i. Questa è la strada seguita da maestro Sun: ricordiamo che i dati del problema, con la nostra notazione, sono:

$$\begin{aligned} &N_1 = 35, N_2 = 21, N_3 = 15, \\ &n_1 = 3, \quad n_2 = 5, \quad n_3 = 7, \\ &b_1 = 2, \quad b_2 = 3, \quad b_3 = 2. \end{aligned}$$

Quindi si tratta di trovare:
- un multiplo di **35** che sia congruo a 1 modulo **3** (e questo è 70), e moltiplicarlo per **2**, si ottiene **140**;
- un multiplo di **21** che sia congruo a 1 modulo **5** (e questo è 21), e moltiplicarlo per **3**, si ottiene **63**;
- un multiplo di **15** che sia congruo a 1 modulo **7** (e questo è 15), e moltiplicarlo per **2**, si ottiene **30**.

Il procedimento di maestro Sun non si ferma qui. Prosegue considerando il numero N (la "madre dell'espansione") nella maniera seguente: sottrae N (= 105) da 233 tante volte quanto possibile, per ottenere quella noi conosciamo come la più piccola soluzione positiva, ossia $233 - 2 \cdot 105 = 23$. Questo è il numero indicato nella risposta.