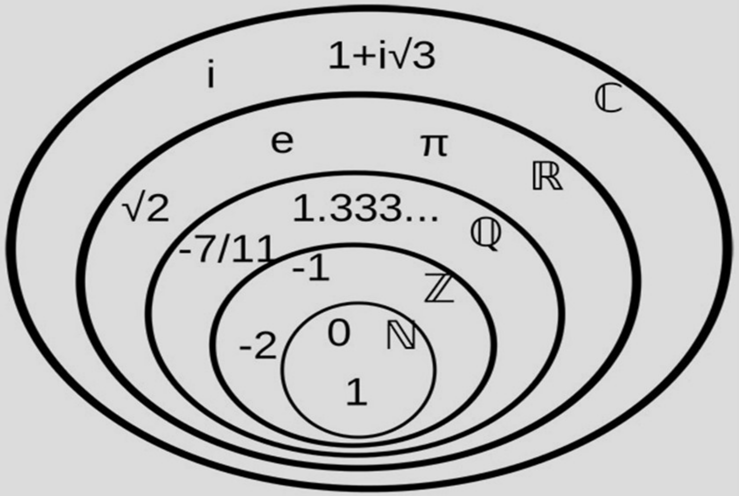

第1.3节 素数和最大公约数

Section 1.3: Primes and Greatest Common Divisors

知识要点

1. 素数及其性质
2. 素数的猜想和开放问题
3. 最大公约数和最小公倍数
4. 欧几里得算法
5. gcd的线性组合的表示

1.3.1 素数

- 【定义】：大于1的整数p称为**素数**(也叫质数)，如果p的正因子只有1和p. 大于1但又不是素数的正整数集合叫做**合数**.
- 例如{2,3,5,7,11,13,17,19,23,...}是素数集合. 1既不是素数, 也不是合数. 再例如9是合数, 因为3整除9.

【基础知识：假如整数p除以m等于一个没有余数的整数(也就是$m|p$), 那么我们称m是p的**整数因子**. 比如42=6*7, 因此7是42的因子. 正整数因子简称**正因子**或称**正因数**】

1.3.1 素数

- 【素数性质】
  - 1、设p是素数, 且$d|p$, 若$d > 1$, 则$d = p$
  - 2、设p是素数, 且$p|ab$, 则必有$p|a$或者$p|b$
  - 3、整数p是合数当且仅当存在整数a, 使得$a|p$并且$1 < a < p$
  - 4、合数必有素数因子, 即设a是合数, 则存在素数p, 使得$p|a$
- 证明略.
- 根据性质4, 任何大于1的整数要么是素数, 要么可以分解成素数的乘积. 这就是下述的算术基本定理. 它表明素数是构成整数的基本元素.