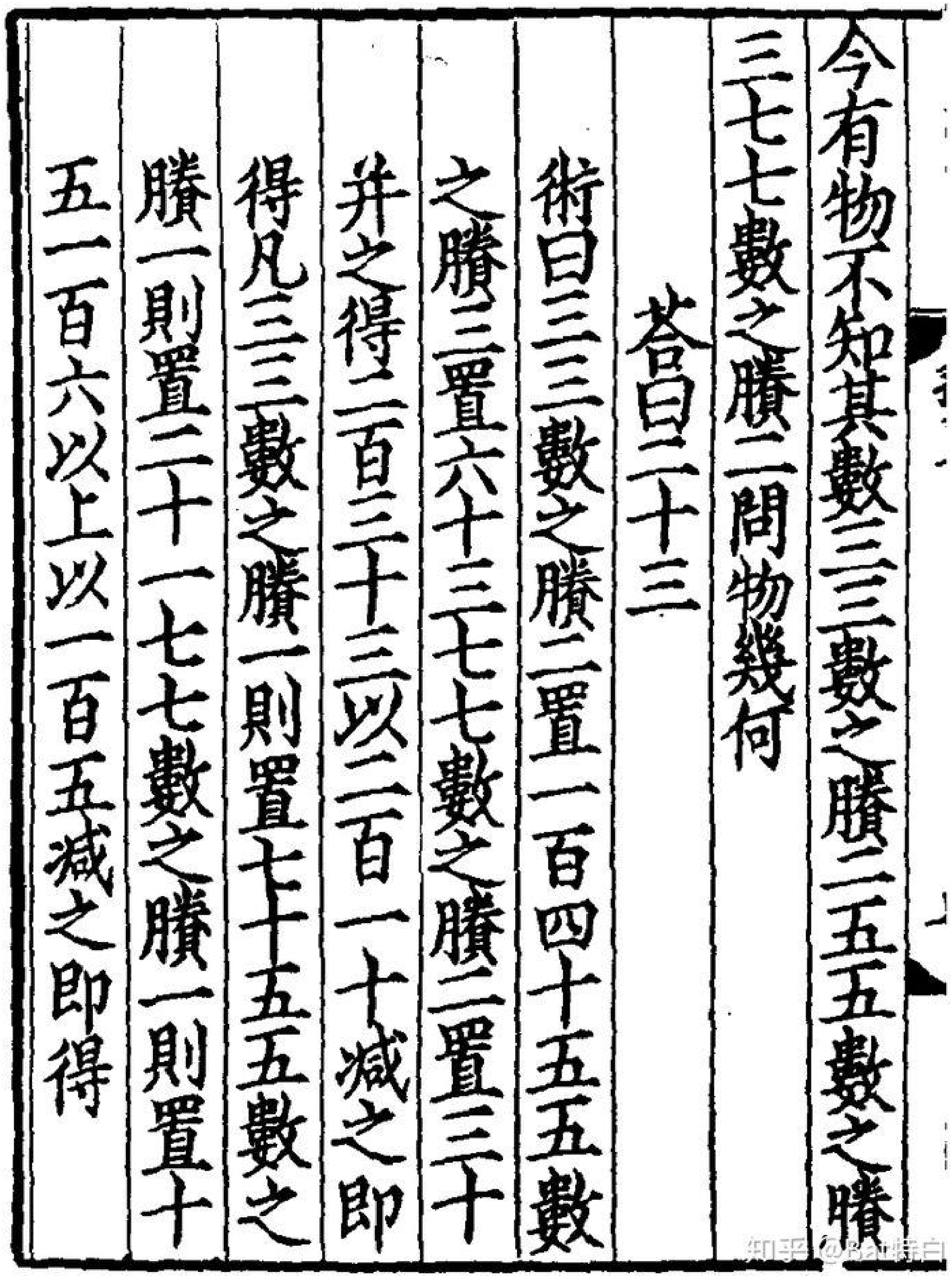
数论基础选讲

山东省实验中学
宁华

问题引入一

- 《孙子算经》-卷下-第26题：


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
并之得二百三十三以二百一十減之即
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減之即得

问题引入—“物不知数”问题：

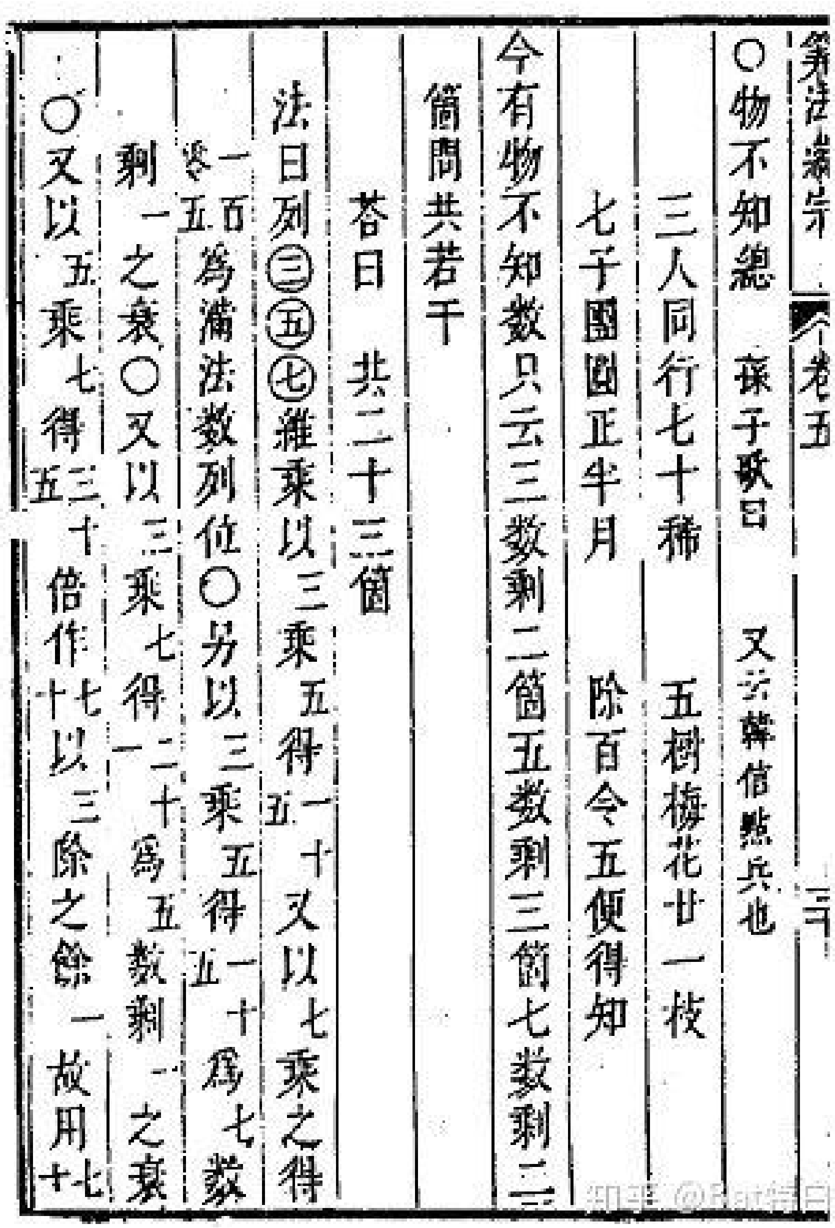
- 《孙子算经》-卷下-第26题：
- 今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？
- 答曰：二十三。
- 术曰：三三数之剩二，置一百四十；五五数之剩三，置六十三，七七数之剩二，置三十，并之。得二百三十三，以二百一十减之，即得。凡三三数之剩一，则置七十；五五数之剩一，则置二十一；七七数之剩一，则置十五；一百六以上以一百五减之即得。

- 一个整数除以3余2、除以5余3、除以7余2，求这个整数。
- 答案：23
- 解法：由于除以3余2，因此加上一个140；由于除以5余3，因此加上一个63；由于除以7余2，因此加上一个30；这三个数的和是140+63+30=233，再减去210，就得到了23了。
- 这么说吧，只要是除以3余了一个1，就加上一个70；只要是除以5余了一个1，就加上一个21；只要是除以7余了一个1，就加上一个15。然后累加。超过了106就减去105就行了。

孙子歌诀

- 明朝 程大位 《直指算法统宗》
- （简称《算法统宗》）卷五

- 孙子歌：
- 三人同行七十稀，
- 五树梅花廿一枝，
- 七子团圆正半月，
- 除百令五便得知。


算法統宗 卷五 三

○物不知總 孫子歌曰 又云韓信點兵也

三人同行七十稀 五樹梅花廿一枝

七子團圓正半月 除百令五便得知

今有物不知數只云三三數剩二箇五五數剩三箇七七數剩二

箇問共若干

答曰 共二十三箇

法曰列三五七維乘以三乘五得一十五又以七乘之得

一百零五為滿法數列位○另以三乘五得一十五為七數

剩一之衰○又以三乘七得二十一為五數剩一之衰

○又以五乘七得三十五倍作七十以三除之餘一故用七十

- 问题1：
- 计算一个整数x，使得它满足除以3余2、除以5余3、除以7余2。

- 如果能够找到三个整数 x1, x2, x3，使得：

- x1 除以3余2、除以5余0、除以7余0；
- x2 除以3余0、除以5余3、除以7余0；
- x3 除以3余0、除以5余0、除以7余2；

- 那么令 x = x1 + x2 + x3, 就很容易验证这时的 x 就满足除以3余2、除以5余3、除以7余2。
- 分别称找到整数 x1, x2, x3 的问题为问题1-1、问题1-2、问题1-3。可以看出这三个问题本质上是类似的。

- 下面对问题1-1继续分解，如果能够找到一个整数y1 满足y1 除以3余1、除以5余0、除以7余0，那么令 x1=2*y1 ，就很容易验证这时的 x1 就满足除以3余2、除以5余0、除以7余0。

- 因此定义

- 问题1-1-1为：寻找整数 y1 满足 y1 除以3余1、除以5余0、除以7余0；
- 问题1-2-1为：寻找整数 y2 满足 y2 除以3余0、除以5余1、除以7余0；
- 问题1-3-1为：寻找整数 y3 满足 y3 除以3余0、除以5余0、除以7余1。

- 这三个问题本质上是相同的。
- 如果找到了y1,y2,y3, 那么就可以取 x = 2*y1+3*y2+2*y3。

- 下面就以问题1-1-1为例：
- 寻找整数 z 使得 z 除以3余1、除以5余0、除以7余0。
- 于是 z 一定是 5*7=35 的倍数，假设 z=35k 。

- 那么就有 $35k \equiv 1 \pmod 3$ ，而这时的 k 就是 5*7 模3的逆，将这个 k 记作 $[35^{-1}]_3$ ，那么 z 就等于 $5*7*[(5*7)^{-1}]_3$，恰好就是 5*7*2=70 ，对应“凡三三数之剩一，则置七十”一句及“三人同行七十稀”一句。

- 于是类推得到，

- 问题1-2-1的解答是 $3*7* [(3*7)^{-1}]_5$ ，恰好就是 3*7*1 = 21 ，对应“五五数之剩一，则置二十一”一句及“五树梅花廿一枝”一句；

- 问题1-3-1的解答是 $3*5* [(3*5)^{-1}]_7$，恰好就是 3*5*1 = 15 ，对应“七七数之剩一，则置十五”一句及“七子团圆月正半”一句。

- 所以将分解的问题复原，可得：

- $x = 2*(5*7*[(5*7)^{-1}]_3) + 3*(3*7* [(3*7)^{-1}]_5) + 2*(3*5* [(3*5)^{-1}]_7)$

- 最后，注意到，如果 x 满足除以3余2、除以5余3、除以7余2，那么 x + 3*5*7 也同样满足。

- 因此要计算满足要求的最小的非负整数，就只需要计算总和除以 105 的余数即可。——对应“除百令五便得知”一句。

- 下面要讨论的是：如果有多个满足要求的整数，那么它们之间有什么关系呢？
- 假设 X, Y 都满足“除以3余a、除以5余b、除以7余c”。
- 观察 X-Y 会发现， X-Y 满足“除以3余0、除以5余0、除以7余0”。因此 X-Y 一定是 3*5*7 =105 的倍数。
- 这也就是说，在“模105同余”的意义下，之前通过分解问题、组合解答的方法所得到的 X 恰恰就是唯一解。

中国剩余定理(Chinese remainder theorem, CRT) 孙子定理

- 下面把这个问题一般化：
- 假设整数 m1,m2,...,mn 两两互素，则对于任意的整数 a1,a2,...,an ，方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

- 都存在整数解，且若X, Y 都满足该方程组，则必有 $X \equiv Y \pmod{N}$
- 其中 $N = \prod_{i=1}^{n} m_i$
- 具体而言， $x \equiv \sum_{i=1}^{n} a_i \times \frac{N}{m_i} \times \left[\left(\frac{N}{m_i} \right)^{-1} \right]_{m_i} \pmod{N}$