A First Course in Number Theory

HIT

数论经典著作系列

数论初等教程

[俄] A·K·苏什凯维奇 著 叶乃膺 译

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

数论经典著作系列

数论初等教程

A First Course in Number Theory

[俄] A·K·苏什凯维奇 著

叶乃膺 译

HITP

哈爾濱工業大學出版社

HARBIN INSTITUTE OF TECHNOLOGY PRESS

◎目录

第一章　数的可约性

§1　关于可约性的初等定理(一)

在下文中 $a,b,c,\cdots,x,y,\cdots,\alpha,\beta,\cdots$ 这些字母我们将只用来表示整数，它可能是正的或负的，已知的或未知的，常数或变数. 从初等算术知道，整数的和、差、积仍然是整数，但是两个整数的商只有在特殊情形下才是整数. 对于整数我们来证明下面的基本定理.

定理 1　若 a 及 b 是两个任意的整数且 $b\neq 0$，那么总可以找到这样的整数 q 及 r，使

$$a=bq+r \tag{1}$$

其中，$0\leqslant r<|b|$[①]，r 及 q 是唯一确定的.

证　先假设 $a>b>0$. 我们来考察数 b 的倍数，即下面的一些数：$1\cdot b=b$，$2\cdot b,3\cdot b,\cdots$，一般地写作 $k\cdot b$. 根据有名的阿基米德公理，对于足够大的 k 有：$k\cdot b>a$. 因此，总存在这样一个自然数 q，使得恰好有 $bq\leqslant a$ 而且 $b(q+1)>a$. 我们记：$a-bq=r$；显然，$r\geqslant 0$；由此 $a=bq+r$，而 $b(q+1)=bq+b>a$，即 $bq+b>bq+r$；由是 $r<b$. 对于这个情形定理已被证明.

若 $a=b>0$，则 $q=1,r=0$；若 $b>a>0$，则 $q=0,r=a$；若 $a<0,b>0$，则有：$|a|=bq+r$，因此 $a=b(-q)-r$；对于 $r=0$ 公式(1)已成立. 对于 $r>0$ 我们记：$b-r=r_1,0<r_1<b,r=b-r_1$，并得

$$a=b(-q)-b+r_1=b(-q-1)+r_1$$

因为 $0<r_1<b$，所以这是与公式(1)相同的式子.

最后，对于 $b<0$ 根据已经证明的我们有

---

① 通常我们用 $|x|$ 表示数 x 的绝对值，也就是当 $x>0$ 时，$|x|=x$；当 $x<0$ 时，$|x|=-x$；而 $|0|=0$.

$$a=|b|q+r \quad 0\leqslant r<|b|$$

因此

$$a=b(-q)+r$$

即是仍然得到公式(1).

现在证明 q 及 r 是唯一确定的.

假定我们由两个方法得到

$$a=bq+r=bq_1+r_1$$

其中,$0\leqslant r<|b|$,$0\leqslant r_1<|b|$,于是

$$bq-bq_1=r_1-r$$

$$b(q-q_1)=r_1-r$$

在这里等式右边绝对值小于 $|b|$,但是左边能被 b 除尽. 因此,$r_1-r=0$,$r_1=r$,$q_1=q$,于是定理 1 已经完全被证明了.

注意 对于所给(正)的 a 和 b,数 q 及 r 的求法乃是自然数的通常的"带余数除法",它在初等算术中已讲过了. 在这里我们严格地证明了:对于任意整数 a 及 b,数 q 及 r 是存在的;q 是以 b 除 a 所得的不完全商数,r 是所得的余数.

以 b 除等式(1)的两边,我们得到

$$\frac{a}{b}=q+\frac{r}{b} \tag{2}$$

在这里左边(当 $|a|\geqslant b>0$ 时)是假分数,但是 $\frac{r}{b}$ 总是真分数;公式(2)表示从假分数中分出整数部分;q 是分数 $\frac{a}{b}$ 的整数部分;记为

$$q=\left[\frac{a}{b}\right]=E\left(\frac{a}{b}\right)$$

注意 在一般情形,若 x 是任意实数(有理数或无理数,正数或负数),则称适合 $[x]\leqslant x<[x]+1$ 的整数 $[x]$ 或 $E(x)$ 为其整数部分,当 x 是整数时 $[x]=x$.

相仿地就引用记号:$\{x\}=x-[x]$;$\{x\}$ 是数 x 的分数部分;$\{x\}$ 总是非负的. 最后,用 (x) 表示数 x 到与 x 的最近的整数的距离,即是 x 和与 x 最近的整数之差的绝对值,也就是二数 $\{x\}$ 及 $1-\{x\}$ 中的最小的.

当 $r=0$ 时的情形是值得注意的,这时公式(1)变成 $a=bq$,或 $\frac{a}{b}=q$. 在这个情形就说:a 被 b 除尽(即除尽无余),b 是数 a 的约数或因数;a 是数 b 的倍数.

§2　关于可约性的初等定理(二)

定理 2　若 a 被 b 除尽，而 b 被 c 除尽，则 a 也被 c 除尽.

证　这可由乘法的结合律导出：由 $a=bq, b=cq_1$，因此

$$a=(cq_1)q=c(qq_1)$$

定理 2 表示所谓可约性的“传递律”.

定理 3　若 $a_1, a_2, \cdots, a_k$ 都被 c 除尽，而 $x_1, x_2, \cdots, x_k$ 是任意的(整)数，则 $a_1x_1+a_2x_2+\cdots+a_kx_k$ 也被 c 除尽.

证　这可由分配律导出

$$a_1=cb_1, a_2=cb_2, \cdots, a_k=cb_k$$

由此　$$a_1x_1+a_2x_2+\cdots+a_kx_k=c(b_1x_1+b_2x_2+\cdots+b_kx_k)$$

定理 4　若 a 被 b 除尽，则一般 $\pm a$ 被 $\pm b$ 除尽，特别 $|a|$ 被 $|b|$ 除尽.

证　$a=bq=(-b)(-q), -a=b(-q)=(-b)q$.

定理 5　每一个数自己被自己除尽.

证　$a=a\cdot 1$.

定理 6　± 1 是任何数的约数，除了 ± 1 没有别的数有这样的性质.

证　$a=1\cdot a=(-1)(-a)$. 若 a 是任何数的约数，则 1 也被 a 除尽，但是 1 只能被 ± 1 除尽.

定理 7　0 被任何数除尽，除零外没有别的数具有这样的性质.

证　$0=a\cdot 0$；若 $a\neq 0$，则 a 不可能被 $a+1$ 除尽.

定理 4 使其在可约性问题中可以只限于正数. 因此在本章中我们所用的文字不但仅表示整数，而且仅仅表示正整数. 譬如说，谈到数的可约性时，我们所注意的是它的正约数. 一般说来，在可约性问题中，数 a 及 $-a$ 的作用相同；这样的数(相差一个符号或相差一个因数 -1)称为相联数.

§3　最小公倍数

设 $a_1, a_2, \cdots, a_n$ 是所给的(正整)数，它们的乘积 $a_1a_2\cdots a_n$ 能被它们当中每一个所除尽，也就是它们的公倍数. 这样的公倍数有无数多个，因为对于任意的整数 k 来说，$ka_1a_2\cdots a_n$ 也是所给诸数的公倍数；数 0 也是它们的公倍数. 因此，存在一个这些数的最小的正的倍数. 这就是所谓的最小公倍数. 我们用 m 来表示它.

或用记号：$m=M(a_1,a_2,\cdots,a_n)=\{a_1,a_2,\cdots,a_n\}$.

显然，$0<m\leqslant a_1a_2\cdots a_n$.

设 m_1 是同样这些数 $a_1,a_2,\cdots,a_n$ 的任一别的公倍数，则我们以 m 除 m_1 并由定理 1 得到

$$m_1=mq+r\quad 0\leqslant r<m$$

由是 $r=m_1-mq$，按照定理 3 我们导出：r 也是这些数 $a_1,a_2,\cdots,a_n$ 的公倍数. 但是 $r<m$，而 m 是最小公倍数，所以 $r=0$，从而我们得到下面的定理.

定理 8 在若干个所给数的所有公倍数当中，总可找到这样的一个公倍数，它是这些数的任何别的公倍数的约数，这就是最小公倍数.

§4 最大公约数

任意 n 个（正数）数总是有一个等于 1 的公约数. 如果除 1 外（最好是说成除了 ±1 而外）它们没有别的公约数，则这样的诸数称为是互素的. 但是除 1 外，所给诸数还可以有公约数，这一事实是可能发生的（例如，若它们全是偶数，则 2 也是它们的公约数）. 不论在怎样的情形下，所给一些数的公约数的个数总是有限的，因为它们中的每一个（按绝对值）都不可能大于所给诸数中的最小的. 设 $d',d'',d''',\cdots$ 是所给诸数的所有（正）公约数而

$$d=M(d',d'',d''',\cdots)$$

所给诸数 $a_1,a_2,\cdots,a_n$ 中的每一个都是所有约数 $d',d'',d''',\cdots$ 的公倍数，因而（按定理 8）也都能被 d 除尽. 可见 d 也是所给诸数的公约数，也就是 d 包含在诸数 $d',d'',d''',\cdots$ 的集合之中. 同时，d 显然是所有这些约数中的最大者，因为 d 能被它们中的每一个所除尽. 我们用记号

$$d=D(a_1,a_2,\cdots,a_n)=(a_1,a_2,\cdots,a_n)$$

因而有下面的定理.

定理 9 在所给诸数的所有公约数中存在着这样一个公约数：它能被这些数的任何别的公约数所除尽，这就是所给诸数的最大公约数.

定理 10 当而且仅当商数 $\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d}$ 互素时，数 d 才是诸数 $a_1,a_2,\cdots,a_n$ 的最大公约数.

证 (1) 设 $d=D(a_1,a_2,\cdots,a_n)$，并设商数 $\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d}$ 有公约数 $\delta>1$，则商数 $\frac{a_1}{d\delta},\frac{a_2}{d\delta},\cdots,\frac{a_n}{d\delta}$ 都是整数，即是 $a_1,a_2,\cdots,a_n$ 有公约数 $d\delta>d$，但这是与 d 为

最大公约数相矛盾的.

(2) 现在设诸数$\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d}$互素，设$d$不是最大公约数，则按定理9，$D(a_1,a_2,\cdots,a_n)$有形式$d\delta$，其中$\delta>1$. 从而$\frac{a_1}{d\delta}=\frac{a_1}{d}:\delta,\frac{a_2}{d\delta}=\frac{a_2}{d}:\delta,\cdots,\frac{a_n}{d\delta}=\frac{a_n}{d}:\delta$都是整数，即$\delta>1$是诸数$\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d}$的公约数，这是与这些数互素相矛盾的.

定理 11　若$d=D(a_1,a_2,\cdots,a_n)$，则$D(a_1k,a_2k,\cdots,a_nk)=dk$，$D\left(\frac{a_1}{k},\frac{a_2}{k},\cdots,\frac{a_n}{k}\right)=\frac{d}{k}$(只有在$k$是诸数$a_1,a_2,\cdots,a_n$的一个公约数时，后式才成立).

证　这个定理可由$\frac{\alpha_\lambda}{d}=\frac{\alpha_\lambda k}{dk}=\frac{\alpha_\lambda:k}{d:k}$，根据定理10得到.

§5　关于互素的数与可约性的较深定理(一)

我们来研究所给的是两个数a及b的情形. 设$m=M(a,b)$，按定理8，ab能被m除尽. 我们记

$$\frac{ab}{m}=d$$

于是

$$\frac{a}{d}=\frac{m}{b},\frac{b}{d}=\frac{m}{a}$$

右边是整数，从而左边也是整数，因此d是二数a及b的公约数. 设d'是它们的另外任一公约数，则

$$\frac{ab}{d'}=a\cdot\frac{b}{d'}=b\cdot\frac{a}{d'}$$

即$m'=\frac{ab}{d'}$是二数a及b的公倍数. 按定理8，m'应被m除尽

$$\frac{m'}{m}=\frac{ab}{d'},\frac{ab}{d}=\frac{d}{d'}$$

因为这是整数，即d能被d'除尽，所以(参阅定理9)d是二数a及b的最大公约数.

因而有下面的定理.

定理 12 若 $m=M(a,b),d=D(a,b)$，则

$$ab=md \tag{3}$$

当 $d=1$ 时从式(3) 直接导出下面的推论.

推论 当而且仅当二数 a 及 b 的最小公倍数等于它们的乘积时，二数 a 及 b 互素.

注意若所给的数多于两个，则这推论并不真实：互素的几个数其最小公倍数也可能不等于它们的乘积. 例如：$D(6,4,9)=1$，但是 $M(6,4,9)=36<6\times 4\times 9$.

在下文中我们还要回到这个问题上来(参阅定理 17).

§6 关于互素的数与可约性的较深定理(二)

定理 13 为了求几个数的最大公约数，可以先求其中任何二数的最大公约数，然后求这个所得的数与所给数中任何第三数的最大公约数，其次再求第二次所得的数与所给数中任何第四数的最大公约数，以此类推. 这样下去最后所得的公约数也就是全部所给数的最大公约数.

证 只要对于三个所给数 a,b,c 来证明这个定理就够了. 对于许多个所给数，这个定理的证明是相仿的. 因此，设 $D(a,b)=e,D(e,c)=d$；按定理 2，a 及 b 都能被 d 除尽，即 d 是 a,b,c 的公约数. 设 d' 是 a,b,c 的任何别的公约数，则(按定理 9)e 能被 d' 除尽，从而(按同样的定理 9)，d 也能被 d' 除尽，即 d 是 a,b,c 的最大公约数. 公式的形式为

$$D(a,b,c)=D(D(a,b),c)$$

对于最小公倍数也有相仿的定理.

定理 14 为了求几个数的最小公倍数，可以先求其中任何二数的最小公倍数，然后求这个所得的数与所给数中第三数的最小公倍数，以此类推. 最后所得的公倍数也就是全部所给数的最小公倍数.

这个定理也是只要对于三个所给数 a,b,c 来证明就够了. 证明完全和定理 13 的证明相仿(不过不用定理 9 而应该引用定理 8 罢了)，我们把它留给读者去做.

也可以用公式来表示这个定理

$$M(a,b,c)=M(M(a,b),c)$$

这样一来，求几个数的最大公约数(或最小公倍数) 的问题便化成了求仅仅两个数的最大公约数(或最小公倍数) 问题. 至于求两个数的最大公约数的

具体方法我们在下一章中就要讲到.

§7　关于互素的数与可约性的较深定理(三)

定理 15　若 ab 能被 c 除尽,而 a 与 c 互素,则 b 必能被 c 除尽.

证　ab 既能被 a 除尽又能被 c 除尽,因而(按定理 8),也能被它们的最小公倍数除尽,按定理 12 的推论,这个最小公倍数等于它们的乘积:$M(a,c)=ac$;因此,$\frac{ab}{ac}=\frac{b}{c}$ 是一个整数.

定理 16　若 a 与 c 互素,则

$$D(ab,c)=D(b,c)$$

证　设 $D(b,c)=d$,则 ab 也能被 d 除尽. 反之,设 $D(ab,c)=d$,则 $D(a,d)=1$,因为否则(按定理 2)a 与 c 就不可能是互素的. 因此,ab 能被 d 除尽,而 a 与 d 互素;由定理 15,在这情形下 b 也能被 d 除尽. 定理也就被证明了.

注意定理 15 乃是定理 16 当 $d=c$ 时的特殊情形.

如果不仅 $D(a,c)=1$,而且 $D(b,c)=1$,则由定理 16

$$D(ab,c)=1$$

下面的推论成立.

推论 1　若 c 与 a 互素,c 与 b 也互素,则 c 与乘积 ab 也互素.

这个推论可直接扩张到几个因数的情形.

推论 2　若诸数 $a_1,a_2,\cdots,a_m$ 中每一个与诸数 $b_1,b_2,\cdots,b_n$ 中每一个互素,则乘积 $a_1a_2\cdots a_m$ 与 $b_1b_2\cdots b_n$ 也互素.

若 $a_1=a_2=\cdots=a_m$ 且 $b_1=b_2=\cdots=b_n$,则得下面的推论.

推论 3　若 a 与 b 互素,则 a 的任何乘幂也与 b 的任何乘幂互素[①].

§8　关于互素的数与可约性的较深定理(四)

我们现在来研究,在怎样的情形下几个数的最小公倍数等于它们的乘积. 设所给的是三个数 a,b,c. 按定理 14,为了去求 $M(a,b,c)$,我们先求 $M(a,b)$;若 $M(a,b)<ab$,则 $M(a,b,c)<abc$. 因此,应该有 $M(a,b)=ab$,故而(按定理 12

① 当然,这里所指的是所有这些乘幂的方次数都是正整数.

的推论)$D(a,b)=1$.

其次,我们有:$M(a,b,c)=M(ab,c)$;要这式等于abc,就应该有$D(ab,c)=1$,从而显然,$D(a,c)=1$,$D(b,c)=1$.这样一来,三数a,b,c中每两个是互素的,换句话说,三数a,b,c"两两互素".

反之,现在如果已知三数a,b,c两两互素;在这个情形下$M(a,b)=ab$.由定理16的推论1,则ab与c也互素,即

$$M(a,b,c)=M(ab,c)=abc$$

这也可以直接扩张到几个数的情形.

因而有下面的定理.

定理17 当而且仅当几个数两两互素时,它们的最小公倍数才等于它们的乘积.

推论 若数c能被诸数$a_1,a_2,\cdots,a_n$中每一个所除尽,而这几个数两两互素,则c也能被乘积$a_1a_2\cdots a_n$所除尽.

这可由定理17及定理8直接导出.

§9 某些应用

(1) 设x是整数.我们证明:若$\sqrt[m]{x}$不是整数,则这个根数不可能是有理数.假定$\sqrt[m]{x}=\frac{a}{b}$,其中$\frac{a}{b}$是不可约分数,即$D(a,b)=1$.则$x=\frac{a^m}{b^m}$,并且按定理16的推论3,分数$\frac{a^m}{b^m}$也是不可约分数,因而当$b>1$时不可能等于整数x.

一般言之,具有整系数而且最高次项的系数等于一的n次代数方程不可能有有理分数根.

设这样的方程是

$$x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n=0 \tag{4}$$

并且$x=\frac{a}{b}$是它的有理根,同时$D(a,b)=1$.将这个x值代入方程(4)并以b^{n-1}乘两边,我们得到

$$\frac{a^n}{b}+a_1a^{n-1}+a_2ba^{n-2}+\cdots+a_nb^{n-1}=0$$

在这里当$b>1$时第一项是分数(仍按定理16的推论3),但是所有其余各项都是整数;如此相加绝不可能等于零.因此,必然要$b=1$,即$x=a$是整根.

注意　式(4)型的方程之根若非有理数，则称之为代数整数.

(2) 我们讨论二项系数

$$\binom{b}{a}=\frac{b(b-1)(b-2)\cdots(b-a+1)}{1\times 2\times 3\times\cdots\times a}$$

其中 $b\geqslant a$，我们有

$$\binom{b}{b}=1,\binom{b}{1}=b$$

另外有记号

$$\binom{b}{0}=1$$

当 $a>b$ 时

$$\binom{b}{a}=0$$

由直接计算容易导出公式

$$\binom{b}{a}=\binom{b-1}{a}+\binom{b-1}{a-1} \tag{5}$$

由此我们用完全归纳法导出：$\binom{b}{a}$ 总是整数. 其次，有

$$\binom{b}{a}=\frac{b}{a}\binom{b-1}{a-1} \tag{6}$$

设 $b>a$ 且 $D(a,b)=1$. 由公式(6)得知：$b\cdot\binom{b-1}{a-1}$ 能被 a 除尽，从而，按定理 15，$\binom{b-1}{a-1}$ 能被 a 除尽. 故而由公式(6)推知：$\binom{b}{a}$ 能被 b 除尽.

因此，当 a 与 b 互素时 $\binom{b}{a}$ 能被 b 除尽.

§10　素数，素因数分解式

在所有的整数中间，数 ± 1 及 0 与众不同；± 1 只有一个约数 1[①]；0 能被任何整数除尽，即有无数多个约数. 此外任何整数 a 至少有两个约数：1 及 $|a|$；如

① 我们所考虑的只是正的约数.

果它除这两个约数外再没有别的任何(整)约数的话,那么就称它为素数;否则称它为合成数.

若 p 是素数,而 a 是别的任何(整)数,则二数 a 及 p 的最大公约数或为 p 或为 1,这是因为 p 别无约数的缘故.由此得到下面的定理.

定理 18 任何整数或者能被已知素数 p 除尽,或者与 p 互素.

从而由定理 15 导出下面的定理.

定理 19 设有两个或几个数,当而且仅当其中至少一个能被素数 p 除尽时,其乘积才能被 p 除尽.

素数的这个十分重要的性质可以作为素数的新定义.因为逆定理也容易看出是对的:若当而且仅当两个数中至少有一个能被 p 除尽时其乘积才能被 p 除尽,则 p 必为素数.

实际上,设 $p=ab$,但是 p 就是 ab,而 ab 能被 p 除尽,即其中一个因数.例如 a 能被 p 除尽,即有 $a=\pm p, b=\pm 1$,p 不可能有别的分解式,故为素数.

显然,合成数 $a(a\neq 0)$ 有有限个约数.设 q 是数 a 的大于 1 的最小约数,则容易看出 q 是素数,因为数 q 的任何约数 $k>1$ 也将是 a 的约数,但 q 却是数 a 的最小约数.

定理 20 任何整数除 1 外至少有一个素约数.

由是,设 a 能被素数 p 除尽,$a=pa_1$;按定理 20,a_1 也有素约数 q,$a_1=qa_2$,因此:$a=pqa_2$.相仿地,a_2 有素约数 r:$a_2=ra_3$,$a=pqra_3$;以此类推.显然,$a>a_1>a_2>\cdots$.但是小于确定数 a 的正整数只有有限个.意即:某一个 a_k 将等于 1,而 a_{k-1} 是素数.由是,每一个合成数都是有限个素数的乘积:$a=pqr\cdots$.

我们证明数 a 的这种表示法是唯一的.假定我们有两个表示法

$$a=pqr\cdots=p_1q_1r_1\cdots \tag{7}$$

其中,$p,q,r,\cdots,p_1,q_1,r_1,\cdots$ 都是素数.由式(7)看出,$p_1q_1r_1\cdots$ 能被 p 除尽;因此,按定理 19 因数 $p_1,q_1,r_1,\cdots$ 中必有一个能被 p 除尽.设这个因数是 p_1;因为 p_1 是素数,故有 $p_1=p$,即式(7)两边都含 p,约去 p 即得

$$qr\cdots=q_1r_1\cdots$$

相仿地我们知道,q 也必定等于诸数 $q_1,r_1,\cdots$ 中的一个,例如 $q=q_1$;以此类推.因此有下面的定理.

定理 21(基本定理) 任何整数都能分解成素因数,并且只有一个分解法.

最后,在因数 $p,q,r,\cdots$ 中也可能有相同的;把相同的因数合并起来,便得下面形式的分解式

$$a=p^{\alpha}q^{\beta}r^{\gamma}\cdots$$

其中,$p,q,r,\cdots$ 是不同的素数,而 $\alpha,\beta,\gamma,\cdots$ 是大于等于 1 的自然数.

§11　埃拉托塞尼筛子

把一个已知数实际分解成素因数的问题是数学难题之一，至今还没有一个实用的分解法. 现在只能运用实验法去分解. 这个问题的特殊情形是去检验已知数是否是素数. 因此就有这样的问题：求在所给区间内的一切素数. 埃拉托塞尼（在公元前3世纪）早已应用下述的方法来求小于所给限度 A 的一切素数. 写出从2到数 A 的一切整数；在所得的表上划掉2以后的每第二个数，3以后的每第三个数（同时以前已经划掉的那些数也应该计算在内），5以后的每第五个数，7以后的每第七个数，等. 我们注意：利用这样的划法，在每一步骤之后，所留下来的第一个未曾划掉的数一定是素数，也就是下一个素数；在它之后应该重新开始去划. 在所有这样划过之后，留在我们表上的未被淘汰的那些数也就是小于 A 的一切素数. 因为事实上我们把小于 A 的一切合成数统统都已经划掉了.

这个所谓“埃拉托塞尼筛子”的方法虽然简单，但是也有缺点：若数 A 很大，则这个方法便十分冗长，因而也很不实用.

关于这个方法我们还要注意两点：

(1) 只要在开始时留下2（唯一的偶素数），以后光写小于 A 的所有奇数，并且照上面所说的划法进行，即是划掉3以后的每第三个数，5以后的每第五个数，以此类推，也就够了.

(2) 上述步骤进行到大于等于 $\sqrt{A}$ 的第一个素数时就可以停止了：这时一直到 A 本身为止所有留下来未曾划掉的数全是素数. 这是由下述定理得来的.

定理 22　任何合成数 a 必然能被某一个小于等于 $\sqrt{a}$ 的数除尽.

证　设 $a=bc$，若 a 不是完全平方，则二数 b,c 中一个大于 $\sqrt{a}$，而另一个小于 $\sqrt{a}$；若 a 是完全平方，则可能得到 $b=c=\sqrt{a}$.

在确定一个已知数是否是素数，或者在分解一数成素因数时，这个定理可减少实验的步骤.

关于埃拉托塞尼筛子的举例　设 $A=100$，我们有表

2, 3, 5, 7, ~~9~~, 11, 13, ~~15~~, 17, 19, ~~21~~, 23, ~~25~~, ~~27~~, 29, 31

~~33~~, ~~35~~, 37, ~~39~~, 41, 43, ~~45~~, 47, ~~49~~, ~~51~~, 53, ~~55~~, ~~57~~, 59, 61, ~~63~~, ~~65~~

67, ~~69~~, 71, 73, ~~75~~, ~~77~~, 79, ~~81~~, 83, ~~85~~, ~~87~~, 89, ~~91~~, 93, ~~95~~, 97, ~~99~~