《代数结构》作业反馈

学院：计算机科学与技术学院　　Edited By 李昱祁　　2021 年 4 月 4 日

第三周作业

课堂内容

- 2.3.1 同余式及其性质
- 2.3.2 线性同余方程
- 2.3.3 线性同余方程组

1　3 月 23 日周二作业

1.1　Ch2 P17

作业题 1.1:

(1) 证明:

$$10^k \equiv (-1)^k \ (mod\ \ 11)\ ,\ k \in N$$

(2) 推出一个整数能被 11 整除的判别法

Part(1)

1. 由于 $10 \equiv -1\ (mod\ \ 11)$，再根据课本 2.3 节同余式性质 6^* 即可推出

2. 大部分同学的做法都是将 10^k 写为 $(11-1)^k$，之后进行二项展开：

$$(11-1)^k = \sum_{i=0}^{k} C_k^i \cdot 11^i \cdot (-1)^{k-i} = \sum_{i=1}^{k} C_k^i \cdot 11^i \cdot (-1)^{k-i} + (-1)^k$$

其中 $\sum_{i=1}^{k} C_k^i \cdot 11^i \cdot (-1)^{k-i} \equiv 0\ (mod\ \ 11)$，故得证.

Part(2)

1. 显然题目是希望利用 (1) 中结论来进行判断。一个十进制数字 num 可以表示为

$$num = a_0 + a_1 \cdot 10^1 + \ldots\ldots + a_n \cdot 10^n = \sum_{i=0}^{n} a_i \cdot 10^i$$

而 (1) 中已经证明 $10^k \equiv (-1)^k \ (mod\ 11)$，再利用性质 4* 即可得到

$$num \equiv \sum_{i=0}^{n} a_i \cdot (-1)^i \equiv \sum_{i=0}^{\lfloor n/2 \rfloor} a_{2i} - \sum_{i=0}^{\lceil n/2 \rceil - 1} a_{2i+1} \ (mod\ 11)$$

若要求 $11|num$ 即 $num \equiv 0 \ (mod\ 11)$，则等价于

$$\sum_{i=0}^{\lfloor n/2 \rfloor} a_{2i} - \sum_{i=0}^{\lceil n/2 \rceil - 1} a_{2i+1} \equiv 0 \ (mod\ 11)$$

也即 num 的 10 进制表示中，奇数位之和与偶数位之和的差值模 11 等于 0

本题反馈

第 (1) 问同学们出错较少；

第 (2) 问一些同学没有考虑到差值为 11 的倍数的情况，比如 209

1.2 Ch2 P18

作业题 1.2:

解下列线性同余方程:

$$(1)\ 2x \equiv\ 1 \ (mod\ 17)$$

$$(2)\ 3x \equiv\ 6 \ (mod\ 18)$$

$$(3)\ 4x \equiv\ 6 \ (mod\ 18)$$

$$(4)\ 3x \equiv\ 1 \ (mod\ 17)$$

题解

1.

$$2x \equiv 1(mod\ 17) \Leftrightarrow 2x \equiv 18(mod\ 17) \Leftrightarrow^{(2,17)=1} x \equiv 9(mod\ 17)$$

2.

$$3x \equiv 6(mod\ 18) \Leftrightarrow x \equiv 2(mod\ 6) \Leftrightarrow x \equiv 2, 8, 14(mod\ 18)$$

3.

$$4x \equiv 6(mod\ 18) \Leftrightarrow 2x \equiv 3(mod\ 9) \Leftrightarrow 2x \equiv 12(mod\ 9)$$
$$\Leftrightarrow^{(2,9)=1} x \equiv 6(mod\ 9) \Leftrightarrow x \equiv 6, 15(mod\ 18)$$

4.

$$3x \equiv\ 1 \ (mod\ 17) \Leftrightarrow 3x \equiv 18 \ (mod\ 17) \Leftrightarrow^{(3,17)=1} x \equiv 6 \ (mod\ 17)$$

本题反馈

比较简单，出错很少。

对于线性同余方程 $ax \equiv b(mod\ m)$，最终应该指出 x 模 m 不同余的所有解。有一些同学最后的答案格式不太标准。

2 3 月 25 日周四作业

2.1 Ch2 P19

作业题 2.1:

解下列同余方程组:

$$(1)\begin{cases} x \equiv 1 (mod\ 2) \\ x \equiv 1 (mod\ 3) \end{cases} \quad (2)\begin{cases} x \equiv 31 (mod\ 41) \\ x \equiv 59 (mod\ 26) \end{cases} \quad (3)\begin{cases} x \equiv 1 (mod\ 2) \\ x \equiv 1 (mod\ 3) \\ x \equiv 6 (mod\ 7) \end{cases} \quad (4)\begin{cases} 2x \equiv 1 (mod\ 5) \\ 3x \equiv 2 (mod\ 7) \\ 4x \equiv 1 (mod\ 11) \end{cases}$$

Part(1):

- 对于 (1)，根据同余式性质 9^* 可得 $x \equiv 1\ (mod\ 6)$

Part(2):

- 对于 (2)，之后可以直接用中国剩余定理求解，或者推导如下：：

$$(m_1, m_2) = (41, 26) = 1 \Rightarrow (m_1, m_2) \mid (a_1 - a_2)$$

故该方程组有模 $[41, 26] = 1066$ 唯一解。

$$\begin{aligned} x \equiv 31\ (mod\ 41) &\Leftrightarrow x = 41k + 31 \\ x \equiv 59\ (mod\ 26) &\Leftrightarrow 41k + 31 = 59\ (mod\ 26) \\ &\Leftrightarrow 41k \equiv 28\ (mod\ 26) \\ &\Rightarrow^{5^*} 41k \equiv 28\ (mod\ 13) \end{aligned}$$

而

$$\begin{aligned} 41k \equiv 28\ (mod\ 13) \Leftrightarrow 41k \equiv 41\ (mod\ 13) &\Leftrightarrow^{(41,13)=1} k \equiv 1\ (mod\ 13) \\ &\Leftrightarrow k \equiv 1 (mod\ 26) 或 k \equiv 14 (mod\ 26) \end{aligned}$$

再由 $41k \equiv 28\ (mod\ 26)$ 可得 $k \equiv 14 (mod\ 26)$

所以 $x = 41k + 31 = 41(26m + 14) + 31 = 1066m + 605 \Leftrightarrow x \equiv 605\ (mod\ 1066)$

Part(3):

- 对于 (3), 下面展示用中国剩余定理求解的方法:
  $a_1 = 1, a_2 = 6, m_1 = M_2 = 6, m_2 = M_1 = 7$，之后求解 b_1、b_2:

$$M_1 b_1 \equiv 1 (mod\ 6) \Leftrightarrow 7b_1 \equiv 1 (mod\ 6) \Leftrightarrow 7b_1 \equiv 7 (mod\ 6) \Leftrightarrow^{(7,6)=1} b_1 \equiv 1 (mod\ 6)$$

$$M_2b_2 \equiv 1(mod\ 7) \Leftrightarrow 6b_1 \equiv 1(mod\ 7) \Leftrightarrow^{(2,7)=1} 3b_1 \equiv 4(mod\ 7) \Leftrightarrow^{(3,7)=1} b_1 \equiv 6(mod\ 7)$$

取一个符合题意的解 $b_1 = 1$，$b_2 = 6$

所以最终解为 $x \equiv M_1b_1a_1 + M_2b_2a_2 \equiv 7 \cdot 1 \cdot 1 + 6 \cdot 6 \cdot 6(mod\ \ 6 \cdot 7)$

即 $x \equiv 13(mod\ 42)$

Part(4):

- 对于 (4), 需要先求解 3 个线性同余方程，

$$\begin{cases} 2x \equiv & 1(mod\ 5) \\ 3x \equiv & 2(mod\ 7) \\ 4x \equiv & 1(mod\ 11) \end{cases} \Rightarrow \begin{cases} x \equiv & 3(mod\ 5) \\ x \equiv & 3(mod\ 7) \\ x \equiv & 3(mod\ 11) \end{cases}$$

之后可以通过中国剩余定理求解，也可根据性质 9^* 直接求出 $x \equiv 3(mod\ 385)$

本题反馈

除了第 1 题之外，其余小问均有不少同学出错。主要问题有二：

(1) 运算错误

(2) 使用中国剩余定理时把其中一些值搞混了，比如有些同学计算 $\sum_{j=1}^{r} M_jb_ja_j$ 时算成了 $\sum_{j=1}^{r} M_jb_jm_j$; 有些同学第 (4) 问在把题干中方程组变形后，又把原来的 3 个值 $1, 2, 1$ 当作了 $a_1, a_2, a_3 \cdots\cdots$ 可能对于定理的推导过程还不是很理解。因为这个定理的证明是构造性的，所以建议大家对其要熟悉。(CRT 在考试中也是高频考点)

2.2 Ch2 P21

作业题 2.2:

求满足 $2|n$、$3|(n+1)$、$4|(n+2)$、$5|(n+3)$、$6|(n+4)$ 的最小整数 $n(n > 2)$

将题中条件写为同余式形式:

$$\begin{cases} n \equiv & 2(mod\ 2) \\ n \equiv & 2(mod\ 3) \\ n \equiv & 2(mod\ 4) \\ n \equiv & 2(mod\ 5) \\ n \equiv & 2(mod\ 6) \end{cases}$$

再由同余式性质 9^* 即可求得 $n \equiv 2(mod\ [2, 3, 4, 5, 6])$ 即 $n \equiv 2(mod\ 60)$ 最小满足条件的 n 为 62

本题反馈

大部分同学求出了正确答案。我批改的作业中一些同学算出的结果是 $n \equiv 2(mod\ 30)$，我看了看都属于计算错误，还望细心

总结

(1)

本次作业涉及到的课堂内容，首先便是同余式 & 同余方程。课本 2.3.1 节给出了 9 条基本性质，其中前 3 条说明了模 m 同余是一个等价关系 (参考 4.2 节)。

第 4、5、6 条性质根据定义很好理解; 性质 5 的逆命题并不成立，因为若设 $m = cd$，1 个模 d 同余类会对应 c 个模 m 同余类! 比如 19 题第 (3) 问上述做法中，一些同学解出了 $k \equiv 1(mod\ 13)$ 之后直接认为 $k \equiv 1(mod\ 26)$，之后求出了错误的答案

需要注意的是第 7 条性质，它指出了与 $x \equiv y(mod\ m)$ 等价的是 $ax \equiv ay(mod\ am)$!
因为对于 $a, m \neq 0$，那么显然 $x = km + y$ 与 $ax = kam + ay$ 是等价的

对于性质 6：$x \equiv y(mod\ m) \Rightarrow ax \equiv ay(mod\ m)$ 是因为 $m|(x-y) \Rightarrow m|a(x-y)$
而它的逆命题则不一定成立，因为 a 与 m 可能有大于 1 的公因子；若 $(a, m) = 1$，则其逆命题成立，即性质 8

第 9 条性质在本次作业中经常出现，此时 $m_i(1 \leq i \leq r)$ 是 $x - y$ 的因子，比较容易理解

这些基本性质在解方程的过程中会经常使用，需要做到熟练运用

(2)

解线性同余方程 $ax \equiv b(mod\ m)$，实际上就是求解线性不定方程 $ax + my = b$，并求出 x 通解中所有模 m 不同余的情况
一般地，我们解方程的步骤如下：

* 先令 $b = b + km$ 使得 $(a, b) \neq 1$
* 之后 a, b, m 一起约去它们之间的最大公因子
* 新的 a, b 再约去它们之间的最大公因子

重复上述步骤，直至 x 前的系数为 1；之后找出模初始 m 不同余的所有解

(3)

关于中国剩余定理的一些说明:
* 如此构造出的 M_i、m_i 互质，因此 $(m_i, M_i) = 1$，由定理 2.2 知 $km_1 + M_i b_i = 1$ 有解，故 $M_i b_i \equiv 1(mod\ m_i)$ 有解，通过它来构造 y 中满足" 模 m_i 等于 a_i" 的那部分
* 对于 $i \neq j$，$m_i \mid M_j$，因此 $M_j b_j \equiv 0(mod\ m_i)$
* 因此对 $\forall\, i(1 \leq i \leq r)$ 均有:

$$\begin{aligned} y \equiv \sum_{j=1}^{r} M_j b_j a_j &\equiv \sum_{j=1}^{r} \sum_{j \neq i} M_j b_j a_j + M_i b_i a_i (mod\ m_i) \\ &\equiv 0 + 1 \cdot a_i \equiv a_i (mod\ m_i) \end{aligned}$$

上述三部分老师上课时都已经讲过。如果仍对该定理不太明白可以再思考下 ~