CS201 Assignment 3 问题总结

2022 年 4 月

1 Q1

多数同学都是满分，无问题。

2 Q5

既要证明由左至右也要证明由右至左，且不能直接使用未经证明的结论，否则证明题就失去意义了。

3 Q6

这道题绝大多数分数扣在证明过程中，一些重要过程的缺失会让下一步的结论显得莫名其妙。需要指出的一点是一些同学在证明途中出现了分数表达式，式子本身没问题，但在分析约数的时候需要注意分母会消去分子的约数。必要时需要进行分类讨论。

个别同学的证明比较有意思：在反证的过程中找到了 a 和 b 的一个“公约分数”（即该数可以由 a 和 b 分别除以某个整数得到），以此声称 $gcd(a, b)$ 的范围和题设矛盾。可惜的是这些同学没有给出详细的证明。有兴趣的同学可以尝试严格证明一下。

4 Q7

- 部分同学使用了不规范的书写符号，例如% 表示 mod，这次只是提醒一下，不扣分。
- 许多同学在计算过程中，粗心大意，造成简单的加减乘除法错误，导致扣分，希望做作业能认真一些。
- a 小问，有的同学忽略了 a is not divisible by p 的条件，希望以后能仔细读题。

5 Q8

希望同学们好好参考一下答案，将符号和过程写规范，写完整。

6 Q9

以下问题均出自第 9 题：

$gcd(a,b) = 1$ 不代表 $a \ mod \ b = 1$。不少同学在第 9 题中直接得出了 $ax \ mod \ m = x \ mod \ m$ 的结论，这是不对的。

第 9 题里，因为定义域和值域大小相同的，因此确实只要证明单射和满射里任意一个即可。但在作业中，请务必体现出你是怎么得出这个结论的（比如说明一下这两个集合有相同的基数），不要证完一个就直接说是双射了。

有些同学试图通过反证来证明这个函数不可能不是双射。需要注意的是，“函数是双射”的否定为“函数不是单射或不是满射”。这意味着不是单射和不是满射都需要讨论证明，只证明“不可能不是单射”并不能证明原命题。

有些同学在证明 onto 时，是这样找反函数的：“因为 $y = ax\%m$，所以存在 $y = ax+km$，因此有反函数 $x = (y - km)/a$，从而证明 onto。”这里的问题是，$y = ax + km$ 中，k 的取值取决于 x，换句话说，x 和 k 都是变量，所以 $(y - km)/a$ 并不仅仅是关于 y 的函数。虽然对本题而言，对同一个 y 来说 k 取值确实唯一（因为甚至 x 都唯一，为什么?），但这并不代表这种构造反函数的方法是正确的。

一些注意事项：

比较重要的，以下命题，对于 a, m：

$$ax \equiv 1 \ (mod \ m) \ has \ solution \ ... \ (1)$$

$$gcd(a, m) = 1 \ ... \ (2)$$

$$\exists (s, t) \ sa + tm = 1 \ ... \ (3)$$

虽然这三个命题确实都是等价的，但大多数情况下还是不要直接说它们等价，因为我们学的定理并不能直接表示出它们。比如，我们可以由贝祖定理直接得到 (2)->(3)，但不能由贝祖定理直接得到 (3)->(2)，这需要同学们再去认真查看定义。虽然 (3)->(2) 确实是贝祖定理的引理，但做题时还是需要给出证明的。在这两题的批改中，直接使用上述推论没有算错，但还是希望同学们在考试时注意。

以及一些同学还会存在 $=$ 和 $\equiv$ 错用的情况，望注意。

7 Q14

这题的平均分相对较低。我对这道题的理解是这个命题等价于课件 Lecture 8 p25（或者教材 p268）的引理。因此这道题是不适合直接援引这个引理的。同时，课件中的 Euclidean Algorithm 和 Bezout’s Identity 也是基于该引理的，引用这些结论会出现循环论证，因此我在这道题的给分比较严格。望见谅。

这道题的一般解法是证明 $d \mid a \wedge d \mid m \rightarrow d \mid b$ 和 $d \mid b \wedge d \mid m \rightarrow d \mid a$ 从而得出最大公约数相等的结论。一部分同学讨论的时候漏掉了一边或者误认为证明一边就能声称相等。这里要吸取一下教训。

8 Q15

这题整体完成的比较好，极个别同学没看到 back substitution 的题干以及出现计算错误，比较可惜。最后请记得写出完整解集（给出表达数或指出同余关系均可）。

9 Q16

- 在同余式中应当使用恒等号“≡”，避免使用等于号“=”。
- 使用整除表达时，请尽量考虑可读性问题。例如当想表达“b 与 c 之和能被 a 整除”的意思时，建议为加法运算加上括号，即：

$$a \mid (b + c)$$

- 在 Q16 中，有同学使用 back substitute 方法解题，但最后得到的结果为

$$x \equiv 23 \ (mod\ 900)$$

或

$$x \equiv 143 \ (mod\ 900)$$

等等。
此类答案都是不对的，问题在于取模过大。我们可拿标准答案来进行对比：

(i) 标准答案为 $x \equiv 23 \ (mod\ 30)$，可表示为 $x = 23 + 30k_1 \ (k_1 \in Z)$
(ii) 取 $x \equiv 23 \ (mod\ 900)$ 做对比，可表示为 $x = 23 + 900k_2 \ (k_2 \in Z)$
(iii) 我们令 $k_1 = 1$，则有 $x = 53$，而我们发现无论 k_2 如何取值，都不能得到 $x = 53$。
(iv) 这说明 $x \equiv 23 \ (mod\ 900)$ 与标准答案 $x \equiv 23 \ (mod\ 30)$ 是不等价的。
(v) 同理可得 $x \equiv 143 \ (mod\ 900)$ 与标准答案 $x \equiv 23 \ (mod\ 30)$ 不等价。

事实上，当使用 back substitute 方法时，最终所取的模应当为所有同余式的模的最小公倍数。在本题中，三个同余式的模分别为 6,10,15, 它们的最小公倍数为 30，因此最后的结果是模 30 的。
在使用中国剩余定理时，我们也能发现相同的规律。我们会把 6,10,15 分别作分解质因子的操作，得到 2,3,5。运用定理最后得到的模为质因子 2,3,5 的乘积，而质因子的乘积恰好就是最小公倍数。

- 在 Q16 中，有同学得到如下答案：

$$x \equiv 53 \ (mod\ 30)$$

该答案是正确的。但从严谨考虑，模 30 的同余式中最好不要出现大于或等于 30 的数字，因此该答案定性为未化至最简。

10 Q17

- Q17 可使用多种方法证明，现取一种作为例子：

（其他步骤略）
假设 $gcd(M, p) = p$，且 $gcd(M, q) = 1$,
根据费马小定理 (步骤与参考答案相同，故略) 可得 $C^d \equiv M \ (mod\ q)$,

因此有 $C^d \equiv M^{ed} \equiv M \ (mod\ q)$,
令 $M^{ed} = M + tq \ (t \in Z)$,
得 $M \mid t$ (详细证明见下方 **[1]**),
又由 $gcd(M,p) = p$ 得 $p \mid M$，根据整除的传递性, 有 $p \mid t$，可设 $t = kp \ (k \in Z)$,
因此

$$\begin{aligned} & M^{ed} = M + tq \\ \Rightarrow\ & M^{ed} = M + kpq \\ \Rightarrow\ & C^d \equiv M^{ed} \equiv M \ (mod\ pq) \end{aligned}$$

[1] 为推导 $M \mid t$，我们可做如下分析:

(i) 要证 $M \mid t$，只需证 $\frac{t}{M}$ 的值恒为整数。
(ii) 由 $M^{ed} = M + tq$ 可得 $\frac{t}{M} = \frac{M^{ed-1}-1}{q}$，因此只需证 $\frac{M^{ed-1}-1}{q}$ 恒为整数。
(iii) 已知 $de \equiv 1 \ (mod\ (p-1)(q-1)\ )$，可设 $de - 1 = k_1 \cdot (p-1)(q-1) \ (k_1 \in Z)$
(iv) 根据费马小定理，有 $M^{q-1} \equiv 1 \ (mod\ q)$，可设 $M^{q-1} = 1 + k_2 \cdot q \ (k_2 \in Z)$
(v) 因此有

$$\frac{M^{ed-1}-1}{q} = \frac{M^{k_1 \cdot (p-1)(q-1)}-1}{q} = \frac{(1+k_2 \cdot q)^{k_1 \cdot (p-1)}-1}{q}$$

(vi) 而 $\frac{(1+k_2 \cdot q)^{k_1 \cdot (p-1)}-1}{q}$ 恒为整数，因此 $M \mid t$ 得证。

方法仅供参考，如有错误尽请指正。

- 在 Q17 中，有同学考虑到 $gcd(M,p) = 1$ 与 $gcd(M,q) = 1$ 同时成立的情况，实际上该情况是不存在的，我们可使用反证法分析:

  假设 $gcd(M,p) = 1$ 与 $gcd(M,q) = 1$ 同时成立时，我们可以得到 $gcd(M,pq) = 1$，然而这与题设条件 $gcd(M,pq) > 1$ 矛盾。

- 在 Q17 中，有同学使用如下说法:

  $\because gcd(e,(p-1)(q-1)\ ) = 1$
  根据贝祖定理 (Bezout's Theorem)，得 $ed + k(p-1)(q-1) = 1$

  此种说法不严谨。我们可做如下分析:

  (i) 假设 $gcd(a,b) = d$，且 $sa + tb = d$.
  (ii) 任取 $s \in Z$，则 $t = \frac{d-sa}{b}$.
  (iii) 任举一反例，例如取 $s = 0, d < b$，我们发现此时 $t = \frac{d}{b}$，t 不为整数。
  (iv) 由此可得，当 s 为任意整数时，不一定存在 $t \in Z$，使得 $sa + tb = d$.

  事实上，贝祖定理 (Bezout's Theorem) 只说明在 $gcd(a,b) = d$ 的前提下，丢番图方程

$sa + tb = d$ 的解 (s, t) 的存在性，此解并不是可任取的。
另一方面，$ed + k(p-1)(q-1) = 1$ $(k \in Z)$ 的结论，实际上来源于

$$\begin{cases} de \equiv 1 \ (mod \ (p-1)(q-1) \ ) \\ gcd(e, \ (p-1)(q-1) \ ) = 1 \end{cases}$$

这是题目本身提供的条件。