作业1 证明 division algorithm 和 bezout theorem

1 证明 division algorithm

```
给定两个整数a和b, b>0, 存在唯一的整数 商q和 余数r,  有a=bq+r ,其中0≤r<b
```

(1)存在性证明

构造集合S

$$S = a - bk : k \in Z\text{并且} a - bk \geq 0$$

因为a-bk>=0，故集合S必定存在一个最小的数使得S不为空。

由良序定理知，存在一个最小的整数r=a-bq ∈ S，有a-bk≥0，故r ≥0成立

假定r>b，有

$$r - b = a - bq - b = a - (q + 1)b$$

我们由良序定理可知，r是S中最小的整数，而a-(q+1)b <a-qb ， 且q+1 ∈Z ，如果r-b>0那，r将不再是最小的整数，与我们的假设冲突，故 r<b

所以存在整数a和b(b>0)，有a=bq+r成立，其中0≤r<b

(2)唯一性证明

有

$$a = bq + r$$

假设存在另一组 r' 和 q' 使得

$$a = bq' + r'$$

成立，其中 0≤ r' <b

假设 r' ≥ r ， 则 有

$$r' - r = b(q' - q)$$

由上式可知，q'-q ∈ Z ，(r' - r) | b ， 且

$$0 \leq (r' - r) < r' < b$$

这与我们的存在最小整数r使得S集合非空的假设冲突

所以只有当r' = r 的时候，a = bq + r成立， 因此r'= r ,q' =q ， r和q是唯一的。

2 证明 bezout theorem

```
bezout theorem: a和b为非0整数，存在整数r和s使得gcd(a,b)=ar+bs成立
```

证明:

(1)存在性证明:

先构造集合 S={ ax + by : x,y∈ Z 并且 ax+by >0}

$$S = ax + by : x, y \in Z\text{并且}ax + by > 0$$

由良序原理可知，集合S必定有一个最小的数使得该集合不为空

我们构造这个最小的数为d,并且

$$d = ar + bs$$

我们假定

$$d = gcd(a, b)$$

由division algorithm可知,

$$a = dq + r1,\text{其中}0 \le r1 < d$$

如果 r1>0 ，有

$$r1 = a - dq = a - (ar + ds)q = a(1 - rq) + b\text{（}-sq\text{）}$$

使得 r1也存在于集合S中，且会比d更小,但这与我们的假定d是S中最小的数的结论冲突

因此，r1=0 并且d 应该要整除a，同理d也整除a， 故d是a和b的公因子

(2)唯一性证明

假定d' 是除d外的整数a和b的另一个公因子，假设 d' | d ,设为 a=d'k b=d'c

有

$$d = ar + bs = d'(rk + sc)$$

则必有d'整除d， 因此d必须是a和b唯一的最大公约数