第五次作业反馈

> 反馈主笔：王原龙
>
> 最后修改：2021.4.20

习题参考解答与要点整理

Ch2 38

2. $9x\equiv 2(mod\ 29)$

   解：由于29的最小原根为2，我们在两边取离散对数得到$ind_2 9+ind_2 x\equiv 1(mod\ 28)$，查原根指数表得知模29意义下有$ind_2 9=10$（注意根据指数的定义，此处是严格等于），带入得到$ind_2 x\equiv 19(mod\ 28)$，再查表得知$x\equiv 2^{19}\equiv 26(mod\ 29)$如果没想到查表计算$2^{19}$的话可以这样计算：首先$2^5\equiv 32\equiv 3(mod\ 29)$，然后
   $2^{19}\equiv 2^4\times(2^5)^3\equiv 2^4\times 3^3\equiv 2^4\times(-2)\equiv -2^5\equiv -3\equiv 26(mod\ 29)$

   - 虽然理论上这题不化简2^{19}也是正确的，但是从简洁的角度还是希望大家化简到$\{0,1,\cdots,28\}$当中

3. $x^9\equiv 2(mod\ 29)$

   解：同上题取对数，得到$9ind_2 x\equiv 1(mod\ 28)$，容易得到$ind_2 x\equiv -3\equiv 25(mod\ 28)$，故查原根指数表有$x\equiv 2^{25}\equiv 11(mod\ 29)$，或$x\equiv(2^5)^5\equiv 3^5\equiv 3^3\times 3^2\equiv(-2)\times 9\equiv 11(mod\ 29)$

Ch2 40

解：欲求37的12个原根，首先要知道它的一个原根，这可以简单地通过查表得到，为2。然后由书上29页最上面一段的结论（书上此处有印刷错误，将最后一句中 l 改为 p 即可），通过对2求指数得到其它原根如下：

$$
\begin{aligned}
2^5 &\equiv 32 \\
2^7 &\equiv 17 \\
2^{11} &\equiv 13 \\
2^{13} &\equiv 15 \\
2^{17} &\equiv 18 \\
2^{19} &\equiv 35 \\
2^{23} &\equiv 5 \\
2^{25} &\equiv 20 \\
2^{29} &\equiv 24 \\
2^{31} &\equiv 22 \\
2^{35} &\equiv 19
\end{aligned}
$$

由于2是37的最小原根，所以这里的计算可以通过查原根与指数表直接得到，当然也可以如上题所述方法进行计算。当然建议大家练习计算的方法，因为考试考到不一定会给完整的原根指数表。

- 注：同样建议大家化简结果

Ch2 41

证明：由于$q \mid (a^p+1)$，于是$-a^p \equiv 1(mod\ q)$，由于p是奇素数，所以$(-a)^p \equiv 1(mod\ q)$，设$-a$的阶为l，则由阶的性质知道$l \mid p$，同样由于p为奇素数，所以 $l=1$ 或 $l=p$ 成立。

1. 当 $l=1$，此时$(-a)^1 \equiv 1(mod\ q)$，即$q \mid (a+1)$
2. 当$l=p$，此时由于$(-a)^p \equiv 1(mod\ q)$，所以显然 $-a$ 并非 q 的倍数，否则$(-a)^p \equiv 0(mod\ q)$所以由欧拉定理，$(-a)^{q-1} \equiv 1(mod\ q)$成立，由阶的定义，$p \mid q-1$ 成立，即存在 k' 使得 $q=k'p+1$ 成立，而由于$q-1$为偶数，所以存在 k 使得 $k'=2k$ 成立，于是 $q=2kp+1$ 成立，原题得证。

- 由于我们改过题目，所以此题难度相较于修改之前稍微加大，但是如果把握了阶部分的知识的话本题的脉络就相对比较清晰了。
- 本题雷同的答案实在是太多了，虽然极大减少了助教工作量，但还是希望大家能够独立思考，即使参考答案也要彻底理解。（此处说的雷同不只是方法一样，解答的组织结构，使用的语言，甚至前面加的引理，使用的字母全都一样）

Ch3 1

1. $\{(x_1,x_2) \mid x_1,x_2 \in \mathbb{N}, x_1+x_2<10\}$

   不是映射，比如$(1,1)$以及$(1,2)$均属于此集合，不满足映射定义中像唯一的要求

2. $\{(y_1,y_2) \mid y_1,y_2 \in \mathbb{R}, y_2=y_1^2\}$

   显然是映射

3. $\{(y_1,y_2) \mid y_1,y_2 \in \mathbb{R}, y_2^2=y_1\}$

   不是映射，如$(4,2)$以及$(4,-2)$均属于此集合，不满足映射定义中像唯一的要求

Ch3 2

1. 通过列举所有自变量的可能知道$R_f=\{-2,-1,0,1,2\}$.
2. $A \to B$的所有映射有$|B|^{|A|}$种，所以所求为$|R_f|^{|\{-1,0,1\}^2|}=5^9$.
   - 很多同学粗心看错题，这里$A=\{-1,0,1\}^2$，所以$|A|=9$.

Ch3 6

证明：

1. 先证g为单射，即$\forall f_1, f_2 \in F, g(f_1) = g(f_2) \Rightarrow f_1 = f_2$.

$$
\begin{aligned}
& g(f_1) = g(f_2) \\
\Rightarrow\ & (f_1(a_1), f_1(a_2), \cdots, f_1(a_n)) = (f_2(a_1), f_2(a_2), \cdots, f_2(a_n)) \\
\Rightarrow\ & (f_1(a_1) = f_2(a_1)) \wedge (f_1(a_2) = f_2(a_2)) \wedge \cdots \wedge (f_1(a_1) = f_2(a_1)) \\
\Rightarrow\ & f_1 = f_2
\end{aligned}
$$

   其中第二行依据为 g 的定义，第三行依据为有序n数组相等的定义（书第4页），第四行依据为映射相等的定义（书36页**定义3.4**）

2. 再证 g 为满射，对$S(B)$中任意元素$(b_{i_1}, b_{i_2}, \cdots, b_{i_n})$，令$f : A \to B$使得$f(a_j) = b_{i_j}$，显然$f \in F$，且由 g 的定义，$g(f) = (f(a_1), f(a_2), \cdots, f(a_n)) = (b_{i_1}, b_{i_2}, \cdots, b_{i_n})$，所以$S(B)$中任意元素皆有原像，所以 g 为满射

综上所述，g 为双射，所以由**定理3.4**，$|F| = |S(B)| = |B|^n = m^n$成立（$S(B)$的势计算由书第四页**定义1.4**以及**定理1.5**得到）

- 注：表面上看这题基本在说废话~~（其实就是在说废话）~~，但是这种严格依据定义与定理的证明方式是希望大家学习的~~（而不是广泛运用显然成立法）~~，这也是迈向形式化证明的重要一步。
- 比较集中的错误点是没有用单射的定义证明单射，而是说对于每个原像能找到唯一像与之对应，但这仅仅是**映射**本身的定义；另外一点是证满射的时候没有显式地给$S(B)$中的每个元素找到原像，只是反复在说对于每个原像能找到唯一像与之对应，但这仅仅是**映射**本身的定义。

Ch3 7

证明：

1. $\alpha(A \cup B) = \alpha(A) \cup \alpha(B)$

   法1：

$$
\begin{aligned}
\alpha(A \cup B) &= \{\alpha(x) \mid x \in A \cup B\} \\
&= \{\alpha(x) \mid (x \in A) \vee (x \in B)\} \\
&= \{\alpha(x) \mid x \in A\} \cup \{\alpha(x) \mid x \in B\} \\
&= \alpha(A) \cup \alpha(B)
\end{aligned}
$$

   - 此方法写起来简单，但是比较容易出错，比如另一个式子就不能简单地用这种方式来做

   法2：

$$
\begin{aligned}
\alpha(A \cup B) &= \{y \in T \mid \exists x((x \in A \cup B) \wedge (\alpha(x) = y))\} \\
&= \{y \in T \mid \exists x(((x \in A) \vee (x \in B)) \wedge (\alpha(x) = y))\} \\
&= \{y \in T \mid \exists x(((x \in A) \wedge (\alpha(x) = y)) \vee ((x \in B) \wedge (\alpha(x) = y)))\} \\
&= \{y \in T \mid \exists x((x \in A) \wedge (\alpha(x) = y)) \vee \exists x((x \in B) \wedge (\alpha(x) = y))\} \\
&= \{y \in T \mid \exists x((x \in A) \wedge (\alpha(x) = y))\} \cup \{y \in T \mid \exists x((x \in B) \wedge (\alpha(x) = y))\} \\
&= \alpha(A) \cup \alpha(B)
\end{aligned}
$$

   - 这种方式稍微严格，但是对于同学们来说命题的运算还是很有可能出错，所以仍然推荐依靠包含关系的反对称性

   法3：

对于任意$y \in \alpha(A \cup B)$，存在 $x \in A \cup B$ 使得$\alpha(x) = y$，若$x \in A$，则由$\alpha(A)$的定义，$y \in \alpha(A)$，故$y \in \alpha(A) \cup \alpha(B)$，否则$x \in B$，则由$\alpha(B)$的定义，$y \in \alpha(B)$，故$y \in \alpha(A) \cup \alpha(B)$，于是$\alpha(A \cup B) \subseteq \alpha(A) \cup \alpha(B)$成立

反之，对于任意$y \in \alpha(A) \cup \alpha(B)$，若$y \in \alpha(A)$，则存在$x \in A$使得$\alpha(x) = y$，由$A \subseteq A \cup B$，$x \in A \cup B$成立，所以$y \in \alpha(A \cup B)$成立。否则$y \in \alpha(B)$，存在$x \in B$使得$\alpha(x) = y$，由$B \subseteq A \cup B$，$x \in A \cup B$成立，所以$y \in \alpha(A \cup B)$成立。综上有$\alpha(A \cup B) \supseteq \alpha(A) \cup \alpha(B)$成立

综上，$\alpha(A \cup B) = \alpha(A) \cup \alpha(B)$成立

2. $\alpha(A \cap B) \subseteq \alpha(A) \cap \alpha(B)$

   证明：

   对于任意$y \in \alpha(A \cap B)$，存在 $x \in A \cap B$ 使得$\alpha(x) = y$，由于$A \cap B \subseteq A$，即存在$x \in A$使$\alpha(x) = y$，于是$y \in \alpha(A)$，由于$A \cap B \subseteq B$，即存在$x \in B$使$\alpha(x) = y$，于是$y \in \alpha(B)$，综上，$y \in \alpha(A) \cap \alpha(B)$，所以$\alpha(A \cap B) \subseteq \alpha(A) \cap \alpha(B)$成立

   对$\alpha(A \cap B) \neq \alpha(A) \cap \alpha(B)$，可取
   $A = \{1, 2\}, B = \{2, 3\}, S = \{1, 2, 3\}, T = \{1, 2\}, \alpha(1) = \alpha(3) = 1, \alpha(2) = 2$，此时
   $A \cap B = \{2\}, \alpha(A \cap B) = \{1\}, \alpha(A) = \alpha(B) = \{1, 2\}, \alpha(A) \cap \alpha(B) = \{1, 2\}$

   - 之所以不能取等就是因为左边的集合中元素原像必须来源于两集合共有的元素，而右边集合中只要在两个集合中各自有原像即可，这两个原像可以不同，所以不必属于交集当中。

- 本题常见的错误为证集合相等只证了一个包含的方向而忽略了另一个；跳步过多，相当于把题又抄了一遍当证明（显然成立法）

Ch3 8

解：

1. α为单射时任取$y \in \alpha(\tilde{A})$，存在$x \in \tilde{A}$使$\alpha(x) = y$，由于α为单射，所以x是唯一的，所以不存在$z \in A$使得$\alpha(z) = y, z \neq A$，于是$y \notin \alpha(A), y \in \widetilde{\alpha(A)}$，**所以**$\alpha(\tilde{A}) \subseteq \widetilde{\alpha(A)}$**成立**

   作为不取等的例子，考虑$S = \{1, 2\}, T = \{1, 2, 3\}, A = \{1\}, \alpha(1) = 1, \alpha(2) = 2$

2. α为满射的时候任取$y \in \widetilde{\alpha(A)}$，则由于$\alpha$为满射，于是存在$x \in S$使得$\alpha(x) = y$，而由于$y \in \widetilde{\alpha(A)}$，所以$x \notin A$，否则$y \in \alpha(A)$，产生矛盾。于是$x \in \tilde{A}, y \in \alpha(\tilde{A})$。**所以**$\alpha(\tilde{A}) \supseteq \widetilde{\alpha(A)}$**成立。**

   作为不取等的例子，考虑$S = \{1, 2\}, T = \{1\}, A = \{1\}, \alpha(1) = \alpha(2) = 1$

- 本题主要问题是大家给出的结论其实不够强，包括比较二者元素个数以及往交并集的方向考虑（严格来说诸如$\alpha(\tilde{A}) \cup \alpha(A) = T$这种答案并没有给出$\alpha(\tilde{A})$和$\widetilde{\alpha(A)}$的关系吧），实际他们的包含关系是可以导出的，而且还能说明这个包含是不能进一步加强的，就像第七题一样，其实本体也是第七题的一个延申。

Ch3 11

解：

1. 此题取法很多，如取$f(x) = \lceil \frac{x}{2} \rceil$（上取整函数），$g(x) = 2x$.
2. 若f为双射，则f^{-1}存在，由于$f \circ g = I_s$，所以在两边作用f^{-1}得到$f^{-1} \circ f \circ g = f^{-1} \circ I_s = f^{-1}$，又因为映射复合有结合性，所以$f^{-1} \circ f \circ g = g$，所以$g = f^{-1}$，所以$g$也为双射，此时$g \circ f = f^{-1} \circ f = I_s$一定成立。

- 部分同学输在了语文上，直接考虑了f为双射的情形导出矛盾，但其实这个题目分两部分。

知识点整理

- 原根与指数，从略

- 映射的定义：

  $f:A\to B$，称f为从A到B的映射，当对于A中的任意元素a，有且仅有唯一的元素$b\in B$使得$f(a)=b$成立。

  f具有集合表示，表示为$f=\{(a,b)\mid a\in A,b\in B,f(a)=b\}$

  $f:A\to B$，$g:A\to B$，则$f=g\Leftrightarrow\forall a\in A,f(a)=g(a)$

- 映射相关定义

  定义域：$f:A\to B$，则称A为f的定义域

  值域$R_f=^{def}\{b\in B\mid\exists a\in A,s.t.\ f(a)=b\}$

  当$f(a)=b$，称a为b的原像，b为a的像

  对于$f:S\to T,A\subseteq S$，$f(A)=^{def}\{f(a)\mid a\in A\}$

  - 注意到$R_f=f(S)$成立，$f(S)$又称像集。
- 特殊映射，设$f:A\to B$

  f是单射等价于$\forall a_1,a_2\in A,f(a_1)=f(a_2)\Rightarrow a_1=a_2$

  f是满射等价于$\forall b\in B,\exists a\in A,s.t.\ f(a)=b$

其它问题整理

从本次作业可以看出，大部分同学并不会写严格的证明，只是在用感性的认知来解释题目要求的命题，缺乏严格的推理依据。比如证明的语言中大量包含如下类似的句子，在作业第6题中：

> g为F到S(B)的映射
>
> 每个f对应不同的f(a_i),f为单射
>
> 所有f(a_i)构成S(B)，则为满射
>
> 综上为双射

这样的证明基本没有任何实际意义，这些话话本身就表意不明确，助教看了知道你仿佛理解这个题命题成立的原因了，但是你所写的文字并不能作为"证明"而被承认。

作为数学证明强调严格性，从已知的条件开始，每一步的推导基本都必须属于下面几种情况中的一个：

- 是题目条件
- 是已证明的定理
- 是定义
- 是假设，服务于分类讨论或反证法

同时所有语言都应尽量用数学语言描述，做到使用的符号要么是约定俗成的使用，如函数使用f,g，要么在前面的叙述中或题目中有其定义

彩蛋——数论与密码学

数论在密码学中有诸多应用，下面展示几个简单的例子

对称密码算法与非对称密码算法

对于信息m，我们欲对其进行加密，而加密是需要密钥的，也就是额外的信息，比如我们将一条消息中的每个字母用字母表中其后的第n个字母代替，如将abc加密为bcd，就是$n=1$的情形，这基本是最简单的加密算法，这时我们引入了n用于加密，它就是所谓的密钥。

若我们用$c=E(m)$表示对m实施加密算法的结果，$m=D(c)$表示对应的解密过程，那么对于对称密码算法，其加密与解密使用相同的密钥，如上面的例子，若要将bcd解密，也要用到$n=1$这一密钥。而对于非对称加密算法，加密与解密的密钥是不一样的，且算法通常有这样的性质：$E(D(m))=D(E(m))$，即加解密算法是可交换的。

公钥密码体制

长久以来我们使用对称密码算法进行加密，因为它计算上比较简单，也符合所谓"解铃还须系铃人"的一种直觉。但是这就要求加密交流的双方提前拥有一个共享的密钥，如果两方是熟人，私下里约定好了还好，但如果是网络上的陌生人，如何在不泄漏对称密钥的情形下完成交流呢？基于此提出了非对称密码算法以及公钥密码体制，其中最著名的就是RSA算法

公钥密码体制中每个人拥有一对密钥，称公钥和私钥，私钥自己掌管，不外泄，而公钥公之于众，可供任何人拿来使用，且满足使用某个人私钥加密的消息可以使用其公钥解密，而使用某个人公钥加密的消息可以使用其私钥解密。这样当Alice需要给Bob发送消息时，使用Bob的公钥加密要发送的信息，而Bob收到消息后用自己的私钥解密即可查看，但别人没有Bob的私钥，所以无法解密消息，这样就在没有对称密钥交换的情形下完成了保密沟通。

当然这里还有衍生问题：比如Alice如何保证自己用的就是Bob的公钥，而不是其他人假冒的Bob的公钥？Bob如何保证是Alice发送的消息而不是别人冒充Alice发送的消息？这些问题都是非常经典且重要的，限于篇幅这里就不再赘述了。

RSA加密算法

铺垫了这么多终于可以进入正题，RSA加密算法就是以数论为基础的非对称加密算法，它的安全性基于大整数质因数分解计算的困难程度，即要对足够大的整数进行质因数分解是困难的。

RSA密码算法将待加密的内容视为一整数（因为是二进制串，所以这是可以做到的），所以对消息加密等同于对整数加密，为了这一目的，我们考虑加密消息m，取一很大的整数$N=pq>m$，其中p,q为很大的质数，令$z=\phi(N)=(p-1)(q-1)$，再取$e<z$使得$(e,z)=1$，所以存在d使得$ed\equiv 1(mod\ z)$，然后令密文$c=m^e\ mod\ N$，而解密过程为$m=c^d\ mod\ N$，这里考虑$m^z\equiv 1(mod\ N)$，从而$(N,e),(N,d)$（这里为有序对的含义）为公私钥对。

RSA的安全性就在很难从公钥推导出私钥，因为计算大整数的质因子分解很困难

Diffie-Hellman密钥交换

从上面的介绍可以看出，RSA加密算法需要用到指数运算，这远远慢于对称加密算法，这给交流带来不便，所以常有的做法是使用非对称加密算法约定一个对称密钥来使用，RSA当然也可以使用，但是还有一个比较有趣的算法，即DH-密钥交换算法，它的安全性基于计算离散对数的难度

首先全局已知的信息是一个质数q以及它的一个原根α，Alice和Bob要交换密钥的时候，Alice产生一个随机数$X_A<q$，并计算$Y_A=\alpha^{X_A}\ mod\ q$，然后将Y_A发送给Bob，而Bob收到后产生随机数$X_B<q$，并计算$Y_B=\alpha^{X_B}\ mod\ q$发送给Alice，然后对于Alice，对称密钥$K=(Y_B)^{X_A}\ mod\ q$，而对Bob为$K=(Y_A)^{X_B}\ mod\ q$，所以外界只知道Y_A,Y_B而不知道Alice和Bob产生的随机数是什么，于是$K=\alpha^{X_AX_B}\ mod\ q$成为Alice与Bob的对称密钥。

当然DH-密钥交换只是一个简单的模型，由于计算量比较大，它很难防止阻塞性攻击，即申请大量密钥使得主机无法做其它正常工作，同时也无法验证双方身份信息，无法防止所谓重放攻击等等。