代数结构HW2答案

张朔宁

March 19, 2025

7. 证明：当$n > 0$时，$n(n+1)$不是一个平方数

   Proof. 由于$n^2 < n(n+1) < (n+1)^2$，故其夹在两个相邻的平方数之间，不可能是平方数 □

11. 用30张票面值为5分、1角（10分）、2角5分（25分）的纸币，换5元（500分）钱。问有多少种不同的兑换方法?

    解. 设5分、10分、25分纸币的数量分别为x, y, z，则有方程组:

$$
\begin{aligned}
x + y + z &= 30 \\
5x + 10y + 25z &= 500 \\
x, y, z &\in \mathbb{N}
\end{aligned}
$$

消元可得$y + 4z = 70$, 通解为

$$
\begin{cases}
x = 5 - 3t \\
y = 10 + 4t \\
z = 15 - t, t \in \mathbb{Z}
\end{cases}
$$

注意到$x, y, z \geq 0$ 因此t只能取$1, 0, -1, -2$. 故共有4种不同兑换方法

注. t不一定要≥ 0, t只是一个中间变量。

14. 证明：每个大于3的素数模6或与1同余或与5同余。

    Proof. $p \mod 6$ 共有6中不同的结果$0, 1, 2, 3, 4, 5$，又$p > 3$,因此
    若$p \equiv 0, 2, 4 \pmod 6$,则$2 \mid p$, 与p是素数矛盾
    若$p \equiv 3 \pmod 6$, 则$3 \mid p$, 与p是素数矛盾
    因此$p \equiv 1, 5 \pmod 6$ □

16. 证明：若一个整数的各位数字之和能被3整除,那么该数也能被3整除.

    Proof. 由于$10 \equiv 1 \pmod 3$, 两边同时k次方, 因此$10^k \equiv 1 \pmod 3, \forall k$
    设原数为$N = \sum_{i=0}^{k} a_i \cdot 10^i$, 则$N \equiv \sum_{i=0}^{k} a_i \pmod 3 \equiv 0 \pmod 3$. □

    注. 这次证明题不难，绝大部分同学做的很好，但也有少部分同学的证明存在错误。错误的主要原因是其证明完全依靠直觉，用自然语言而非数论语言去证明，这种证明是不严谨的。
    随着数论学习的深入，证明题的复杂性会逐渐增加，大部分题目并不能仅凭直觉一眼得出答案，需要一步一步严格推导。

18. 解下列线性同余方程:

    (2). $3x \equiv 6 \pmod{18}$;

    (4). $3x \equiv 1 \pmod{17}$.

解. (2). 原式等价于$x \equiv 2 \pmod 6$, 故$x \equiv 2, 8, 14 \pmod{18}$

(4). $\gcd(3,17) = 1$, 原方程有唯一解. 不难验证$x \equiv 6 \pmod{17}$是解

19. 解下列同余方程组:

(2). $\begin{cases} x \equiv 31 \pmod{41} \\ x \equiv 59 \pmod{26} \end{cases}$

(4). $\begin{cases} 2x \equiv 1 \pmod 5 \\ 3x \equiv 2 \pmod 7 \\ 4x \equiv 1 \pmod{11} \end{cases}$

解. (2)先解方程$\begin{cases} 26b_1 \equiv 1 \pmod{41} \\ 41b_2 \equiv 1 \pmod{26} \end{cases}$ 解得 $\begin{cases} b_1 \equiv 30 \pmod{41} \\ b_2 \equiv 7 \pmod{26} \end{cases}$ 因此$x \equiv 30 \cdot 31 \cdot 26 + 7 \cdot 59 \cdot 41 \equiv 605 \pmod{1066}$

(4)原方程等价于$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 7 \\ x \equiv 3 \pmod{11} \end{cases}$ 由方程解的唯一性，$x \equiv 3 \pmod{385}$是原方程的解

注. (a) 当方程的解比较容易看出的时候，可以直接猜出答案，再证明解的唯一性。

(b) 有同学第(4)问算出来331这个答案，是因为没有对方程左边的系数归一化就直接套公式。要注意书上的公式只能处理$x \equiv a_i \pmod{m_i}$,不能处理$b_i x \equiv a_i \pmod{m_i}$

(c) 这次作业19题的错误率非常高，大家在算完方程组后，可以把算出来的解代回原方程验证一下(非常重要！)

21. 求满足 $2 \mid n, 3 \mid (n+1), 4 \mid (n+2), 5 \mid (n+3), 6 \mid (n+4)$ 的最小整数 $n (> 2)$.

解. 把原题条件改写为

$$\begin{cases} n \equiv 0 \pmod 2 \\ n \equiv 2 \pmod 3 \\ n \equiv 2 \pmod 4 \\ n \equiv 2 \pmod 5 \\ n \equiv 2 \pmod 6 \end{cases}$$

等价于

$$\begin{cases} n \equiv 2 \pmod 3 \\ n \equiv 2 \pmod 4 \\ n \equiv 2 \pmod 5 \end{cases}$$

由方程解的唯一性, $n \equiv 2 \pmod{60}$ 故n最小为62

注. 在使用中国剩余定理前，应该先验证各个方程模的元素是否两两互素