同余

2019年4月17日 12:24

整除

1. 定义
2. 三大基本性质： 加性 a|b a|c -> a|b+c
   乘性 a|b -> a|bc
   传递性 a|b b|c -> a|c
3. 整除的线性性
   利用加性和 乘性证明

同余

1. 定义
2. 辨析 a 同余 b （mod m）和 a mod m=b 的区别
3. 同余的运算律：
   a. 合并加/两边直接加 a同余b c同余d a+b同余 c+d
   b. 合并乘 a同余b c同余d ab同余cd
   c. 不能合并除 （gcd=1除外）
   d. (a+b)modm=(amodm+bmodm)mod m
      (ab)mod m=(amodm * bmodm)mod m

   证明：定义证明
4. 模运算：加法和乘法的
   a. 交换律
   b. 结合律
   c. 双向分配率
   d. 加法逆元和单位元
5. 进制转化
6. 基本运算复杂度

   1.加法 O（n） bits addtions
   2.乘法 O(n2)
   其中O(n2) shift
   O(n2) bits additions
   3.除法 O(n2)
   O(n2) bit operations,
   n = max(loga,logd)
   4.幂取模 O((logm)2 logn)

```
procedure modular exponentiation(b: integer, n = (a_{k-1}a_{k-2}...a_1a_0)_2 , m: positive
    integers)
 x := 1
power := b mod m
for  i := 0 to k − 1
      if a_i = 1 then x := (x·power) mod m
      power := (power·power) mod m
return x {x equals b^n mod m }
```

7.素数

Approach 1: test if each number $x < n$ divides n.

Approach 2: test if each prime number $x < n$ divides n.

Approach 3: test if each prime number $x < \sqrt{n}$ divides n.