第十章高斯整数与唯一因子分解

张志强
智能信息处理研究中心
http://rciip.hrbeu.edu.cn

高斯整数

- 之前我们研究了整数集合的一些性质，有趣的是，在其他一些数集中也存在类似于整数的一些性质，如整除、素数和因数分解等
- 所谓高斯整数就是指，形如a+bi的数，其中a,b是有理整数，i是-1的平方根，即$i^2=-1$
  - 高斯整数的整除
  - 高斯素数
  - 高斯整数的素数分解

复数回顾

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$

$$(a+bi)-(c+di)=(a-c)+(b-d)i$$

$$(a+bi)\times(c+di)=ac+adi+bci+bdi^2=(ac-bd)+(ad+bc)i$$

$$\frac{a+bi}{c+di}=\frac{a+bi}{c+di}\times\frac{c-di}{c-di}=\frac{ac+bd}{c^2+d^2}+\frac{(-ad+bc)i}{c^2+d^2}$$

- 复数的加法和乘法是可以交换的

复数回顾

- 度量复数的大小
  - 若z=x+iy是复数，则z的绝对值|z|等于

$$|z|=\sqrt{x^2+y^2}$$

  - 而z的范数N(z)等于

$$|z|^2=x^2+y^2$$

复数回顾

- 共轭
  - 复数$z=a+bi$的共轭复数是$z=a-bi$，记做$\overline{z}$
  - 若w和z是两个复数，则wz的共轭是w和z的共轭的乘积，即 $(\overline{wz})=(\overline{w})(\overline{z})$
  - 若$z=x+yi$是复数，则

$$z*\overline{z}=(x+yi)(x-yi)=x^2+y^2=N(z)$$

复数回顾

- 范数的性质
  - (i)对任意复数z，$N(z)$是非负数
  - (ii)对任意复数z和w，$N(zw)=N(z)*N(w)$
  - (iii)$N(z)=0$当且仅当$z=0$
- 证明
  - (i)显然
  - (ii)z和w是复数有，

$$N(zw)=(zw)(\overline{zw})=(z\overline{z})(w\overline{w})=N(z)N(w)$$

  - (iii)显然

高斯整数

0011

- 高斯整数加减乘封闭性
  - 设α =x+iy和β =w+iz是高斯整数，其中x,y,w,z是有理整数，则α + β、 α - β、 α β都是高斯整数
- 高斯整数的整除性
  - 设α和β都是高斯整数，我们称α整除β，是指存在一个高斯整数γ使得β = α γ。若α整除β，记做α | β，否则记做α∤β

12
45

高斯整数

0011

- 例1，由于(2-i)(5+3i)=13+i，故2-i|13+i
- 例2，请问3+2i是否高斯整除6+5i

$$\frac{6+5i}{3+2i}=\frac{(6+5i)(3-2i)}{(3+2i)(3-2i)}=\frac{28+3i}{13}=\frac{28}{13}+\frac{3i}{13}$$

- 例3，请证明-i整除任意高斯整数a+bi

  因为对于任意的高斯整数a+bi，均有

  a+bi=-i(-b+ai)

12
45

高斯整除

- 若α,β,γ是高斯整数，$\alpha|\beta$，$\beta|\gamma$，则有$\alpha|\gamma$；再者若α,β,γ,μ和υ是高斯整数，$\gamma|\alpha$，$\gamma|\beta$,则$\gamma|(\mu\alpha+\beta\upsilon)$
- 证明：作业
- 定义：若$\varepsilon|1$，则称高斯整数ε是<u>单位</u>。若ε是单位，则称$\varepsilon\alpha$为高斯整数α的一个<u>相伴</u>

高斯整除

- 高斯整数的单位为1,-1,i,-i
- 例如，高斯整数-2+3i的相伴有哪些？
  - 1(-2+3i)=-2+3i
  - -(-2+3i)=2-3i
  - i(-2+3i)=-3-2i
  - -i(-2+3i)=3+2i
- 对于一个任意的高斯整数β来说，它的全部相伴是四个高斯整数β,-β,iβ,和-iβ

高斯素数

- 定义：若非零高斯整数π不是单位，而且只能够被单位和它的相伴整除，则称之为<u>高斯素数</u>
  - 由定义可知一个高斯素数π是素数当且仅当它有8个因子，即4个单位和它的4个相伴
- 定理：若π是高斯整数，而且N(π)=p，其中p是有理素数，则π和$\bar{\pi}$是高斯素数，而p不是高斯素数

高斯素数

- 例1，请证明2-i是高斯素数
  - 证明：因为$N(2-i)=2^2+1^2=5$，而5是有理素数，再由5=(2+i)(2-i)可知5不是高斯素数
- 例2，证明3是高斯素数
  - 证明：由于N(3)=N(3+0i)=9不是有理素数，因为不能从定理得到证明。假设3=(a+bi)(c+di)，其中a+bi和c+di不是单位，两边取范数有N(3)=N(a+bi)N(c+di)=9，由于a+bi和c+di不是单位，因此有N(a+bi)≠1，N(c+di) ≠1，所以N(a+bi)=N(c+di)=3，也就是$a^2+b^2=3$，这是不可能的，因为3不存在两个有理数的平方和，因此3是高斯素数
- 例3，证明2不是高斯素数
  - 证明：因为2=(1+i)(1-i)，而2是有理素数，因此有1+i和1-i都是高斯素数

高斯整数的唯一分解

- 定理：每个高斯整数$\alpha \neq 0$都可以唯一的分解为一个单位μ乘以规范的高斯素数的乘积$\alpha = \mu\,\pi_1\pi_2\ldots\pi_r$
- 我们称x+yi是规范的，如果x>0,y≥0

高斯素数整除性质

- 定理(高斯素数整除性质)：设π为高斯素数， α,β为高斯整数，并假设π整除乘积$\alpha\beta$，则π要么整除α，要么整除β(或α,β均被π整除)
  - 同样也可以将其推广到n个高斯整数乘积的情形