CINTA作业三、证明题、编程

```
markdown 本地图片：![avatar](本地路径)
```

CINTA作业三，证明题，编程

1，证明：让\ mathbb {G} 为一组，对于 $mathbbG$中的任意两个元素a，b\。然后，等式 ax = b 和 xa = b 在 \ mathbb {G} $中具有唯一解。

2，证明：让 $mathbbG$为一组，让a，b，c in $mathbbG$为一组。那么$ba = ca$意味着$b = c$，而$ab = ac$意味着$b = c$。

3，编写一个Python程序来计算Eurler的phi函数。也就是说，给定整数n，则返回Phi（n）。

4，证明：令$m = p_1^{a_1} p_2^{a_2}\ cdots p_k^{a_k}$，则 $phi\,(\,m\,) = m\,(\,1 - 1/p_1\,)\,(\,1 - 1/p_2\,)\ cdots\,(\,1 - 1 - p_k\,)$。

1.prove：ax=b和xa=b各有有唯一解，且该解也在G内部

设a,b∈G，G是群

(1)existence.

设ax=b， 两边同时左乘a的逆元a'，有 a'ax=a'b ，由于a'a =e ,故有

$$a'ax = ex = x = a'b$$

成立，解得x=a'b，因为a'和b均为G中元素，所以a'b∈G

xa=b同理，可得 x=ba'，都存在x的解使得等式成立

(2)uniqueness

利用反证法，假设存在x1 ≠ x2，有ax1=b 并且 ax2=b成立，那么

利用左乘a'的方法，有

$$a'ax1 = ex1 = x = a'b = x2 = ex2 = a'ax2$$

即有x1=x2的结果，这与我们的假设冲突，因此，x1=x2，ax=b有唯一解x=a'b

xa=b同理，有唯一解x=ba'

2.prove:

设a,b,c∈G，G为群，有ba=ca 和 ab =ac成立，欲证明ba=ca能推导出 b=c（或ab=ac能推导出ab=ac)

（1）当a为单位元时，很显然，ba=b 且 ca=c， 有 ba=ca -》 b=c成立， 同理 ab=ac 也能推导出b=c成立

（2）当a不为单位元时，显然a存在唯一逆元a'，使得 aa'=e

因此，对ba = ca 式子的两边同时右乘 a'，有 baa' = caa'

因为aa' =e 故有

$$baa' = be = b = caa' = ce = c$$

，使得 b = c成立 ，同理ab=ac左乘a'也能得到b=c成立

4.prove:

设

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

我们知道，m是由k个素数p1⋯pk的含幂乘积组成的，它们之间都是互素的，有

$$\Phi(m) = \Phi(p_1^{a_1}) \cdot \Phi(p_2^{a_2}) \cdots \Phi(p_k^{a_k})$$

我们知道 p是素数，p^k中不是素数的只能是p的倍数，如p,2p...(p^(k-1)-1)*p，这些合数总共有p^(k-1)-1个

所以在[1,p^k)的范围内，只有

$$p^k - 1 - (p^(k-1) - 1) = p^k - p^{k-1}$$

个素数因子，由欧拉函数可知

$$\Phi(p^k) = p^k \cdot (1 - 1/p)$$

用上式的形式整理Φ(m)，可得

$$\begin{aligned} \Phi(m) &= p_1^{a_1} \cdot (1 - 1/p_1) \cdot p_2^{a_2} \cdot (1 - 1/p_2) \cdots p_k^{a_k} \cdot (1 - 1/p_k) \\ &= p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} \cdot (1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k) \\ &= m \cdot (1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k) \end{aligned}$$

得证

$$\Phi(m) = m(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k)$$