# 第三章因数分解与算术基本定理

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

## 什么是素数?

- 定义：所谓素数就是这样的整数p≥2，它的(正)因数仅有1与p
- 不是素数的整数m≥2称作合数

- 素数：2,3,5,7,11,13,17,19,23,29,……
- 合数：4,6,8,9,10,12,14,15,16,18,……

# 引理1

- 引理3.1 令p是素数，假设p整除乘积a*b，则p整除a或p整除b（或者p既整除a也整除b）
- 证明：已知p整除ab，如果p整除a，则证明完成，假设p不整除a。现在考虑gcd(p,a)等于什么。由于这个公因数整除p，而p又是素数，则它是1或p。同时它又整除a，由于假设p不整除a，所以gcd(p,a)=1。

  已知存在整数x,y，使得形如ax+by的最小正整数等于gcd(a,b)，因此有存在一组x和y，使得px+ay=1

  在上述方程两边同乘b，得pbx+aby=b，显然p整除pbx，由于p整除ab，因此p也整除aby。进而p也整除这两项的和px+aby，故p整除b。

- 注：上述引理是素数的特殊性质，对合数并不成立，例如，6整除乘积15*14，但6既不整除15也不整除14.



# 素数整除性质

- 定理3.1：假设素数p整除乘积$a_1a_2a_3...a_r$，则p整除$a_1,a_2,a_3,...,a_r$中至少一个因数
- 证明：略
  - 数学归纳法
  - 直接证

# 偶数的世界

- 假设离开我们熟悉的整数世界，进入到偶数的世界，也称为E-地带

  E={…,-8,-6,-4,-2,0,2,4,6,8,10,…}

  - 在这个世界上，同样可以进行加减乘的运算，因为偶数的和差积还是偶数，也可以谈论整除性，如果存在数k使得n=km，则称数m“E-整除”数n，但这个k一定是E集合中的元素，即为偶数。例如，12=6*2，所以6“E-整除”12，而6不能“E-整除”18，因为找不到这样的k



# 偶数的世界

- 在偶数的世界里面，同样可以谈论“素数”，如果任何偶数不整除p，则称p是E-素数。

  2,6,10,14,18,22,26,30,…

- 那么前面的在正常整数空间中显然成立的断言是否在E-地带上也成立呢？

  p是素数假设p整除乘积a*b，则p整除a或p整除b（或者p既整除a也整除b）

# 偶数的世界

- 考虑E-地带的素数6和数a=10,b=18，因为180=6*30，所以6“E-整除”ab=180，但是6既不“E-整除”10，也不“E-整除”18，所以前面在正常整数空间中成立的断言在这里不成立
- 我们知道在正常的空间中有断言“每个数都可以唯一分解为素数乘积”成立。在E-地带上是否成立？

  180=6*30=10*18=2*90

  – 其中6,10,18,30,90均为E-地带中的E-素数

很多显然的断言或结论其实并不是那么显然的，需要更加细致的考查和研究！



# 算术基本定理

- 定理3.2 每个整数n≥2可唯一分解成素数乘积$n=p_1p_2p_3\ldots p_r$
- 几点说明
  – 如果n是素数，那么n=n是单个素数的乘积
  – 当记做$n=p_1p_2p_3\ldots p_r$时，并不意味着这r个素数都是不同的，如300=2*2*3*5*5
  – 因数的不同排列不是新的因数分解，如12=2*2*3, 12=2*3*2等看做相同的分解

# 算术基本定理

- 证明过程
  - 首先证明数n可以以某种方式分解成素数的乘积
    - 数学归纳法
  - 最后证明只有一种这样的因数分解（因数重排除外）
    - 直接证



# 素数分解

- 给定一个整数n≥2，如何将其表示成素数乘积？
  - 因数分解方法，如

    180=2*90=2*2*45=2*2*3*15=2*2*3*3*5

    n比较小时，这种方法还可以接受
  - 素数整除法，n比较大时因数分解方法不再适用，可以采用素数整除法，即用素数2,3,5,7,11…等去试除n，直到得到一个因数为止，如 n=9 105 293，经过试除得到整除n的最小素数为37， 9 105 293=37*246 089，接着继续检查37,41,43,47,…来求整除246 089的素数，得到246 089=43*5723，继续这个过程用43,47,53,59…试除5723得到，5723=59*97，最后得到

    n=9 105 293=37*43*59*97

# 素数分解

- 分析
  - 前面的方法虽然均可以得到素数分解，存在什么问题？
    - 因数分解只适用于n比较小的时候
    - 素数整除法虽然可以处理n比较大的情况，但是要求至少要知道比n小的所有素数，如果n越来越大的话，此方法总有失灵的时候
  - 那么对一个大于等于2的整数进行素数分解与判断一个大于等于2的整数是否为素数两者之间有什么必然关联吗？



# 素数分解

- 引理3.2 如果n本身不是素数，则必有整除n的素数 $p \le \sqrt{n}$
- 证明：假设p是整除n的最小素数，则有n=mp，m≥p，从而有n=mp≥$p^2$，两边取平方根得 $p \le \sqrt{n}$

# 素数分解

- 素数乘积分解新方法
  - 用小于等于 $\sqrt{n}$ 的每个数（或正好每个素数）2,3,...试除n，如果没有求得整除n的整数，那么n本身一定就是素数。否则求得的第一个因数是素数p。分解得到n=pm后，再继续对m重复上述过程。
- 请问这个方法的效率如何？是否很容易在计算机上实现？
  - 例如$n=10^{128}+1$，如果其是素数的话，就需要检查到$10^{64}$个可能的因数才能停下来，如果每秒钟能检查10亿个的话，也需要$3*10^{48}$年！



# 素数分解

- 问题1：如何分辨已知数n是素数还是合数？
- 问题2：如果n是合数，如何将其分解成素数乘积？

- 显然第一个问题比第二个要容易回答。我们可以利用前面的方法得到很大的素数p和q，这样给某人n=p*q的乘积值，他就很难获得数p与q这个分解。
- 很容易将两个数相乘，但是很难分解其积，这个事实就是今天利用数论建立高度安全密码的基础。

# 作业

- 编写将正整数n分解成素数乘积的程序（如果输入0，则转到错误处理而非进入死循环），表示n的因数分解的简便方法是2×r阶矩阵，因此如果

$$n=p_1^{k1}p_2^{k2}p_3^{k3},\ldots,p_r^{kr}$$

- 则n的因数分解可存储成矩阵

$$\begin{bmatrix} p_1 & p_2 & \cdots & p_r \\ k1 & k2 & \cdots & kr \end{bmatrix}$$

- 用你的程序求1 000 000与1 000 030之间的所有整数的完全因数分解