信息安全数学基础

陈恭亮　教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

1.5 整数分解

思考题

1. 当n 是平方数时, 如何分解合数n ?
2. 当n 有平方因数时, 如何判断n 是合数?
3. 当n 是合数时, 用平凡除法分解n 的时间是多少?
4. 当n 是合数时, 如何分解n ? 有哪些有效的分解方法?
5. 整数n 一定可以表示为素因数的乘积吗? 该乘积表达式惟一吗? 保证整数分解惟一性的主要定理是什么?
6. 设a, b 是正整数. 如何构造整数u, v 使得$u \mid a$, $v \mid b$, $(u, v) = 1$, $u \cdot v = [a, b]$?

1.5 整数分解

本节讨论整数一种分解方法.

定理1.5.1 (整数分解定理) 给定正合数$n>1$. 如果存在整数$a,\ b$使得

$$n \mid a^2-b^2, \quad n \nmid a-b, \quad n \nmid a+b. \tag{1}$$

则$(n,a-b)$和$(n,a+b)$都是n的真因数.

证 若$(n,a-b)$不是n的真因数, $(n,a-b)$为1或n.

对于$(n,a-b)=1$, 由$n\mid a^2-b^2=(a-b)(a+b)$, 推出$n\mid a+b$, 与假设矛盾.

对于$(n,a-b)=n$, 推出$n\mid a-b$, 与假设矛盾.

故$(n,a-b)$是n的真因数.

同理, $(n,a+b)$也是n的真因数. 证毕

例1.5.1 对于$n = 167 \cdot 227 = 37909$, 有$a = 16355$, $b = 11$ 使得

$$n \mid a^2 - b^2, \quad n \nmid a - b, \quad n \nmid a + b$$

以及$(n, a-b)$ 和$(n, a+b)$.

证 我们有$a^2 - b^2 = 267485904 = 7056 \cdot 37909$ 以及

$$a - b = 16344 = 0 \cdot 37909 + 16344, \quad a + b = 16366 = 0 \cdot 37909 + 16366$$

和

$$(n, a-b) = 227, \quad (n, a+b) = 167$$

这里计算最大公因数的算式如下:

$$\begin{array}{rcrcr} 37909 &=& 2 \cdot 16344 &+& 5221 \\ 16344 &=& 3 \cdot 5221 &+& 681 \\ 5221 &=& 7 \cdot 681 &+& 454 \\ 681 &=& 1 \cdot 454 &+& 227 \\ 454 &=& 2 \cdot 227 &+& 0 \end{array} \qquad \begin{array}{rcrcr} 37909 &=& 2 \cdot 16366 &+& 5177 \\ 16366 &=& 3 \cdot 5177 &+& 835 \\ 5177 &=& 6 \cdot 835 &+& 167 \\ 835 &=& 5 \cdot 167 &+& 0 \end{array}$$

例1.5.2 对于$n = 167 \cdot 227 = 37909$, 有$a = 5344184$, $b = 150$ 使得

$$n \mid a^2 - b^2, \quad n \nmid a - b, \quad n \nmid a + b$$

以及$(n, a-b)$ 和$(n, a+b)$.

证 我们有$a^2 - b^2 = 28560302603356 = 753391084 \cdot 37909$ 以及

$$a-b = 5344034 = 140 \cdot 37909 + 36774, \quad a+b = 5344334 = 140 \cdot 37909 + 37074$$

和

$$(n, a-b) = 227, \quad (n, a+b) = 167$$

这里计算最大公因数的算式如下:

$$\begin{array}{rcrcr}
5344034 & = & 140 \cdot 37909 & + & 36774 \\
37909 & = & 1 \cdot 36774 & + & 1135 \\
36774 & = & 32 \cdot 1135 & + & 454 \\
1135 & = & 2 \cdot 454 & + & 227 \\
454 & = & 2 \cdot 227 & + & 0
\end{array}
\qquad
\begin{array}{rcrcr}
5344334 & = & 140 \cdot 37909 & + & 37074 \\
37909 & = & 1 \cdot 37074 & + & 835 \\
37074 & = & 44 \cdot 835 & + & 334 \\
835 & = & 2 \cdot 334 & + & 167 \\
334 & = & 2 \cdot 167 & + & 0
\end{array}$$

1.6 素数 算术基本定理

1.6.1 算术基本定理

前面讨论过素数, 并证明了每个整数都有一个素因数. 下面要证明每个整数一定可以表示成素数的乘积, 而且该表达式是惟一的(在不考虑乘积顺序的情况下).

定理1.6.1 (算术基本定理) 任一整数$n > 1$ 都可以表示成素数的乘积, 且在不考虑乘积顺序的情况下, 该表达式是惟一的. 即

$$n = p_1 \cdots p_s, \qquad p_1 \le \ldots \le p_s, \tag{2}$$

其中p_i是素数, 并且若

$$n = q_1 \cdots q_t, \qquad q_1 \le \ldots \le q_t,$$

其中q_j 是素数,则$s = t,\ p_i = q_i,\ 1 \le i \le s.$

证 首先用数学归纳法证明: 任一整数$n > 1$ 都可以表示成素数的乘积, 即(2) 式成立.

$n = 2$, (2) 式显然成立.

假设对于$< n$ 的正整数, (2)式成立.

对于正整数n, 若n 是素数, 则(2) 式对n 成立.

若n是合数, 则存在正整数n_1, n_2 使得

$$n = n_1 \cdot n_2, \qquad 1 < n_1 < n,\ 1 < n_2 < n.$$

根据归纳假设, 有

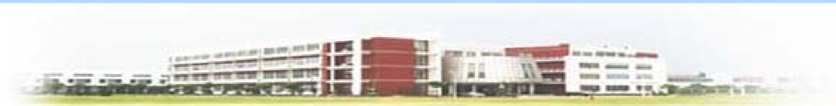
$$n_1 = p_1' \cdots p_u', \quad n_2 = p_{u+1}' \cdots p_s'.$$

于是,

$$n = p_1' \cdots p_u' \cdot p_{u+1}' \cdots p_s'.$$

适当改变p_i'的次序即得(2) 式, 故(2)式对于n 成立.

根据数学归纳法原理, (2) 式对于所有$n > 1$ 的整数成立.



再证明表达式是惟一的. 假设还有

$$n = q_1 \cdots q_t, \qquad q_1 \leq \ldots \leq q_t,$$

其中q_j 是素数, 则

$$p_1 \cdots p_s = q_1 \cdots q_t. \tag{3}$$

因此$p_1 \mid q_1 \cdots q_t$. 根据定理1.4.3, 存在q_j使得$p_1 \mid q_j$. 但p_1, q_j 都是素数, 故$p_1 = q_j$.   同理, 存在p_k 使得$q_1 = p_k$. 这样,

$$p_1 \leq p_k = q_1 \leq q_j = p_1,$$

进而$p_1 = q_1$. 将(3) 式的两端同时消除p_1, 我们有

$$p_2 \cdots p_s = q_2 \cdots q_t.$$

同理可推出$p_2 = q_2$. 依此类推, 可得到

$$p_3 = q_3, \ \ldots, \ q_s = p_t.$$

以及$s = t$. 证毕

例1.6.1 写出整数$45,\ 49,\ 100,\ 128$ 的因数分解式.

解 根据定理1.6.1, 我们有

$$\begin{aligned} 45 &= 3\cdot 3\cdot 5, & 49 &= 7\cdot 7,\\ 100 &= 2\cdot 2\cdot 5\cdot 5, & 128 &= 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2. \end{aligned}$$

为了更好地表达整数的因数分解式, 我们将相同的素数乘积写成素数幂的形式

$$\underbrace{p\cdot\cdots\cdot p}_{\alpha}=p^{\alpha},$$

定理1.6.1 可表述为:

定理1.6.2 任一整数$n>1$ 可以惟一地表示成

$$n=p_1^{\alpha_1}\cdots p_s^{\alpha_s},\quad \alpha_i>0,\ i=1,\ldots,s, \tag{4}$$

其中$p_i<p_j\ \ (i<j)$是素数.

(4)式叫做n **的标准分解式**.

例1.6.2 写出整数45, 49, 100, 128, 1024, 4096 的标准分解式.

解 根据定理1.6.1 和例1.6.1, 我们有

$$\begin{aligned}45&=3^2\cdot5, & 49&=7^2, & 100&=2^2\cdot5^2,\\ 128&=2^7, & 1024&=2^{10}, & 4096&=2^{12}.\end{aligned}$$

1.6.2 算术基本定理的应用

本节将利用算术基本定理来对整数的性质作进一步的探讨.
在应用中, 为了表述方便起见, 整数的因数分解式常写成

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad \alpha_i \geq 0,\ i = 1, \dots, s. \tag{5}$$

首先讨论因数的性质.

定理1.6.3 设n 是大于1 的一个整数, 且有标准分解式:

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad \alpha_i > 0,\ i = 1, \dots, s,$$

则d 是n 的正因数当且仅当d 有因数分解式:

$$d = p_1^{\beta_1} \cdots p_s^{\beta_s}, \quad \alpha_i \geq \beta_i \geq 0,\ i = 1, \dots, s. \tag{6}$$

证 设$d \mid n$, 且d 有因数分解式: $d = p_1^{\beta_1} \cdots p_s^{\beta_s}, \quad \beta_i \geq 0,\ i = 1, \ldots, s.$
则我们一定有 $\alpha_i \geq \beta_i, \qquad i = 1, \ldots, s.$
否则, 存在$1 \leq i \leq s$, 使得$\alpha_i < \beta_i$. 不妨设$\alpha_1 < \beta_1$. 根据$d \mid n$ 及$p_1^{\beta_1} \mid d$, 有

$$p_1^{\beta_1} \mid p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}.$$

两端消除$p_1^{\alpha_1}$, 得到

$$p_1^{\beta_1 - \alpha_1} \mid p_2^{\alpha_2} \cdots p_s^{\alpha_s}.$$

再根据定理1.3.12 之推论, 存在$j,\ 2 \leq j \leq k$ 使得

$$p_1 \mid p_j.$$

这不可能. 故(6) 式成立.
反过来, 若(6) 式成立, 则 $n' = p_1^{\alpha_1 - \beta_1} \cdots p_s^{\alpha_s - \beta_s}$
是一个整数, 且使得

$$n = n' \cdot d.$$

这说明, $d \mid n$. 证毕

访问主页
标题页
目录页
第 12 页 共 31 页
返回
全屏显示
关闭
退出

例1.6.3 设正整数n 有因数分解式

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad \alpha_i > 0,\ i = 1, \ldots, s.$$

则n 的因数个数

$$d(n) = (1 + \alpha_1) \cdot \cdots \cdot (1 + \alpha_s).$$

证 设d 是整数n 的正因数. 根据定理1.6.3, 我们有

$$d = p_1^{\beta_1} \cdots p_s^{\beta_s}, \quad \alpha_i \geq \beta_i \geq 0,\ i = 1, \ldots, s.$$

因为β_1 的变化范围是0 到α_1 共$1 + \alpha_1$ 个值, $\ldots$, β_s 的变化范围是0 到α_s 共$1 + \alpha_s$ 个值, 所以n 的因数个数为

$$d(n) = (1 + \alpha_1) \cdot \cdots \cdot (1 + \alpha_s).$$

证毕

其次, 讨论最大公因数和最小公倍数的性质.

定理1.6.4 设a, b 是两个正整数, 且都有素因数分解式:

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad \alpha_i \geq 0,\ i = 1, \dots, s,$$

$$b = p_1^{\beta_1} \cdots p_s^{\beta_s}, \quad \beta_i \geq 0,\ i = 1, \dots, s.$$

则a 和b 的最大公因数和最小公倍数分别有因数分解式:

$$(a, b) = p_1^{\gamma_1} \cdots p_s^{\gamma_s}, \qquad \gamma_i = \min(\alpha_i, \beta_i),\ \ i = 1, \dots, s,$$

$$[a, b] = p_1^{\delta_1} \cdots p_s^{\delta_s}, \qquad \delta_i = \max(\alpha_i, \beta_i),\ \ i = 1, \dots, s.$$

证 根据定理1.6.3, 我们知道整数 $d = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$,
满足§1.3 最大公因数的数学定义, 所以 $(a, b) = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$.
同样, 整数 $D = p_1^{\delta_1} \cdots p_s^{\delta_s}$,
满足§1.4 最小公倍数的数学定义, 所以

$$[a, b] = p_1^{\delta_1} \cdots p_s^{\delta_s}.$$

证毕

推论 设a, b 是两个正整数, 则

$$(a,b)[a,b] = a \cdot b.$$

证 对任意整数α, β, 我们有

$$\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta.$$

根据定理1.6.3, 推论是成立的. 证毕

更进一步, 利用整数的因数分解式(5), 我们可以表述多个整数的最大公因数和最小公倍数.

定理1.6.5 设$a_1,\ \ldots,\ a_k$ 是k 个正整数, 且都有素因数分解式:

$$a_j = p_1^{\alpha_{1j}} \cdots p_s^{\alpha_{sj}}, \quad \alpha_{ij} \geq 0,\ 1 \leq i \leq s,\ 1 \leq j \leq k.$$

则$a_1,\ \ldots,\ a_k$ 的最大公因数和最小公倍数分别有因数分解式:

$$(a_1,\ \ldots,\ a_k) = p_1^{\gamma_1} \cdots p_s^{\gamma_s}, \qquad \gamma_i = \min(\alpha_{i1}, \ldots, \alpha_{ik}),\ \ 1 \leq i \leq s,$$

$$[a_1,\ \ldots,\ a_k] = p_1^{\delta_1} \cdots p_s^{\delta_s}, \qquad \delta_i = \max(\alpha_{i1}, \ldots, \alpha_{ik}),\ \ 1 \leq i \leq s.$$

证 根据定理1.6.3, 我们知道整数 $d = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$,
满足§1.3 最大公因数的数学定义, 所以 $(a_1,\ \ldots,\ a_k) = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$.
同样, 整数 $D = p_1^{\delta_1} \cdots p_s^{\delta_s}$,
满足§1.4 最小公倍数的数学定义, 所以

$$[a_1,\ \ldots,\ a_k] = p_1^{\delta_1} \cdots p_s^{\delta_s}.$$

证毕

利用定理1.6.4, 可直接求出如下四个整数的最大公因数和最小公倍数.

例1.6.4 计算整数120, 150, 210, 35 的最大公因数和最小公倍数.

解 根据定理1.6.1, 我们有

$$\begin{aligned} 120 &= 2^3\cdot 3\cdot 5, & 150 &= 2\cdot 3\cdot 5^2,\\ 210 &= 2\cdot 3\cdot 5\cdot 7, & 35 &= 5\cdot 7. \end{aligned}$$

再根据定理1.6.5, 我们有

$$(120,\ 150,\ 210,\ 35) = 2^{\min(3,1,1,0)}\cdot 3^{\min(1,1,1,0)}\cdot 5^{\min(1,2,1,1)}\cdot 7^{\min(0,0,1,1)} = 5$$

以及

$$[120,\ 150,\ 210,\ 35] = 2^{\max(3,1,1,0)}\cdot 3^{\max(1,1,1,0)}\cdot 5^{\max(1,2,1,1)}\cdot 7^{\max(0,0,1,1)} = 4200.$$

最后, 利用整数的惟一因数分解式, 我们给出如下结果, 该结果将用于原根的构造.

定理1.6.6 设a, b 是两个正整数, 则存在整数$a' \mid a$, $b' \mid b$ 使得

$$a' \cdot b' = [a, b], \quad (a', b') = 1.$$

证 将整数a, b 作如下的因数分解式:

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \qquad b = p_1^{\beta_1} \cdots p_s^{\beta_s},$$

其中$\alpha_i \geq \beta_i \geq 0$, $(i = 1, \ldots, t)$; $\beta_i > \alpha_i \geq 0$, $(i = t + 1, \ldots, s)$.
我们取

$$a' = p_1^{\alpha_1} \cdots p_t^{\alpha_t}, \qquad b' = p_{t+1}^{\beta_{t+1}} \cdots p_s^{\beta_s},$$

则整数a', b' 即为所求. **证毕**

例1.6.5 设$a = 79720245000 = 2^3 \cdot 5^4 \cdot 11^6 \cdot 3^2 \cdot 7^0$, $b = 9318751596 = 2^2 \cdot 5^0 \cdot 11^3 \cdot 3^6 \cdot 7^4$.

我们取

$$a' = 2^3 \cdot 5^4 \cdot 11^6, \quad b' = 3^6 \cdot 7^4, \quad (a', b') = 1,$$

则有

$$a' \cdot b' = 2^3 \cdot 5^4 \cdot 11^6 \cdot 3^6 \cdot 7^4 = [a, b].$$

例1.6.6 设n 是合数, p 是n 的素因数. 设$p^\alpha \| n$ (即$p^\alpha | n$, 但$p^{\alpha+1} \nmid n$), 则$p^\alpha \nmid \binom{n}{p}$, 其中 $\binom{n}{p} = \dfrac{n(n-1)\cdots(n-p+1)}{p!}$.

证 因为$p^\alpha \| n$, 我们设$n = p^\alpha m$, $(m,p)=1$, 则对于$1 \le k \le p-1$, 有$(n-k,p)=1$. 否则, $p | n-(n-k)=k$, 矛盾. 根据§1.4 定理3, 我们有$((n-1)\cdots(n-p+1), p) = 1$. 从而,

$$\binom{n}{p} = \frac{n}{p}\frac{(n-1)\cdots(n-p+1)}{(p-1)!} = p^{\alpha-1}m\frac{(n-1)\cdots(n-p+1)}{(p-1)!}.$$

但

$$(m\frac{(n-1)\cdots(n-p+1)}{(p-1)!},\ p) = 1,$$

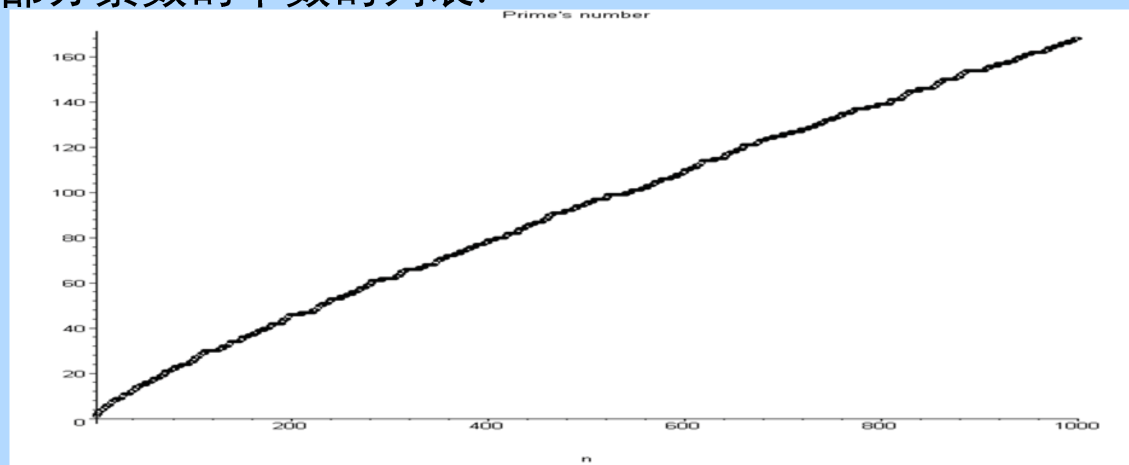
故$p^\alpha \nmid \binom{n}{p}$. 证毕.

1.7 素数定理

设$\pi(x)$ 表示不超过x 的素数个数, 即

$$\pi(x) = \sum_{p \le x} 1$$

是关于素数个数的函数. 根据定理1.1.8, 存在无穷多个素数, 这就是说, $\pi(x)$ 随x 趋于无穷. 如下是$\pi(x)$ 在区间$[2, 1000]$ 上的图形, 以及一部分素数的个数的列表.



x	2	10	50	100	500	1000	10^4	10^5	10^6	10^7	10^8
$\pi(x)$	1	4	15	25	95	168	1229	9592	78498	664579	5761455

访问主页
标题页
目录页
第 21 页 共 31 页
返回
全屏显示
关闭
退出

但人们希望知道$\pi(x)$ 的具体公式. 为了方便读者的学习, 我们将一些结果列在这里. 希望知道详细证明过程的读者可以阅读相关书籍.

定理1.7.1 (契比谢夫不等式) 设$x \geq 2$. 则我们有

$$\frac{\ln 2}{3}\frac{x}{\ln x} < \pi(x) < 6\ln 2\frac{x}{\ln x}$$

和

$$\frac{1}{6\ln 2}n\ln n < p_n < \frac{8}{\ln 2}n\ln n, \quad n \geq 2$$

其中p_n 是第n 个素数.

定理1.7.2 (素数定理)

$$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$