arXiv:2611.29380v1 [math.NT] 22 Nov 2026

论希腊人的数论

FRANZ LEMMERMEYER

Zusammenfassung. 本文将介绍欧几里得数论基本定理，并提供证据说明：这一如今已鲜为人知的定理，在高斯之前的数论学家中曾像高斯版本的基本定理一样广为人知。

在第二部分，我们将阐释欧几里得算术基本定理对现代代数的意义。为此，我们从满足高斯引理的环出发，进而探讨整闭性等概念，以及戴德金—普拉格定理。

第一部分：欧几里得算术基本定理

算术基本定理，即自然数 $\mathbb{N}$中的素因数分解唯一性，最早由高斯在其《算术研究》 [14] 中明确表述并证明。有时会读到这一定理源自欧几里得的说法。这当然不全错，不过更好的做法是换个角度提问：关键并不在于欧几里得是否知道每个数都能唯一分解为素因子；研究完全数和亲和数构造的多数作者，至少都熟悉这一结果的某些特殊情况；其中一些人（欧几里得之后尤以 al-Farisi（见 [1], ）和 Prestet（见 [15]）为然）还给出了仿照欧几里得方法的证明 `。但直到高斯，唯一素因数分解才被确立为一条基本定理。

因此，更有趣的问题是：欧几里得是否像我们一样理解这一结果，即是否认识到它的基础性特征。后者无疑并非如此。这就引出了这样一个问题：欧几里得数论究竟以什么为基础？对此，通常的回答是指出欧几里得算法的基础性特征。可是，欧几里得数论的主要成果，尤其是断言不可约元素为素元的欧几里得引理，在欧几里得那里都是借助命题 VII.19 证明的。下文将说明，这个鲜为人知的命题不仅对欧几里得具有基础性意义，而且还被欧拉和其他数论学家用作唯一素因子分解的“替代”，即使在今天，它仍以不同的名称在现代代数中发挥着一定作用。

1. Eindeutige Primzerlegung?

当人们读到欧几里得已知并证明了唯一素因数分解时，这一说法指的是欧几里得的著作版本（参见 Thaer[30]和 Heath [16]的欧几里得著作版本）：

2020 *Mathematics Subject Classification.* 01A20,01A60,11T55.1

> 命题 *IX.14.* 如果一个数是能被给定素数整除的最小数，那么它不会被除原先那些素数以外的任何其他素数整除。

换句话说：若 $n = \mathrm{kgV}(p_1, \dots, p_t)$ 是 p_j的最小公倍数[1]，那么 p_1、…、 p_t 就是 n的唯一质因数。看来是 Heath [16, vol. II, p. 402],在其中看到了唯一素因数分解：他在对 IX.14 的评论中写道：

> 换句话说，一个数只能以一种方式分解为质因数。[2]

欧几里得不用乘积，而是使用能被 p_1、…、 p_t 整除的最小数，这是因为欧几里得的几何语言只允许他谈论两个数（平面数）或三个数（立体数）的乘积。

他以一个能被三个不同素数整除的数为例来进行证明¨，这符合希腊数学的惯例，也是因为希腊人缺乏完全归纳法这一技巧。

与唯一素因数分解定理相比，命题 IX.14 的主要缺陷在于，它只对不同素数的乘积给出唯一素因数分解，也就是说，只适用于无平方因子数；归根结底，命题 IX.14 对一个乘积只说明 $n = p_1^{a_1} p_2^{a_2} p_3^{a_3}$的素因子只有 p_1、 p_2 和 p_3 n [3]。

尽管存在这一缺陷，欧几里得的命题 IX.14 与今天的唯一素因数分解定理一样，都是借助“欧几里得引理”（命题 VII.30）来证明的；该引理指出，由 $p \mid ab$ 可知，若¨是素元[4] p，则必有 $p \mid a$ 或 $p \mid b$ 。因此，阻止欧几里得完整阐述并证明算术基本定理的原因，一方面无疑是他不得不使用的语言不够完善；另一方面，也因为对欧几里得来说，命题 IX.14 远非基本命题，不过是一个小引理，他只是顺带提及。欧几里得在后文中再也没有用到命题 IX.14；仅凭这一点，就足以说明在此不应将它称作算术基本定理。

欧几里得数论的基础是欧几里得算法的存在性，而从中获得核心定理的基本定理是欧几里得的命题 VII.19，下面我们将转而讨论这一命题。

---

[1]互素数的最小公倍数等于它们的乘积，这由欧几里得命题 VII.34 可知。[2]换句话说，一个数只能以唯一的方式分解为素因子。[3]不过还应补充一点：欧几里得在其他地方证明了一些定理，可用来进一步阐明第九卷命题 14：例如，欧几里得在第九卷中证明（IX.13），素数幂的因数只有数 1、 p、 p^2、……、 p^{n-1}（在欧几里得看来，没有数能整除它自身）。最后，欧几里得还证明（IX.36），数 $2^{p-1}q$ 的因数只有 ¨ 个数，即由 1、2、4、……、 2^{p-1}、 q、 $2q$、 $4q$、……、 $2^{p-2}q$ 给出。[4]欧几里得所说的素数，与现代代数中所谓的不可约元素相符。欧几里得引理所述的性质，则被用来定义素数。

2. Euklids Proposition VII.19

为了理解欧几里得的命题 VII.19，我们需要他的定义 VII.20：

> 当第一个数与第二个数的倍数关系，和第三个数与第四个数的倍数关系相同，或者第一个数是第二个数的部分、第三个数是第四个数的部分，或者两者分别是相同的部分时，这些数便成比例。

第一个数是第二个数的倍数，且第三个数是第四个数的相同倍数，意即存在一个自然数 m，使得 $a = mb$ 和 $c = md$。相应地，“相同的部分”意即存在一个因数 n，属于 b 和 d，使得 $a = \frac{1}{n}b$ 和 $c = \frac{1}{n}d$；由 $b = nx$ 和 $d = ny$ 可得 $a = x$、$b = nx$、$c = y$、$d = ny$。最后，“相同的部分”意即 $a = \frac{m}{n}b$ 和 $c = \frac{m}{n}d$，对于自然数 m，n，使得 $n \mid b$ 和 $n \mid d$。[5] 换言之，这表示：

定义。对于自然数、a，b，c，$d \in \mathbb{N}$，比值 $a : b$ 和 $c : d$ 成比例（即满足 $a : b = c : d$），当且仅当存在 m，n，x，$y \in \mathbb{N}$，使得

$$a = mx, \quad b = nx, \quad c = my, \quad d = ny. \tag{1}$$

例如，$6 : 9 = 2 : 3$ 可通过 $m = 3$、$n = 1$、$x = 2$ 和 $y = 3$ 得到。因此

> 命题 *VII.19*。如果四个数成比例，那么第一个数与第四个数的乘积等于第二个数与第三个数的乘积。如果第一个数与第四个数的乘积等于第二个数与第三个数的乘积，那么这四个数成比例。

因此，欧几里得断言，$a : b = c : d$ 当且仅当 $ad = bc$ 成立。在随后的命题 VII.20 中，欧几里得证明了具有比值 $c : d$ 的最小数 a，b 整除这些数 c 和 d，并且满足 $c = am$ 和 $d = bm$。最后，在 VII.21 和 VII.22 中证明了，a 和 b 当且仅当 a 和 b 互素时，才是具有 $a : b = c : d$ 的最小数。

我们倾向于把欧几里得的数的比例等同于现代的分数（对欧几里得来说，比例不是数，而且他也没有说明如何将比例相加）；用这种语言来说，命题 VII.19 及后续命题要证明的是，每个分数都能以唯一的最简形式表示。

数与量。除了数的比例，欧几里得在第五卷中还讨论了量的比例；量包括角、长度、面积和体积，也就是能够连续变化的对象。欧几里得所说的所有同类量都具有以下性质：它们可以相加，并且具有阿基米德性质，其含义如下：若 A 和 B 是同类的量（这类量可以按大小进行比较），那么总存在一个$n \in \mathbb{N}$，使得 $nB > A$。

对于量 A：B 和 C：D 的关系，根据一条归于欧多克索斯的定义（定义 V.5），A：$B = C$：D 当且仅当满足：对于所有

[5]我们将前两种情况视为最后一个定义的特殊情形，分别对应 $n = 1$ 和 $m = 1$；不过，欧几里得的数的概念与我们的不同：在他看来，数是单位 1 的非零倍数，而单位本身不是数。[6]这里，A 与 B 以及 C 与 D 当然必须是同类量。

自然数 m,n ， $mA<nB$ （$mA=nB$； $mA>nB$）当且仅当$mC<nD$ （$mC=nD$; $mC>nD$）成立。

由此可以证明，例如，内接于圆的相似多边形彼此之比等于其圆的直径上的平方数之比（命题 XII.1），或者圆彼此之比等于其直径上的平方数之比（命题 XII.2）。

为了明确区分数与量的成比例定义，我们指出如下：

> 欧几里得关于数的成比例定义不仅在 $\mathbb{N}$中有意义，而且在任意采用乘法记号幺半群中也有意义。
> 关于量的成比例定义对于所有采用加法记号的、并且在上述意义下具有“阿基米德性质”的幺半群都有意义。

原则上，也可以把数看作大小¨；但欧几里得并没有这样做。有时有人声称，欧几里得有意或无意地将关于大小比例的论述应用于数；我认为这种说法大多缺乏依据，也与这样一个事实不太相符：数的比例论显然比大小的比例论 ¨更早[8] 。

3. Folgerungen aus Euklids VII.19

欧几里得《几何原本》VII.19乍看之下是一个不起眼的结果；但实际上，它是一个非同寻常的结论。接下来，我们将简要讨论由VII.19得出的几个著名推论。首先是

命题1。 由*VII.19*可推出欧几里得引理：所有不可约元都是素元。

证明。 设 p不可约且 $p\mid bc$，因此 $pd=bc$。根据 VII.19，存在 m， n， x， y，使得 $p=mx$、 $b=nx$、 $c=my$ 和 $d=ny$成立。由于 p 不可约， m 或 x 是单位，这意味着在第一种情况下 $p\mid b$ 成立，在第二种情况下 $p\mid c$ 成立。□

VII.19 也足以证明欧几里得引理的以下推广：

命题2。 欧几里得关于自然数的命题 *VII.19* 等价于以下结果：若 $a\mid bc$ 且 最大公因数 $(a,b)=1$，则 $a\mid c$成立。

证明。 假设 VII.19 成立。若 $a\mid bc$，即对于某个 $d\in\mathbb{N}$，有 $ad=bc$和¨，那么存在m， n， x， $y\in\mathbb{N}$，使得 $a=mx$、 $b=nx$、 $c=my$和 $d=ny$成立。由于最大公因数$(a,\ b)=1$，因此必有 $x=1$，所以 $a=m$ 是 $c=my$的因数。

设 $ad=bc$，并令 $x=\mathrm{ggT}(a,\ b)$。那么存在 m， $n\in\mathbb{N}$，使得 $a=mx$和 $b=nx$。因此， $md=nc$ 且 $\mathrm{ggT}(m,\ n)=1$；这意味着 $m\mid c$，所以$c=my$ f¨ur ein $y\in\mathbb{N}$。然而，这就有 $d=\frac{nc}{m}=ny$，即满足（1）。□ —

如今，借助命题2（或欧几里得引理）来证明素因子分解的唯一性，当然已不成问题。在

[7]因为 $\mathbb{N}$ 本身也是一个加性阿基米德幺半群。[8]范德瓦尔登在 [31] 中实际上将整部第七卷归于毕达哥拉斯学派；正如我们将在下文解释的那样，当像毕达哥拉斯学派那样研究和声学与整数时，关于数的成比例定义几乎会自然浮现出来。相反，关于量的成比例定义通常归于欧多克索斯。

借助 Zermelo 的一个想法 [33] ，我们也可以直接从欧几里得《几何原本》VII.19 推导出这一点：

命题3. 不可约元素分解的唯一性可由欧几里得《几何原本》*VII.19*推出。

证明。若分解的唯一性不成立，则存在最小的自然数 N具有两种不同的因式分解。设 p 是第一种因式分解中的一个不可约因子，并写作 $N = ph$；同理，设 q 是第二种因式分解中的一个不可约因子，且 $N = qk$。由 $ph = qk$ ，根据VII.19，存在m、n、 x、 $y \in \mathbb{N}$，使得 $p = mx$、 $q = nx$、 $k = my$且 $h = ny$。由于 p不可约，必有$m = 1$ 或 $x = 1$ 。但在第一种情况下可得 $p \mid q$ （从而 $p = q$），在第二种情况下可得 $p \mid k$。在第二种情况下， $k < N$；根据 N 的选取， k 因此具有唯一的不可约元素分解；由于 $p \mid k$ ，其中包含 p ，所以由 N的第二种因式分解删去 q 后得到的 k的分解中也包含它。在这两种情况下， p 也都出现在第二种因式分解中；约去 p ，便得到一个自然数 $M = \frac{N}{p} < N$ ，它有两种不同的不可约元素因式分解：这与 N 具有最小性的假设矛盾，从而证明了该定理。□

Kalm´ar（参见 Sur´anyi [27, 28]）称欧几里得《几何原本》VII.19 为四数定理，并将其归功于欧拉。欧拉也早已知道将其推广到更多个数的情形（从一个因式分解 $a_1 \cdots a_i = b_1 \cdots b_j$ 出发）；只需根据简单的四数定理，按因子个数作归纳法 ¨即可得出这一推广。随后，Kalm´ar 指出，这一推广可以推出素因子分解的唯一性（另见 Bell [4, 5], Rosenthall [26] 和 Erd˝os & Sur´anyi [9]）；Sur´anyi [28, 在第 44 页及后续页] 为四数定理给出了一个几何证明。似乎迄今为止还没有人注意到，四数定理源自欧几里得 [9]。

¨例如，借助唯一素因子分解定理证明下述结果是很容易的。许多关于丢番图方程的初等研究都会用到这一结果：¨

命题4。 若 a、 $b \in \mathbb{N}$ 互素，且 ab 是一个平方数，那么 a和 b 也都是平方数。

这个命题也是欧几里得《几何原本》VII.19 的一个简单推论，稍加验算即可得出（我们将在命题 9 的证明中再次回到这一点）。高斯在《算术研究》中最早指出，这个结果（或者说推广到 n 次幂的情形）可由 $\mathbb{Z}$ 中的唯一素因子分解推出。有人常常反过来说，命题 4 只能借助算术基本定理来证明，但这种说法是错误的。

欧拉常被认为在自己的著作中无意识地使用了唯一素因数分解，或将其视为理所当然。他在第一篇关于丢番图问题的论文中提到了命题 4：

[9]熟悉《几何原本》的人，自然能立刻说出这一点；但看来，同时对《几何原本》和现代代数都足够熟悉的数学家寥寥无几。就连专门研究希腊数学的 Sur´anyi，也忽略了欧几里得《几何原本》VII.19 与四数定理之间的联系。

> 由两个或多个彼此互素的数相乘所得的数，不可能是平方数、立方数或任何其他次幂，除非各个因子本身分别是平方数、立方数或此类其他次幂。[10]

他没有给出证明，而是接着指出：

> 这一引理的证明很简单，而且欧几里得早已给出，因此在此阐述实属多余。[11]

我不知道欧拉这里指的是欧几里得的哪个结论。对于平方数，这一断言可以相对简单地从欧几里得关于相似平面数的理论推出（用今天的话来说，相似平面数是指乘积为平方数的数；参见第九卷命题1和命题2）；至于更高次幂，则可以稍费些功夫，从他第八卷中的许多命题推出。

因此，对于我们会借助唯一素因数分解——也就是数论入门课程或高斯《算术研究》——来解决的问题，欧拉只需援引欧几里得即可。我认为颇为合理的是，对于其他一些我们认为存在缺漏、而这些缺漏可以通过唯一素因数分解来弥补的地方，欧拉也会用援引欧几里得的方式来驳回可能的异议。

在 [11] 例如，¨他引入了 $\sigma(n)$，即 $n \in \mathbb{N}$所有因数之和，用来研究亲和数；并在引理1中证明 σ 具有乘法性，也就是说，对于互素的数 m，n 有$\sigma(mn) = \sigma(m)\sigma(n)$¨。他的证明如下：“因为乘积 mn 首先包含两个因子 m 和 n各自的因数，而且还可以被 m 的因数与n的因数的乘积整除。因此，mn 所有因数之和等于 $\sigma(m)$与$\sigma(n)$的乘积。”所以欧拉使用了下面这个未经证明的引理：

引理 5. 设 m 与 n 互素。那么，mn的每个因数 a 都可以唯一地写成 $a = rs$ 的形式，其中 $r \mid m$ 且 $s \mid n$。

如今，我们可以毫不迟疑地从算术基本定理推出这个引理；而欧拉大概会援引欧几里得：r 和 s 的存在性可由以下方式得到：$a \mid mn$ 表示对于某个 $b \in \mathbb{N}$有 $ab = mn$ ¨；欧几里得《几何原本》VII.19给出了 r，s，t，$u \in \mathbb{N}$ 的存在性，使得 $a = rs$、$b = tu$、$m = rt$ 且 $n = su$，于是结论成立。唯一性则显而易见：若 $a = rs = r's'$ 满足r，$r' \mid m$ 且 s，$s' \mid n$，则 $r \mid r's'$，并且最大公因数$(r,\ s')$ |最大公因数$(m,\ n) = 1$，根据命题2，得 $r \mid r'$。同理可得 $r' \mid r$，因此 $r = r'$ 且 $s = s'$。

4. Die Lücke

欧几里得《几何原本》VII.19 的有效性，正如我们所见，是不可约元素分解唯一性的关键。一个简单的结构，其中 VII.19 不再成立，是模 4 的所有自然数组成的幺半群（希尔伯特在他的讲座中使用了模 5 的所有自然数组成的幺半群，以此引出理想的概念）。在其中，显然有（这个等式也立即表明，命题 4 的类比在其中不成立），但 $49 : 21 \neq 21 : 9$；因为由

[10]一个由两个或更多两两互素的因数组成的数，不可能是平方数、立方数或任何其他幂，除非各个因子本身分别是平方数、立方数或相应的其他幂。[11]这个引理的证明很简单，欧几里得早已传述过；因此在此赘述便毫无必要。 ⋯⋯

（1）可知，存在 $m,n,x,y\in M$，使得 $49=mx$、 $21=nx=my$ 和 $9=ny$。由于 9 在 M 中是不可约的，因此必有 $n=1$ 或 $y=1$ 。第一种情形下， $y=9$，所以 $9\mid my=21$；第二种情形下， $n=9$ ，因而同样有 $9\mid nx=21$；这两种情况都不可能。

相反，很容易证明，对于 a， b， $f\in M$，总有 $a\colon\ b=af\colon\ bf$成立。因此

$$49:21=49\cdot 9:21\cdot 9=21\cdot 21:21\cdot 9=21:9,$$

这里我们两次应用了观察结果 $a\colon\ b=af\colon\ bf$ 。然而，正如我们已经看到的，等式 $49\colon\ 21=21:9$ 是错误的。我们在哪一步犯了错？等式 $49\colon\ 21=21\cdot 21:21\cdot 9$和 $21\cdot 21\colon\ 21\cdot 9=21:9$，正如直接检验也很容易发现的那样，无疑是正确的。上述论证中的错误在于假设比例相等[12] 具有传递性：由 $a\colon\ b=c\colon\ d$ 和 $c\colon\ d=e\colon\ f$，一般不能推出 $a\colon\ b=e\colon\ f$ 也成立。

Taisbak 在 [29] 中发现，欧几里得在证明其基本定理 VII.19 时，恰好留下了这个空¨缺：他使用了等式的传递性，却没有证明。如何弥补这个空¨缺，可以在 Tais- [29] bak [22] 以及 Pengelley 与 Richman [22] 的著作中读到。这个简单的论证基于如下思路：证明可以或多或少地“规范地”选取四数定理中的一些数作为最大公¨因数¨:

引理 6. 设 $a\colon\ b=c\colon\ d$。那么存在 p、 q、 r、 $s\in\mathbb{N}$，使得 $a=pr$、 $b=qr$、 $c=ps$ 且 $d=qs$，其中我们可以选取 $r=$最大公因数(a,b) 和 $s=$最大公因数(c,d) ¨。

证明。由 $a\colon b=c\colon d$可知，存在数 $m,n,x,y\in\mathbb{N}$，使得 (1) 成立。因此， $x\mid a$与 b的最大公因数，且 $y\mid c$与 d的最大公因数，于是存在 $i,j\in\mathbb{N}$，使得 a与 b的最大公因数为 $=ix$，而c与 d的最大公因数为 $=jy$。由 $ix\mid a=mx$ 和 $ix\mid b=nx$ 可得 $i\mid m$ 和 $i\mid n$，因此 $m=pi$和 $n=qi$满足 $p,q\in\mathbb{N}$。特别地， $a=pix=p\cdot$是 a与 b的最大公因数，且$b=q\cdot$是 a与 b的最大公因数。

现在我们断言 $i\mid j$。由于对称性理由（将 (a,b,x) 与 (c,d,y) 互换后，情形保持对称），同样有 $j\mid i$，因此 $i=j$。但这样一来，我们就如愿得到 $c=my=piy=pjy=p\cdot$是 c,d的最大公因数，且$d=ny=qiy=qjy=q\cdot$是 c,d的最大公因数。

还需证明 $i\mid j$。由 $m=pi$ 和 $n=qi$可得 $iy\mid my=c$和 $iy\mid ny=d$。因此， $iy\mid\mathrm{ggT}(c,d)=jy$，从而 $i\mid j$ 如所述。□

由此我们可以如下证明等式的传递性：设 $a\colon\ b=c\colon\ d$ 且$c\colon\ d=e\colon\ f$。根据引理 6，存在 $p,q\in\mathbb{N}$，使得 $a=p\cdot\mathrm{ggT}(a,b)$、 $b=q\cdot\mathrm{ggT}(a,b)$、$c=p\cdot\mathrm{ggT}(c,d)$ 且 $d=q\cdot\mathrm{ggT}(c,d)$。再次应用该引理，便可找到 $p',q'\in\mathbb{N}$，使得 $c=p'\cdot\mathrm{ggT}(c,d)$、$d=q'\cdot\mathrm{ggT}(c,d)$、 $e=p'\cdot\mathrm{ggT}(e,f)$且 $f=q'\cdot\mathrm{ggT}(e,f)$。约分后得到 $p=p'$和 $q=q'$，因此显然有$a\colon\ b=e\colon\ f$。

请注意，上述幺半群 M 中的引理 6 并不成立，因为在M 中，两个数未必有最大公因数。因此，

[12]人们可能会试图将其归因于：在欧几里得那里，相等关系的传递性是一条公理（“与同一个量相等的量彼此相等”）；然而，我们所谓的比例相等，并不是欧几里得意义上的相等：欧几里得并不定义两个比例 $a\colon\ b$ 和 $c\colon\ d$ 相等，而是说，如果存在如（1）中的数，那么四个数成比例。正因如此，许多欧几里得注释者所写的不是 $a\colon\ b=c\colon\ d$，而是更准确的 $a\colon\ b\colon\colon c\colon\ d$。

$3^2\cdot 7\cdot 11$ 和 $3^2\cdot 7\cdot 19$ 在 M 中的公约数为 $1, 3^2$ 和 $3\cdot 7$，但不存在关于整除关系的最大公约数，也就是说，不存在一个能被所有公约数整除的公约数。

5. Euklid oder Pythagoras?

许多数学史家将欧几里得进入数论的途径归于毕达哥拉斯学派。人们认为，他们是通过 ¨音乐研究比例的：他们观察到，当相应的音调和谐地鸣响时，振动琴弦的长度彼此呈简单的¨比例。因此，1 : 2 和 2 : 3 的比例分别对应八度和五度。

最初的观察之一¨可能是，某些比例可以化简：例如，$2 : 4 = 1 : 2$。最终，这个问题¨必然导向这样的结论：比例可以唯一地约分：若 m 和 n 以最简形式表示为 $a : b = m : n$，则有 $m \mid a$ 和 $n \mid b$；更确切地说，存在一个$x \in \mathbb{N}$，使得 $a = mx$ 和 $b = nx$。然而，这正是欧几里得命题 VII.20 的内容。随后，在 VII.22 中证明了最简的 m 和 n 互素。

一旦通过经验发现了 VII.20，且有 $a : b = c : d$，便可分别推出 $a = mx$ 和 $b = nx$，以及 $c = my$ 和 $d = ny$。而这恰恰就是欧几里得对数的成比例关系所下的定义；这一关系由此十分自然地从对比例最基本性质的研究中产生。

范德瓦尔登认为，[31] 毕达哥拉斯学派将这一四数定理作为其数论的基础，欧几里得后来基本原样地承袭了这一理论及其构建方式。¨然而，无论是范德瓦尔登，还是他之前和之后的其他注释者，都更倾向于将欧几里得关于数的成比例关系的定义视为失误¨，而非天才之举。 ¨不过，上述考察以及例如引理 5 的证明表明，这一定义一方面十分自然，另一方面，四数定理完全适用于证明丢番图分析中的基本结果。

除了范德瓦尔登为论证欧几里得第七卷源自毕达哥拉斯学派而列举的论据外，数的比例中缺少比例相等的传递性证明，也可以视为支持这一说法的证据：以欧多克索斯给出的比例相等的定义为基础，比例相等的传递性证明几乎不言自明。然而，欧几里得还是在V.11中给出了证明。这或许是因为量的比例理论源自欧多克索斯，而且在他那个时代，数学家们已经普遍认识到，这类推理步骤必须加以证明。在我看来，毕达哥拉斯学派很可能只是忽略了数的比例相等的传递性根本并非不言自明。尽管欧几里得当然知道V.11，但他也没有意识到这一点，这就比较令人惊讶了，不过这或许可以解释为：他几乎没有作任何重大改动，就将毕达哥拉斯学派的数论纳入了自己的第七卷。

---

[13]例如，D. Fowler 在 [12]:

Commentators rarely point out the unsatisfactory nature of this definition: it is a vivid, though incomplete, description of four numbers in proportion, and not the mathematical criterion needed for the foundation of a theory.

不过，这或许可以解释为：他几乎没有作任何重大改动，就将毕达哥拉斯学派的数论纳入了自己的第七卷。

6. Der Vierzahlensatz

为了 ¨明确欧几里得四数定理的意义，我们把满足该定理的整环称为 Riesz[14] 环。在 Riesz 环中， R 由 $ad = bc$ 和 a， b， c， $d \in R$ 可推出存在 m， n， x， $y \in R$，其中 $a = mx$、 $b = nx$、 $c = my$ 以及 $d = ny$。

如果对于任意 b， $c \in R$，由 $a \mid bc$ f¨均可推出存在 r， $s \in R$，且满足 $a = rs$、 $r \mid b$ 和 $s \mid c$，则称元素 $a \in R$ 为原元[15], 。注意，0 和单位元总是原元。

显然，一个整环当且仅当其中的每个元素都是原元时，它才是 Riesz 环。下面的命题表明，在 Riesz 环中，所有不可约元素都是素元：

命题 7。 不可约元素当且仅当它们是素元时，才是原元。

证明。设 a 是素元且 $a \mid cd$；则不妨设 $a \mid c$。由 $r = a$ 和 $s = 1$ 可得 $a = rs$、 $r \mid c$ 和 $s \mid d$，即 a 是原元。

现在设 a 不可约且为原元。若 $a \mid cd$，则存在 r， s，使得 $a = rs$、 $r \mid c$ 且$s \mid d$。由于 a 不可约， r 或 s ——不妨设为 r ——必为单位。由 $s \mid d$可知 $a \mid d$，因此 a 是素元。□

欧几里得在命题 VII.19 中实质上证明了 $\mathbb{Z}$ 是 Riesz 环；他关于 $\mathbb{N}$ 中的不可约元素是素元的证明，实质上是上述证明的一半。

仔细考察欧几里得关于 VII.19 的证明（或由 Taisbak 对其所作的补充），可以发现，四数定理在所有最大公因子环中都成立（这些是整环，其中任意两个元素都有一个最大公因数），也就是说，每个最大公因子环都是 Riesz 环。

这里需要指出，原元与不可约元或素元截然不同：多个不可约元（或素元）的乘积不再是不可约元（或素元），除非只有一个因子这一平凡情形。然而，原元则满足：

引理 8. 原元的乘积仍是原元。

证明。设 $a, b \in R$ 为原元；若 $a = 0$ 或 $b = 0$，则 $ab = 0$ 是原元，因此我们可以假设 $a, b \neq 0$ 。设 $ab \mid c_1c_2$，于是 $c_1c_2 = abd$。由于 a 是原元，存在因式分解 $a = a_1a_2$ ，其中 $a_i \mid c_i$。令 $c_i = a_id_i$，则可得 $abd = c_1c_2 = a_1a_2d_1d_2 = ad_1d_2$，因此 $bd = d_1d_2$。由于 b 是原元，故有 $b = b_1b_2$ ，其中 $b_i \mid d_i$。

由此， $ab = a_1b_1a_2b_2$ 与 $a_ib_i \mid a_id_i = c_i$，因此 ab 是原元。由归纳法可知，任意多个素元素的乘积都是原元。□

现在我们证明命题 4 的以下推广：

---

[14]Zafrullah [32] 将这些环称为准 Schreier 环；不过，下文我们将看到，Riesz 环的整除群是群论意义上的“Riesz 群”。[15]这一概念可追溯至 Cohn [7] 。

命题 9。 设 R *Riesz*。如果对 $a,b,c \in R$， $ab = c^2$ *f* ¨成立，且 a 和b 互素，那么存在一个单位 $e \in R^\times$，使得 ae 和 be 是R 中的平方数。

注。 虽然只有在最大公因子环中，才有意义讨论任意两个环元素的最大公约数，但在任意整环中，我们仍可称某些元素“互素”：按照定义，这些元素的所有公约数都是单位元。例如，在 $R = \mathbb{Z}[\sqrt{-5}]$ 中，2 和 3 互素，而在 R 中，6 和 $2 + 2\sqrt{-5}$ 没有最大公因数。 —

命题 *9* 的证明。 根据四数定理，存在 $m, n, x, y \in R$，使得 $a = mx$、$b = ny$ 和 $c = my = nx$。将四数定理应用于等式 $my = nx$，便可推出存在 $r, s, t, u \in R$，使得 $m = rs$、 $y = tu$、 $n = rt$ 和$x = su$。由 a 和 b，显然 m 与 n，以及 x 与 y 也互素，因此 r 和 u 是 R 中的单位元。由 $e = 1/ru$，于是有 $ae = mxe = rs^2ue = s^2$ 和$be = nye = rt^2ue = t^2$。□

尽管欧拉在未加证明的情况下使用的某些事实可以用欧几里得四数定理加以证明，但 Riesz 环仍然只是“几乎”唯一分解环。考察两个因式分解 $a_1 \cdots a_m = b_1 \cdots b_n$，在 Riesz 环中我们只能推出这两个因式分解具有共同细化：存在元素 $c_{ij} \in R (1 \le i \le m, 1 \le j \le n)$，使得 $a_i = c_{i1} \cdots c_{in}$和 $b_j = c_{1j} \cdots c_{mj}$。对于 $m = n = 2$，这正是四数定理；一般情形（由四数定理通过归纳法得到）称为“Schreier 细化性质”。例如，全体代数整数构成的环具有这一细化性质，但由于缺少不可约元素，它不是唯一分解环。

如果整环中每个非零元素都能写成一个单位与若干不可约元素的乘积，则称该环具有原子性。因此有如下

定理 10. 整环 R 当且仅当它是唯一分解环时，才是 R *Riesz* 环且具有原子性。

证明. 在 Riesz 环中，不可约元素都是素元（由命题7可知）；因此，不可约元素的因式分解是唯一的。反过来，若R 是唯一分解的，则 R 是最大公因子环，因而是 Riesz 环；其次，每个元素 $\neq 0$ 都能分解为不可约元素（甚至是素元）的乘积。□

由于命题7，这一结论比著名的定理稍弱一些；该定理指出，整环当且仅当具有原子性且每个不可约元素都是素元时，才是唯一分解环。

数论的欧几里得构造可以概括如下：

$$\text{Euklid} \longrightarrow \text{GGT} \longrightarrow \text{Riesz} \longrightarrow \text{AP},$$

其中，AP 表示欧几里得引理成立，也就是说，不可约元素（原子）是素元。更一般地，可以证明以下包含关系：

这里，HI 表示主理想环，ZPE 表示唯一分解整环（即能唯一分解为素元的环），AP 表示所有原子（即所有不可约元）都是素元的环。贝祖环指的是其中任意两个

$$\begin{array}{ccccccccc} \text{Euklid} & \subset & \text{HI} & \subset & \text{Bezout} & & & & \\ & & \cap & & \cap & & & & \\ & & \text{ZPE} & \subset & \text{GGT} & \subset & \text{Riesz} & \subset & \text{AP} \\ & & \cap & & & & & & \\ & & \text{atomar} & & & & & & \end{array}$$

元素 a, b 都有最大公因数，且该最大公因数可写成 R-线性组合的形式，由 a 和 b 组成；这等价于两个主理想之和仍是一个主理想。

希尔伯特已将欧几里得几何建立在现代公理基础之上，但据我所知，对欧几里得数论进行相应的研究迄今尚未开展。例如，可以问：下列命题在哪些环中成立：a与 b 互素（即每个公因数都是单位），并且 $a \mid bc$，那么 $a \mid c$。命题2的证明的第一部分表明，这在 Riesz 环中成立；但证明的第二部分利用了最大公因数的存在性，因此我们不能断定这类环也是 Riesz 环。另一方面，具有这一性质的环是原子为素元的环（AP）。现在可以一般地提出这样的问题：欧几里得数论中的命题在哪些整环中成立，也就是说，证明这些命题需要哪些公理。

7. Rieszsche Gruppen

本节将讨论四数定理的一些推广。为此，我们将更一般地研究 Riesz 群。

设 R 是一个整环，其商域为 K。我们提醒，对于 a、$c \in K^\times$，$a \mid c$¨ 意味着存在一个 $b \in R$，使得 $ab = c$。对于整除性质的研究，单位元无关紧要；因此，与其考虑 $K^\times$，不如考虑商群 $G(R) = K^\times/R^\times$，我们也可以将其看作非零分式主理想群；$G(R)$ 的元素暂时记作 $aR^\times$ =(a)。群 $G(R)$ 按照 $(a) \leq (b)$ 半序化，当且仅当 $a \mid b$，即当 $\frac{b}{a} \in R$ 时成立。进一步，$(a) \leq (b)$¨ 等价于对于任意 $(c) \in G(R)$，有 $(ac) \leq (bc)$¨。因此，集合 $G(R)^+ =\{(g) \in G(R) : (g) \geq (1)\}$ 中所有“正”元素，正好由全部整主理想 $\neq (0)$ 构成；显然它是一个幺半群，由 $R^* = R \setminus \{0\}$ 通过转到理想，即通过将相伴元素视为同一元素而得到。

现在我们要把欧几里得四数定理翻译成这种语言
若为 $ad = bc$，则有 $a \mid bc$，因此对于$G(R)$中的相应主理想，有 $(a) \leq (b)(c)$ f¨。根据四数定理，存在 r，s，t，$u \in R$，使得 $a = rs$、$b = ru$、$c = ts$以及 $d = tu$。因此有 $r \mid b$ 和 $s \mid c$，从而有 $(r) \leq (b)$ 以及 $(s) \leq (c)$。因此有

命题11. 设 R 为一个整环。那么，当且仅当 $G(R)$具有以下“*Fuchs* 插值性质” F_2 时，四数定理成立[16]：若 $a, b, c \in G(R)^+$ 且 $a \leq bc$，则存在因式分解 $a = rs$，满足 $r, s \in G(R)^+$，使得 $r \leq b$ 且 $s \leq c$。

[16] 从现在起，我们将 $G(R)$的元素不再记作 (a)，而简单地记作 a。

现在我们将定义偏序阿贝尔群 G的一系列一般插值性质和细化性质:

- "Fuchs 插值性质" F_n: 若 $a, b_1, \ldots, b_n \in G^+$, 且 $a \le b_1 \cdots b_n$, 则存在 $a_i \in G^+$使得 $a = a_1 \cdots a_n$且 $a_i \le b_i$适用于$1 \le i \le n$。
- "Riesz 插值性质"$R_{m,n}$: 若给定 $a_1, \ldots, a_m, b_1, \ldots, b_n \in G$, 且对所有 $1 \le i \le m$ 和 $1 \le j \le n$都有 $a_i \le b_j$, 那么存在一个$c \in G$, 使得对所有 i 和 j都有 $a_i \le c \le b_j$。
- "Schreier 细化性质"$S_{m,n}$: 若给定 $a_1, \ldots, a_m, b_1, \ldots, b_n \in G^+$ 且满足 $a_1 \cdots a_m = b_1 \cdots b_n$, 则存在元素 $c_{ij} \in G^+$ ($1 \le i \le m, 1 \le j \le n$) , 使得 $a_i = c_{i1} \cdots c_{in}$ 且 $b_j = c_{1j} \cdots c_{mj}$。
- "欧几里得细化性质"$E_{m,n}$: 设 a, b_i, $c_j \in G^+$ 以及$a \le b_i c_j$ f¨ur $i = 1, \ldots, m$ 和 $j = 1, \ldots, n$, 那么存在一个因式分解 $a = rs$, 使得 r, $s \in G^+, r \le b_i$ 且对于所有 $1 \le i \le m$ 和 $1 \le j \le n$, 都有 $s \le c_j$ f¨ur。

性质$R_{2,0}$ 和$R_{0,2}$ 可以这样理解: 对于 a_1, $a_2 \in G$, 存在一个 $c \in G$, 使得 $a_1 \le c$ 且 $a_2 \le c$ (即$R_{2,0}$) ; 或者存在一个 $b \in G$, 使得 $b \le a_1$ 且$b \le a_2$ (即 $R_{0,2}$) 。具有此性质的半序群称为有向的[17]。整环的整除群 $G(R)$自动是有向的: 对于 a_1, $a_2 \in K^\times$, 显然总存在一个 $c \in K^\times$, 使得$a_1 \mid c, a_2 \mid c$ (取 c 为 a_1和 a_2中 (任意选取的) 数值的乘积即可) 。同理, 总能找到一个 $b \in K^\times$, 使得 $b \mid a_1$ 且 $b \mid a_2$。

现在我们断言

定理 12. 对于半序有向阿贝尔群 G, 以下性质等价:

(1) 在 G 中成立 $R_{2,2}$; *(2)* 在 G 中成立 $R_{m,n}$ 对所有 $m, n \ge 0$; *(3)* 在 G 中成立 F_2; *(4)* 在 G 中成立 F_n 对所有 $n \ge 1$; *(5)* 在 G 中成立 $S_{2,2}$; *(6)* 在 G 中成立 $S_{m,n}$ 对所有 $m, n \ge 1$; *(7)* 在 G 中成立 $E_{1,1}$; *(8)* 在 G 中成立 $E_{m,n}$ 对所有 $m, n \ge 1$; *(9)* 在 G 中成立 $[1, a] \cdot [1, b] = [1, ab]$ 对所有 $a, b \in G^+$ (此处 $[a, b] = \{r \in G : a \le r \le b\}$) 。

只需假设 G 是有向的, 便可从 $R_{2,2}$ 推出$R_{m,n}$。所有证明都是初等的 (本质上是完全归纳法) , 此处无需给出。

具有定理 12 中所列性质的半序阿贝尔群, 按照 L. Fuchs 的命名称为 [13] Riesz 群[18]。这些群最早由 F. Riesz [25] 1940 研究, 随后由 Birkhoff [6] 和 H. Bauer [3]进行了研究。在这些工作中, 还可以找到定理 12 的部分证明以及其他与其等价的性质。Schreier 细化性质 $S_{m,n}$ 是

[17]由于 $a \le b$ 与 $b^{-1} \le a^{-1}$ ¨等价, 因此半序群只要满足例如$R_{2,0}$, 便已是有向的。[18]更确切地说, 对于 Riesz 群, 不再要求满足交换性; 在这种情况下, 定理 12 中的性质并非都彼此等价。

四数定理的推广，Kalm´ár 曾利用它证明算术基本定理。在第二部分中，我们最终将需要欧几里得细化性质。

Abschliessende Bemerkungen

凡是深入研究欧几里得数论的人，很快就会发现，他的命题 VII.19，即四数定理，起着核心作用。即使只对高斯之前的数论史感兴趣，也必须了解欧几里得的数论著作，尤其是核心结果 VII.19：人们常常指责欧拉有些地方暗中使用了高斯的一项结果，即唯一素因数分解；这种说法首先多少有些时代错置，其次，鉴于欧几里得的 VII.19，恐怕也站不住脚。不过，这些话并非要为欧拉洗脱一切“过错”：按照今天的理解，他相当多的证明并不严谨，而且并非所有漏洞都能用欧几里得来弥补。但笼统地指责欧拉常常默默使用唯一素因数分解，或许确实值得重新审视。

[19]其他作者（甚至在高斯之后）也曾使用四数定理，而且没有提及欧拉或欧几里得：参见 Barlow [2, 页。 401], Kramer [20] 或 P´epin [23, 页。 24], [24, 页。 413]。

第一部分：欧几里得算术基本定理

Abstract. 本文介绍欧几里得的数论基本定理，并提供证据支持这样一种观点：这条如今鲜为人知的定理，在高斯之前的数论学家中，或许就像基本定理的高斯版本对我们一样广为人知。

在第二部分中，我们将阐释欧几里得算术基本定理对现代代数的意义。从满足高斯引理的环出发，我们将引出整闭包、戴德金布拉格定理等概念。

算术基本定理，即自然数集 $\mathbb{N}$ 中素因数分解的唯一性，最早由高斯在其《算术研究》 [14]中明确表述并证明。我们偶尔会读到，这条定理源自欧几里得。这当然并非全然错误；不过，更好的做法是换个角度提出问题：关键不在于欧几里得是否知道每个数都能唯一分解为素数。例如，研究完全数和亲和数构造的大多数作者都熟悉这一结果的至少一些特殊情形；其中一些人（在欧几里得之后，尤其是 al-Farisi，见 [1], ，以及 Prestet，见 [15]）也仿照欧几里得给出了证明 `。但只有高斯将唯一素因子分解确立为一条基本定理。

因此，真正有意思的问题是：欧几里得是否像我们一样理解这一结果，也就是说，他是否认识到它的基础性。这显然并非如此。由此引出一个问题：欧几里得数论的基础究竟是什么？通常的答案是指出欧几里得算法的基础性。然而，在欧几里得那里，他数论中的主要结果，尤其是欧几里得引理——不可约元素是素元——都是借助命题 VII.19 证明的。接下来，我们将说明，这个鲜为人知的命题不仅对欧几里得至关重要，欧拉和其他数论学家也曾将它用作唯一素因子分解的“替代品”；而且直到今天，它虽有不同的名称，在现代代数中仍发挥着一定作用。

8. Unique prime factorization?

当人们读到欧几里得知道并证明了唯一素因子分解时，这一说法指的是欧几里得的（参见 Thaer [30] 和 Heath[16] 编的欧几里得著作）：

> 命题 *IX.14*。如果一个数是被若干素数整除的最小数，那么除最初整除它的那些素数外，它不会被任何其他素数整除。

换句话说：如果 $n = \mathrm{lcm}(p_1, \ldots\ldots, p_t)$ 是[20] 这些数的最小公倍数，那么$p_1, \ldots\ldots, p_t$ 就是 n的唯一质因数。显然，Heath [16, 在第二卷第402] 页首次从这条陈述中看到了唯一素因子分解；他在对命题 IX.14 的评注中写道：

> 换句话说，一个数只能以唯一的方式分解为质因数。

[20]互素数的最小公倍数等于它们的乘积，这一点可由欧几里得《几何原本》第七卷命题34推出。

欧几里得使用的不是乘积，而是能被p_1、……、 p_t整除的最小数，这是因为欧几里得的几何语言只允许他讨论两个数的乘积（平面数）或三个数的乘积（立体数）。

他以三个不同素元整除的数为例完成证明，这符合希腊数学的惯例，也是希腊人缺乏数学归纳法这一技巧的结果。

与唯一素因子分解定理相比，命题 IX.14 的根本弱点在于，命题 IX.14 只对不同素元的乘积，也就是对无平方因子数，给出唯一的素因子分解；归根结底，对于乘积 $n = p_1^{a_1} p_2^{a_2} p_3^{a_3}$，命题 IX.14 只说明 p_1、 p_2 和 p_3 是 n[21] 的唯一质因数。

尽管存在这一缺陷，欧几里得的命题 IX.14 与今天的唯一素因子分解定理一样，都是利用“欧几里得引理”（命题 VII.30）证明的；根据该引理，对于素元[22] p，$p \mid ab$ 总是意味着 $p \mid a$ 或 $p \mid b$。一方面，欧几里得不得不使用的不完善语言，另一方面，命题 IX.14 对欧几里得而言远非基础性的事实——它不过是一个他顺带提及的小引理——这两点无疑使他无法完整地表述并证明算术基本定理。欧几里得此后再也没有使用他的命题 IX.14，而仅这一点就足以阻止我们在这一语境下称其为一个基本定理。

欧几里得数论的基础是欧几里得算法的存在，而推导出核心结果的基本定理是欧几里得命题VII.19，下面我们就来讨论它。

9. Euclid's Proposition VII.19

要理解欧几里得命题VII.19，我们需要先了解他的定义 VII.20：

> 当第一个数与第二个数成相同倍数、相同分数或相同份数时，第三个数与第四个数也如此，这些数便成比例。

第一个数与第二个数成相同倍数，正如第三个数与第四个数成相同倍数，意思是存在一个自然数 m，使得 $a = mb$ 和 $c = md$。类似地，“相同分数”是指存在一个因数 n，它是 b 和 d 的因数，且满足 $a = \frac{1}{n}b$ 和 $c = \frac{1}{n}d$；结合 $b = nx$ 和 $d = ny$，便得到 $a = x$、 $b = nx$、 $c = y$、 $d = ny$。最后，“相同份数”是指自然数 m 满足 $a = \frac{m}{n}b$ 和 $c = \frac{m}{n}d$，n，且 $n \mid b$ 和 $n \mid d$。[23]翻译过来，这意味着：

定义。对于自然数 $a, b, c, d \in \mathbb{N}$，比 $a : b$ 和 $c : d$ 成比例（即 $a : b = c : d$），当且仅当存在 $m, n, x, y \in \mathbb{N}$ 使得

$$a = mx, \quad b = nx, \quad c = my, \quad d = ny. \tag{2}$$

---

[21]不过还应补充一点：欧几里得在其他地方证明了一些可用于强化 IX.14 的定理。例如，在第九卷中，他证明了（除其他内容外，见 IX.13）：素数幂的唯一因数 p^n 是数 1、 p、 p^2、……、 p^{n-1}（对欧几里得而言，没有任何数能整除自身）。最后，欧几里得还证明了（IX.36）：对于素数 $q = 2^p - 1$，数 $2^{p-1}q$ 的唯一因数是 1、2、4、……、 2^{p-1}、 q、 $2q$、 $4q$、……、 $2^{p-2}q$。[22]欧几里得关于素数的概念与现代代数中所谓的不可约元相一致。欧几里得引理中的性质随后被用来定义素元。[23]我们会把前两种情形分别视为最后一个定义中的特殊情形 $n = 1$ 和 $m = 1$；然而，欧几里得的数概念与我们的不同：对他而言，数是真倍数 1，而单位元并不是一个数。

因此，例如，$6:2=9:3$ 可通过 $m=3, n=1, x=2$ 和 $y=3$ 得到。现在我们可以陈述

> 命题 *VII.19*。如果四个数成比例，则由第一数与第四数相乘所得的数等于由第二数与第三数相乘所得的数；反之，如果由第一数与第四数相乘所得的数等于由第二数与第三数相乘所得的数，则这四个数成比例。

因此，欧几里得断言，$a:b=c:d$ 当且仅当 $ad=bc$。在接下来的命题 VII.20 中，欧几里得证明，具有比值 $c:d$ 的最小数 a,b 整除这些数 c和 d，即满足 $c=am$和 $d=bm$。最后，VII.21 和 VII.22 表明，a 和 b是具有 $a:b=c:d$的最小数，当且仅当 a 和 b 互素。

我们倾向于将欧几里得的数的比例等同于现代分数（对欧几里得而言，比例不是数，而且他没有解释如何相加比例）；用这种语言来说，命题 VII.19 及后续命题旨在说明，每个分数都能唯一地写成最简形式。

关于数与量。除了数的比例之外，欧几里得还在第五卷中讨论了量的比例；这些量包括角、长度、面积和体积，也就是说，包括能够连续变化的对象。欧几里得所研究的同类量都具有以下性质：它们可以相加，并且以如下意义满足阿基米德性质：如果 A 和 B 是同类量（这类量可以按照大小进行比较），那么总存在一个 $n\in\mathbb{N}$，使得 $nB>A$。

对于量的比 $A:B$ 和 $C:D$，[24], 欧多克索斯所提出的一个定义（定义 V.5）表明，$A:B=C:$ 当且仅当满足以下条件：对于所有自然数 m,n，我们都有 $mA<nB$ $(mA=nB;\ mA>nB)$ 当且仅当 $mC<nD(mC=nD;\ mC>nD)$。

由此可证明，例如，内接于圆中的相似多边形彼此之比等于这些圆的直径的平方之比（命题 XII.1）；又如，圆彼此之比等于其直径的平方之比（命题 XII.2）。

为清楚说明数的比例关系定义与量的比例关系定义之间的差异，我们注意到以下几点：

- 欧几里得关于数的比例关系的定义，不仅适用于$\mathbb{N}$，也适用于任意以乘法记号表示的幺半群。
- 量的比例关系定义适用于所有以加法记号表示、且具有上述意义上的“阿基米德性”的幺半群。

原则上，数也可以被视为量[25]；然而，欧几里得并未这样做。我认为，有时会听到的那种说法——欧几里得有意或无意地将关于量的比例的命题应用于数——大体上缺乏依据，而且也与数的比例理论远早于量的比例理论这一事实不太相符[26]。

---

[24]当然，这里的 A和 B，以及 C 和 D，必须是同类的量。[25]毕竟，$\mathbb{N}$ 也是一个加性阿基米德幺半群。[26]在 [31], 中，范德瓦尔登将第七卷几乎全部内容归于毕达哥拉斯学派；正如下文将要说明的，如果像毕达哥拉斯学派那样关注和声学与整数，那么数的比例关系定义几乎是不言自明的。另一方面，量的比例关系定义通常被认为出自欧多克索斯。

10. Consequences of Euclid's VII.19

乍看之下，欧几里得《几何原本》VII.19 是一个不起眼的结果；然而事实上，它相当非凡。接下来，我们将简要讨论 VII.19 的一些著名推论。我们先从

命题13。 欧几里得引理由*VII.19*推出：所有不可约元素都是素元。

证明。 设 p 为不可约元素，且 $p \mid bc$，即 $pd = bc$。由VII.19，存在 m、 n、 x、 y，满足 $p = mx$、 $b = nx$、 $c = my$ 和 $d = ny$。由于 p 是不可约元素， m 或 x 是单位元；这意味着在第一种情况下 $p \mid b$ ，在第二种情况下 $p \mid c$ 。□

VII.19同样足以证明欧几里得引理的以下推广：

命题14。 对于自然数，欧几里得命题*VII.19*等价于以下结果：如果 $a \mid bc$ 且最大公因子$(a, b) = 1$，那么 $a \mid c$。

证明。 假设 VII.19 成立。若 $a \mid bc$，即对某个 $d \in \mathbb{N}$有 $ad = bc$ ，那么存在$m, n, x, y \in \mathbb{N}$，使得 $a = mx$、 $b = nx$、 $c = my$且 $d = ny$。由于 gcd$(a, b) = 1$，我们必须有 $x = 1$，因此 $a = m$ 是 $c = my$的因数。

现在设 $ad = bc$，并令 $x =$ gcd(a, b)。那么存在 $m, n \in \mathbb{N}$ ，使得 $a = mx$且 $b = nx$。因此 $md = nc$ 且 gcd$(m, n) = 1$；这意味着 $m \mid c$，即对某个 $y \in \mathbb{N}$有 $c = my$ 。但这样一来， $d = \frac{nc}{m} = ny$，也就是说 (2) 成立。□

如今，借助命题14（或欧几里得引理）证明素因数分解的唯一性当然已不成问题。然而，利用 Zermelo 的一个想法 [33]„ 可以直接从欧几里得《几何原本》VII.19 推导出这一结论：

命题15。 不可约元素分解的唯一性由欧几里得《几何原本》*VII.19*推出。

证明。 若唯一性不成立，则存在一个最小的自然数 N ，它有两种不同的分解。设 p 是第一种分解中的一个不可约因子，并记为 $N = ph$；同样，设 q 是第二种分解中的一个不可约因子，并记为 $N = qk$。由 $ph = qk$，VII.19给出 m、 n、 x、 $y \in \mathbb{N}$ 的存在，使得$p = mx$、 $q = nx$、 $k = my$ 以及 $h = ny$。由于 p 是不可约的，我们必有 $m = 1$或 $x = 1$。但在第一种情形下， $p \mid q$ （从而 $p = q$），而在第二种情形下， $p \mid k$ 。在第二种情形下，我们有 $k < N$，因此根据 N 的选取，数 k 具有唯一的不可约元素分解；由于 $p \mid k$，因子 p 出现在其中，因而也出现在由 N 的第二种分解删去 q后得到的 k 的分解中。因此在两种情形下， p 也都出现在第二种分解中，约去 p 后得到一个自然数 $M = \frac{N}{p} < N$ ，它有两种不同的不可约元素分解：这一矛盾违背了 N 的最小性，从而证明了该结论。□

Kalm´ar [19] （参见 Sur´anyi [27, 28]）称欧几里得《几何原本》VII.19为四数定理，并将其归功于欧拉。将定理推广到更多数（从一个分解 $a_1 \cdots a_i = b_1 \cdots b_j$ 出发）也早已为欧拉所知；这一推广可通过对因子个数应用归纳法，由简单四数定理推出。随后，Kalm´ar指出，素因数分解的唯一性可由这一推广得出（另见 Bell [4, 5], Rosenthall [26] 和 Erd˝os 与 Sur´anyi [9]），而 Sur´anyi

[28, 第44页及以下。] 给出了四数定理的几何证明。迄今似乎无人注意到，四数定理源自欧几里得[27]。

证明下面的结果是很容易的，例如可以借助唯一素因子分解定理；这一结果被广泛用于丢番图方程的许多初等研究中：

命题16。 如果 a、$b \in \mathbb{N}$ 互素，且 ab 是平方数，那么 a 和 b 也都是平方数。

这一命题同样是欧几里得《几何原本》VII.19的简单推论，这一点很容易验证（我们将在命题21中回到这一证明）。高斯在《算术研究》中首次指出， [14] 这一结果（或其推广到 n次幂）可由 $\mathbb{Z}$中的唯一素因子分解推出。相反的结论，即命题16只能借助算术基本定理来证明，也常被提及，但这是错误的。

欧拉常被认为在其著作中无意识地使用了唯一素因子分解，或者认为它是显然的；他在关于丢番图问题的第一篇论文[10]中提到了命题16：

> 由两个或多个彼此互素的数所组成的数，不可能是平方数、立方数或任何其他幂，除非各个因子分别是平方数、立方数或相应的其他幂。[28]

他没有给出证明，而是接着说道：

> 这个引理的证明很容易，而且欧几里得已经给出过，因此没有必要在这里再加以阐述。[29]

我不知道欧拉在这里指的是欧几里得的哪些结果。对于平方数，这一论断可以相对容易地由欧几里得相似平面数理论推出（用现代术语来说，相似平面数是乘积为平方数的数；参见 IX.1 和 IX.2）；而对于更高次幂，则可稍费周折地由他在第八卷中的许多命题推出。

因此，对于我们会借助唯一素因子分解来处理的问题——也就是说，诉诸数论入门课程或高斯的《算术研究》 [14], ——欧拉只需引用欧几里得便解决了这一问题。在我看来，很有理由相信，在其他地方，当我们发现某个空缺可以通过唯一素因子分解来填补时，欧拉也会以引用欧几里得来驳回应有的质疑。

例如，在研究亲和数时，他引入了 $n \in \mathbb{N}$ 的所有因数之和 $\sigma(n)$，并在引理1中证明 σ 是积性函数，即对于互质数 m, n，有 $\sigma(mn) = \sigma(m)\sigma(n)$。他的证明如下：“对于乘积 mn，它首先包含两个因子 m 和 n 各自的因数，而且还可被 m 的因数与 n 的因数的乘积整除。因此， mn 的所有因数之和等于 $\sigma(m)$ 与 $\sigma(n)$ 的乘积。”由此可见，欧拉使用了以下引理而未加证明：

---

[27]任何更加仔细地研读过《几何原本》的人当然都能立即指出这一点，但显然，同时对《几何原本》和现代代数都十分熟悉的数学家相当少。甚至是 Sur´anyi——他在 [28] 中相当明确地论述了希腊数学——也忽视了欧几里得《几何原本》VII.19与四数定理之间的联系。[28]两个或更多两两互素的数之积不可能是平方数、立方数或任何其他幂，除非各个因子本身分别是同类的平方数、立方数或其他幂。[29]这个引理的证明很简单，而且欧几里得早已将其传承下来，因此在此处再予以阐述便是多余的。

引理17。设 m 和 n 互素。那么 mn 的每个因数 a 都可唯一地写成 $a = rs$ 的形式，其中 $r \mid m$ 和 $s \mid n$。

如今，我们可以毫不犹豫地由算术基本定理推出这个引理；而欧拉大概会援引欧几里得： r 和 s 的存在性如下得出： $a \mid mn$ 对某个 $b \in \mathbb{N}$意味着 $ab = mn$ ；欧几里得《几何原本》VII.19推出存在 r、 s、 t、 $u \in \mathbb{N}$，满足 $a = rs$、$b = tu$、 $m = rt$ 和 $n = su$，于是结论成立。唯一性同样显然：若$a = rs = r's'$满足 r、 $r' \mid m$ 和 s、 $s' \mid n$，那么 $r \mid r's'$，且最大公因子(r、 s') $\mid$最大公因子(m、 n) $= 1$，因此根据命题14有 $r \mid r'$。类似地， $r' \mid r$，所以 $r = r'$ 和 $s = s'$。

11. The gap

正如我们所见，欧几里得《几何原本》VII.19的有效性保证了 $\mathbb{N}$中不可约元素分解的唯一性。VII.19不再成立的一个简单结构，是由所有模4为 $\equiv 1$ 的自然数 $M = \{1, 5, 9, 13, \ldots\}$ 构成的幺半群（希尔伯特在他的讲座中使用了所有模5为 $\equiv 1$的自然数 [18], 构成的幺半群，以此说明引入理想的动机）。在 M 中，我们显然有 $21 \cdot 21 = 9 \cdot 49$（这个等式也立即表明，命题16的对应结论在 M中不成立），但$49 : 21 \neq 21 : 9$；因为(2)将推出存在 m、 n、 x、 $y \in M$，满足 $49 = mx$、 $21 = nx = my$ 和 $9 = ny$。由于9在 M中是不可约的，我们必须有 $n = 1$ 或 $y = 1$。在第一种情况下， $y = 9$，因此 $9 \mid my = 21$；在第二种情况下$n = 9$，同样有 $9 \mid nx = 21$；二者都不可能。

另一方面，很容易证明 $a : b = af : bf$ 对$a, b, f \in M$始终成立。因此

$$49 : 21 = 49 \cdot 9 : 21 \cdot 9 = 21 \cdot 21 : 21 \cdot 9 = 21 : 9,$$

这里我们两次应用了观察 $a : b = af : bf$。但是，正如我们已经看到的，等式 $49 : 21 = 21 : 9$ 是错误的。我们究竟错在哪里？等式 $49 : 21 = 21 \cdot 21 : 21 \cdot 9$ 以及 $21 \cdot 21 : 21 \cdot 9 = 21 : 9$，正如也可以直接轻易验证的那样，无疑是正确的。上述论证中的错误在于假设比例相等[30] 具有传递性：由 $a : b = c : d$ 和$c : d = e : f$ 一般并不能推出 $a : b = e : f$。

Taisbak 在 [29]发现，欧几里得在其第七卷第19命题的证明中恰恰留下了这一缺口：他使用了等号的传递性，却没有证明它。如何弥补这一缺口，可以在 Taisbak [29] 以及 Pengelley 与 Richman [22]中找到。这个简单的论证基于如下事实：四数定理中的某些数可以或多或少地“规范地”选为最大公因数：

引理18。设 $a : b = c : d$。那么存在 $p, q, r, s \in \mathbb{N}$，使得 $a = pr$, $b = qr$,$c = ps$ 且 $d = qs$；其中我们可以取 $r =$ 最大公因子(a, b) 和 $s =$ 最大公因子(c, d)。

证明。由 $a : b = c : d$，可知存在数 $m, n, x, y \in \mathbb{N}$ 满足（2）。因此 $x \mid$最大公因子(a, b) 和 $y \mid$最大公因子(c, d)，故存在 $i, j \in \mathbb{N}$，使得最大公因子(a, b) $= ix$

[30]人们或许会想把这归因于等号的传递性是欧几里得的一条公理（“等于同一事物的事物也彼此相等”）；然而，我们所说的比例相等并非欧几里得意义上的等式：欧几里得并未定义两个比例 $a : b$ 与 $c : d$ 相等，而是说，如果存在如式（2）所示的数，那么这四个数就成比例。正因如此，许多欧几里得注释者不写作 $a : b = c : d$，而更准确地写作 $a : b :: c : d$。

以及最大公因子$(c,d) = jy$。由 $ix \mid a = mx$ 和 $ix \mid b = nx$ 可得 $i \mid m$ 和 $i \mid n$，即 $m = pi$ 和 $n = qi$，其中 $p, q \in \mathbb{N}$。特别地， $a = pix = p \cdot$ 最大公因子 (a, b) 和 $b = q \cdot$ 最大公因子 (a, b)。

现在我们断言 $i \mid j$。由对称性（交换 (a, b, x) 和 (c, d, y) 时情形保持对称），我们也有 $j \mid i$，因此 $i = j$。但这样一来，便如所需得到 $c = my = piy = pjy = p \cdot \gcd(c, d)$ 和 $d = ny = qiy = qjy = q \cdot \gcd(c, d)$。

剩下要证明 $i \mid j$。由 $m = pi$ 和 $n = qi$，我们得到 $iy \mid my = c$ 和 $iy \mid ny = d$。因此 $iy \mid \gcd(c, d) = jy$，于是得到所声称的 $i \mid j$。□

由此我们可以如下证明等号的传递性：设 $a : b = c : d$ 和 $c : d = e : f$。根据引理18，存在 $p, q \in \mathbb{N}$，使得 $a = p \cdot \gcd(a, b)$,$b = q \cdot \gcd(a, b)$，$c = p \cdot \gcd(c, d)$ 和 $d = q \cdot \gcd(c, d)$。再次应用该引理，可得 $p', q' \in \mathbb{N}$，使得 $c = p' \cdot \gcd(c, d)$，$d = q' \cdot \gcd(c, d)$，$e = p' \cdot \gcd(e, f)$ 和 $f = q' \cdot \gcd(e, f)$。约去后得到 $p = p'$ 和 $q = q'$，于是显然有$a : b = e : f$。

请注意，引理18在上面的幺半群 M 中并不成立，因为在 M 中，两个数未必有最大公因子。例如，在 M 中， $3^2 \cdot 7 \cdot 11$和 $3^2 \cdot 7 \cdot 19$ 的公因子是 1, 3^2 和 $3 \cdot 7$，但按照整除关系，并不存在最大公因数，也就是说，不存在一个能被所有公因子整除的公因子。

12. Euclid or Pythagoras?

许多数学史学家认为，欧几里得的数论研究方法源自毕达哥拉斯学派。据推测，他们是通过音乐得出这些比例的：他们观察到，当相应的音调听起来和谐时，振动的弦的长度彼此成简单的比。因此，比$1 : 2$和$2 : 3$分别对应八度和五度。

最初的观察之一必定是，某些比例可以化简：毕竟，$2 : 4 = 1 : 2$。最终，这一探究路线必然会得出这样的结论：比例可以唯一地约简：如果 m和 n是最简的，且 $a : b = m : n$，那么 $m \mid a$ 和 $n \mid b$；更确切地说，存在一个 $x \in \mathbb{N}$，使得$a = mx$ 且 $b = nx$。但这正是欧几里得《几何原本》VII.20命题的内容。之后，VII.22表明，最简的 m 和 n 互素。

一旦通过经验发现了第七卷第20命题，并且若 $a : b = c : d$，便可得出 $a = mx$ 和 $b = nx$；另一方面，也可得出 $c = my$ 和$d = ny$。但这恰恰就是欧几里得对数的比例关系的定义，因此它是从对比例最基本性质的研究中自然而然得出的。

据范德瓦尔登 [31], 所述，毕达哥拉斯学派以这一四数定理为其数论的基础，后来欧几里得也照搬了这一理论及其结构，基本未作改动。与他前后的其他评论家一样，范德瓦尔登认为欧几里得对数的比例关系所下的定义是一个失误[31]，而非天才之举。然而，上述考量以及例如引理17的证明表明，这一定义一方面相当

[31]D.福勒，例如，在 [12]:
Commentators rarely point out the unsatisfactory nature of this definition: it is a vivid though incomplete description of four numbers in proportion and , , , 中写道 not the mathematical criterion needed for the foundation of a theory.

自然，另一方面，四数定理也完全适用于证明丢番图分析中的基本结果。

除了范德瓦尔登为论证欧几里得《第七卷》源自毕达哥拉斯学派而提出的理由之外，数的比例的等号传递性缺少证明这一点，也可以视为支持该论断的证据：如果以欧多克索斯给出的比例相等定义为理论基础，那么等号传递性的证明几乎不费吹灰之力。然而，欧几里得仍在 V.11 中证明了这一点。这或许是因为量的比例理论源自欧多克索斯，而在他所处的时代，数学家们已经普遍认识到，这类步骤必须加以证明。在我看来，毕达哥拉斯学派完全可能只是忽略了这样一个事实：数的比例的等号传递性绝非显而易见。欧几里得也未能意识到这一点，尽管他当然知道 V.11，这更令人惊讶；不过，这或许可以解释为，他将毕达哥拉斯学派的数论原封不动地收入了《第七卷》。

13. The four number theorem

为阐明欧几里得四数定理的意义，我们将该定理成立的整环称为里斯域[32]。因此，在里斯域中，R $ad = bc$ 对于 a，b，c，$d \in R$ 意味着存在 m，n，x，$y \in R$ 使得$a = mx$、$b = nx$、$c = my$ 且 $d = ny$。

若元素 $a \in R$ 满足以下条件，则称其为原元[33]：对于任意 b，$c \in R$，若 $a \mid bc$，则存在 r，$s \in R$ 使得 $a = rs$、$r \mid b$ 且 $s \mid c$。注意，0和单位元总是原元。

显然，一个整环是里斯域，当且仅当 R中的每个元素都是原元。下面的命题表明，在里斯域中，所有不可约元素都是素元：

命题 19. 不可约元素是原元，当且仅当它们是素元。

证明。设 a 是素元，且 $a \mid cd$；那么不妨设 $a \mid c$。由 $r = a$和 $s = 1$，我们得到 $a = rs$、$r \mid c$ 和 $s \mid d$，即 a 是原元。

现在设 a 是不可约且为原元的。若 $a \mid cd$，则存在 r，s，使得 $a = rs$、$r \mid c$ 且 $s \mid d$。由于 a 不可约，r 或 s ——不妨设为 r ——必为单位元。但由 $s \mid d$ 可知 $a \mid d$，因此 a 是素元。□

在命题 VII.19 中，欧几里得实质上证明了 $\mathbb{Z}$ 是里斯域；他证明 $\mathbb{N}$ 中的不可约元素是素元的方法，实质上就是上述证明的一半。

仔细考察欧几里得对 VII.19 的证明（或 Taisbak 对该证明的补充）便可看出，四数定理适用于所有最大公因数整环（即任意两个元素都有最大公因数的整环），也就是说，每个最大公因数整环都是里斯域。

此时应当指出，一方面，primal元素与另一方面的不可约元素或素元在性质上截然不同：多个不可约元素（或素元）的乘积不再是不可约元素（或素元），除非是只有一个因子的平凡情形。而对于primal元素，我们有：

---

[32]Zafrullah [32]将这些环称为 pre-Schreier 环；不过下文将会看到，里斯域的整除群在群论意义上是“里斯群”。[33]这一概念归功于 Cohn [7]。

引理20。 *primal*元素的乘积是*primal*元素。

证明。令 a，$b \in R$ 为primal元素；若 $a = 0$ 或 $b = 0$，则 $ab = 0$ 为primal元素，因此不妨设 a，$b \neq 0$。令 $ab \mid c_1c_2$，即 $c_1c_2 = abd$。由于 a 为primal元素，存在分解 $a = a_1a_2$，其中 $a_i \mid c_i$。写作 $c_i = a_id_i$，得到 $abd = c_1c_2 = a_1a_2d_1d_2 = ad_1d_2$，从而 $bd = d_1d_2$。由于 b 为primal元素，我们有 $b = b_1b_2$，其中 $b_i \mid d_i$。

因此 $ab = a_1b_1a_2b_2$ 当 $a_ib_i \mid a_id_i = c_i$时，从而 ab是primal元素。由归纳法可知，任意primal元素的乘积都是primal元素。□

现在我们证明命题16的以下推广：

命题21。 设 R 是一个里斯域。若对于 a、b、$c \in R$ 有 $ab = c^2$，且 a 和b 互素，则存在一个单位元 $e \in R^\times$，使得 ae 和 be 是 R中的平方元。

备注。 尽管只有在最大公因子整环中，任意两个环元素的最大公因数这一概念才有意义，但在任意整环中都可以谈论“互素”元素：根据定义，这类元素的所有公因子都是单位元。例如，2和3在 $R = \mathbb{Z}[\sqrt{-5}]$中互素，而6和 $2 + 2\sqrt{-5}$在 R中没有最大公因子。—

命题*21*的证明。 根据四数定理，存在 m、n、x、$y \in R$，使得$a = mx$、$b = ny$ 和 $c = my = nx$。对等式 $my = nx$ 应用四数定理，我们得到存在 r、s、t、$u \in R$，使得 $m = rs$、$y = tu$、$n = rt$ 和 $x = su$。由于 a 和 b 互素，因此 m 和 n也互素，x 和 y同样互素；由此 r 和 u是 R中的单位元。令 $e = 1/ru$，于是有$ae = mxe = rs^2ue = s^2$ 和 $be = nye = rt^2ue = t^2$。□

尽管欧拉未经证明而使用的某些事实可以由欧几里得四数定理加以论证，但里斯域仅仅是“几乎”唯一分解的。若考察两个分解 $a_1 \cdots a_m = b_1 \cdots b_n$，那么在里斯域中只能推出这两个分解具有一个公共细化：存在元素 $c_{ij} \in R$（$1 \le i \le m$、$1 \le j \le n$），使得 $a_i = c_{i1} \cdots c_{in}$和 $b_j = c_{1j} \cdots c_{mj}$。对于 $m = n = 2$，这就是四数定理；一般情形（由四数定理通过归纳法推出）称为“施赖尔细化性质”。例如，全体代数整数构成的环具有这一细化性质，但它不是唯一分解的，因为其中没有不可约元素。

每个非零元素都可以写成一个单位元与不可约元素之积的整环称为原子整环。因此我们有如下

定理 22。 整环 R 是唯一分解的，当且仅当 R 是一个原子 *Riesz* 域。

证明。 在 Riesz 域中，根据命题 19，不可约元素是素元；众所周知，这意味着不可约元素的分解是唯一的。反过来，若 R 是唯一分解的，则 R 是一个最大公因子整环，因而是一个 Riesz 域；其次，每个元素 $\neq 0$ 都有一个由不可约元素（甚至是素元）组成的分解。□

由于命题 19，这一陈述比一个著名定理稍弱。该定理指出，整环是唯一分解的，当且仅当它们是原子的，且每个不可约元都是素元。

欧几里得构建数论的方式可以概括如下：

$$\text{Euclid} \longrightarrow \text{GCD} \longrightarrow \text{Riesz} \longrightarrow \text{AP},$$

其中，AP 表示欧几里得引理成立，也就是说，不可约元素（原子元）都是素元。更一般地，可以证明以下包含关系：

$$\begin{array}{ccccccccc} \text{Euclid} & \subset & \begin{array}{c}\text{PID}\\ \cap \\ \text{UFD}\\ \cap \\ \text{atomic}\end{array} & \subset & \begin{array}{c}\text{Bezout}\\ \cap \\ \text{GCD}\end{array} & \subset & \text{Riesz} & \subset & \text{AP} \end{array}$$

这里，Euclid 表示欧几里得整环，PID 表示主理想整环，UFD 表示唯一分解整环（即每个元素都能唯一分解为素元），而 AP整环则是所有原子元（即所有不可约元素）都是素元的整环。贝祖整环是指任意两个元素 a，b 都有最大公因子，且该最大公因子可写成 a 和 b的 R线性组合的整环；等价地说，两个主理想之和仍是主理想。

希尔伯特为欧几里得几何奠定了现代公理化基础，但据我所知，对欧几里得数论的相应研究迄今尚未开展。例如，可以问：在哪些环中，以下命题成立：若 a 和 b 互素（即每个公因子都是单位元），且 $a \mid bc$，则 $a \mid c$。命题14证明的第一部分表明，这在里斯域中成立；然而，证明的第二部分用到了最大公因子的存在，因此我们不能据此断定这类环也是里斯域。另一方面，具有这一性质的环是原子为素元的环。一般而言，可以问：欧几里得数论中的命题在哪些整环中成立，也就是说，证明这些命题需要哪些公理。

14. Riesz groups

本节将讨论四数定理的一些推广。为此，我们将较为一般地研究里斯群。

设 R 是一个整环，其分式域为 K。回顾一下，对于 a，$a \mid c$ 意味着存在一个 $b \in R$，使得 $ab = c$。研究整除性质时，单位元无关紧要；因此，与其考察 $K^\times$，不如考虑商群 $G(R) = K^\times/R^\times$，我们也可以将其看作非零分式主理想构成的群；暂且将 $G(R)$ 的元素记为 $aR^\times = (a)$。群 $G(R)$ 关于关系 $(a) \leq (b)$ 偏序，当且仅当 $a \mid b$，也就是说，当 $\frac{b}{a} \in R$ 时。此外，对于任意 $(c) \in G(R)$，$(a) \leq (b)$ 等价于 $(ac) \leq (bc)$。因此，所有“正”元素构成的集合 $G(R)^+ = \{(g) \in G(R) : (g) \geq (1)\}$，由所有非零整主理想组成，显然是一个幺半群；它是由 $R^* = R \setminus \{0\}$ 经由取理想得到的，也就是说，将相伴元素视为相同元素。

现在我们要将欧几里得四数定理关于 R 的表述转化为这种语言。若 $ad = bc$，则 $a \mid bc$，因此对于$G(R)$中相应的主理想，有$(a) \leq (b)(c)$。根据四数定理，存在 r，s，t，$u \in R$，使得 $a = rs$、$b = ru$、$c = ts$ 且 $d = tu$。因此 $r \mid b$ 且 $s \mid c$，从而$(r) \leq (b)$，并且$(s) \leq (c)$。所以我们有

命题23。设 R 是一个整环。那么， R 中四数定理成立，当且仅当 $G(R)$ 具有如下*"Fuchs*插值性质"F_2[34]：若 a、b、$c \in G(R)^+$ 且 $a \le bc$，则存在一个分解 $a = rs$，其中r、$s \in G(R)^+$，使得 $r \le b$ 且 $s \le c$。

现在我们将定义偏序阿贝尔群的一系列一般插值性质和细化性质 G:

- "Fuchs插值性质" F_n：若 $a, b_1, \dots, b_n \in G^+$和 $a \le b_1 \cdots b_n$，则存在 $a_i \in G^+$，使得 $a = a_1 \cdots a_n$且 $a_i \le b_i$对$1 \le i \le n$成立。
- "Riesz插值性质"$R_{m,n}$：若给定 $a_1, \dots, a_m, b_1, \dots, b_n \in G$，且对所有 $1 \le i \le m$ 和 $1 \le j \le n$均有 $a_i \le b_j$，则存在一个 $c \in G$，使得对所有 i 和 j均有 $a_i \le c \le b_j$。
- "施赖尔细化性质"$S_{m,n}$：若给定 $a_1, \dots, a_m, b_1, \dots, b_n \in G^+$，且满足 $a_1 \cdots a_m = b_1 \cdots b_n$，则存在元素 $c_{ij} \in G^+(1 \le i \le m, 1 \le j \le n)$，使得 $a_i = c_{i1} \cdots c_{in}$和 $b_j = c_{1j} \cdots c_{mj}$。
- "Euclidean细化性质"E_m：若 a，b_i，$c_j \in G^+$且 $a \le b_i c_j$对 $i = 1$，....., m以及 $j = 1$, ..., n均成立，则存在一个分解 $a = rs$，使得r，$s \in G^+$、$r \le b_i$，并且对所有 $1 \le i \le m$ 和 $1 \le j \le n$均有 $s \le c_j$。

性质$R_{2,0}$和$R_{0,2}$可以作如下解释：对 a_1，$a_2 \in G$，存在一个 $c \in G$，使得 $a_1 \le c$ 且 $a_2 \le c$（这就是$R_{2,0}$）；还存在一个 $b \in G$，使得 $b \le a_1$ 且 $b \le a_2$（这就是$R_{0,2}$）；具有这一性质的偏序群称为有向[35]。整环的整除群 $G(R)$自动具有有向性：对于a_1，$a_2 \in K^\times$，显然总存在一个 $c \in K^\times$，使得 $a_1 \mid c$、$a_2 \mid c$（任选 a_1 和 a_2 的分子，将它们的乘积取作 c 即可）。同样，总能找到一个 $b \in K^\times$，使得 $b \mid a_1$ 且 $b \mid a_2$。

我们现在断言

命题 24。对于偏序有向阿贝尔群 G，以下性质等价：

(1) $R_{2,2}$ 在 G中成立；*(2)* $R_{m,n}$ 对所有 m、$n \ge 0$ 在 G 中成立；*(3)* F_2 在 G中成立；*(4)* F_n 对所有 $n \ge 1$ 在 G 中成立；*(5)* $S_{2,2}$ 在 G中成立；*(6)* $S_{m,n}$ 对所有 m、$n \ge 1$ 在 G 中成立；*(7)* E_1，*1* 在 G中成立；*(8)* E_m，n 对所有 m、$n \ge 1$ 在 G 中成立；*(9)* $[1,a] \cdot [1,b] = [1,ab]$ 对所有 a、$b \in G^+$ 在 G 中成立（此处 $[a,b] = \{r \in G : a \le r \le b\}$）。

假设 G 是有向的，唯一需要之处是为了从$R_{2,2}$ 过渡到$R_{m,n}$。所有证明都很初等（本质上是归纳法），这里无需给出。

---

[34]从现在起，我们将 $G(R)$ 的元素简单记为 a，而不再记为(a)。[35]由于 $a \le b$ 等价于 $b^{-1} \le a^{-1}$，因此，只要满足例如$R_{2,0}$，偏序群就已经是有向的。

沿用 L. Fuchs 的说法，具有定理 24 所列性质的 [13], 偏序阿贝尔群称为里斯群[36]。F. Riesz[25] 于1940年首次研究了它们，后来 Birkhoff [6] 和 H. Bauer [3] 也进行了研究。在这些论文中，还可以找到定理 24 的部分证明，以及与 1 – 9 等价的其他性质。施赖尔细化性质$S_{m,n}$ 是 Kalm´ar 用来证明算术基本定理的四数定理的推广。在第二部分中，我们最终还将用到 Euclidean细化性质。

Concluding remarks

任何人只要更深入地研究欧几里得数论，很快就会注意到命题 VII.19（四数定理）所起的核心作用。但任何仅仅对高斯之前的数论史感兴趣的人，也必须了解欧几里得的数论著作，尤其是核心结果 VII.19：常有人批评欧拉在某些地方暗中使用了高斯的一项结果，即唯一素因子分解；然而，首先，这种说法以这种形式而言多少有些时代错置；其次，鉴于欧几里得的 VII.19[37]，这种批评恐怕难以成立。这些评论并非意在免除欧拉所有的“过失”：按当今标准来看，他的许多证明都不够严谨，而且并非所有漏洞都能用欧几里得来填补。不过，笼统指责欧拉经常默默地使用唯一素因子分解，或许应当重新考虑。

本文发表于《数学学期报告》**55**(2008), 181–195。英文译文是在 Claude（Anthropic）的帮助下完成的。

Literatur

[1] A.G. Agarg¨un、C.R. Fletcher, *Al-Fārisī and the fundamental theorem of arithmetic*, 《数学史》 **21** 1994 162 173 ( ), – P. Barlow, *An elementary investigation of the theory of numbers,*

[2] *with its application to theindeterminate and Diophantine analysis, the analytical and geometrical division of the circle, and several other curious algebraical and arithmetical problems*, 伦敦, J. Johnson and Co, 1811 ¨ http://dlxs2.library.cornell.edu/m/math/；可在线访问：H. Bauer, , 《巴伐利亚科

[3] *Geordnete Gruppen mit Zerlegungseigenschaft* 学院会议报告》1958, 25 36 1959– ( )

[4] *Polynomial diophantine systems* **35** 1933 903 914 E.T. Bell, , 《美国数学会汇

[5] *Reciprocal arrays and diophantine analysis* **55** 1933 50 刊》( ), – E.T. Bell, , 《美国数学杂志》( ), – 66

[6] *Lattice-ordered groups* **43** 1942 298 G. Birkhoff, , 《数学年刊》 331 ( ), –[7] *Bezout rings and their subrings* P.M. Cohn, , 《剑桥哲学学会会刊》

64 1968 251 264 ( ), – M.J. Collison, ,

[8] *The unique factorization theorem: from Euclid to Gauss* **53** 《数学杂志》(1980 96 100), – P. Erdos, J. Sur´anyi, *Topics in the theory of numbers*, Barry Guiduli 从匈牙利语

[9] 翻译，纽约，施普林格， ″ 2003 ¨ 1960 。原始出版物：L.

[10] *Theorematum quorundam arithmeticorum demonstrationes* Euler, , 《彼得堡科学院通讯》**10** (1738), 1747, 第125–146页。《全集》I.2, 第38–58页；可在线访问：EulerArchive.org。

[11] L. Euler, *De numeris amicabilibus*, 《各种论题小品》**2** (1750), 23–107；《全集》I-2, 86 162 **1** 1849 102 145 –；《算术评论》( ), – D. Fowler, , 《美国数学会通报》(新系列)

[12] *Ratio in early Greek mathematics* **1** 1979 807 846 ( ), – L. Fuchs, , 《比

[13] *Riesz groups* **19** 1965 1 34 萨高等师范学校年刊》, III辑。( ), –

[36]严格来说，里斯群并不要求交换性；在这种情况下，定理 24 的所有性质不再等价。[37]其他作者（甚至在高斯之后）也使用过四数定理，而未提及欧拉或欧几里得：参见 Barlow [2, 第 401], Kramer [20],或 P´epin [23, 第 24], [24,第 413]。

[14] C.F. Gauß, *Disquisitiones Arithmeticae*, G. Fleischer, 莱比锡1801；由H. Maser作德语¨译本（1889）[15] C. Goldstein, *On a seventeenth century version of the "fundamental theorem of arithmetic"*, 《数学史》 **19** 1992 177 187 ( ), – Th. L. Heath（编）, *The thirteen books of Euclid's Elements*, 根据 [16] Heiberg文本翻译，附导论和评注。剑桥大学出版社1908；第2版，剑桥 1926 1956 ；重印本, [17] Dover M.D. Hendy, *Euclid and the fundamental theorem of arithmetic*, 《数学史》**2** (1975), 189–191[18] D. Hilbert, *Zahlentheorie*, 讲座1897–1898（E. Maus编），哥廷根大学¨1990[19] L. Kalm´ar, *Über den Fundamentalsatz der Zahlentheorie* （匈牙利语；德语摘要）, 《数学与物理学报》 **43** 1936 27 45 ( ), – A.E. Kramer, [20] *De quibusdam aequationibus indeterminatis quarti gradus* 1839 , 论文。F. [21] *Unique Factorization. The Fundamental Theorem of Arithmetic* Lemmermeyer, , 即将出版的书。[22] D. Pengelley, F. Richman, *Did Euclid need the Euclidean algorithm to prove unique factorization?* **113** 2006 196 , 《美国数学月刊》( ), – 205 [23] ´ *Sur un théorème de Legendre* Th. Pepin, , 《纯粹与应用数学杂志》(3 **5** 1879 21 31)( ), – Th. Pepin, , 《纯 [24] ´ *Sur l'équation* $7x^4 - 5y^4 = 2z^2$ 3 **5** 1879 405 粹与应用数学杂志》( ) ( ), – 425 [25] F. Riesz, *Sur quelques notions fondamentales dans la théorie générale des opérations linéaires* **41** 1940 174 , 《数学年刊》( ), – 206 [26] E. Rosenthall, *On some cubic diophantine equations* **65** 1943 663 672 , 《美国数学杂志》 [27] ´ *On the proofs of the fundamental theorem of number theory* ( ), – J. Suranyi, 《数学分析及相关主题研究》, 第 388 391, 1962 –页，斯坦福大学 [28] ´ *Schon die alten Griechen haben das gewusst Große Augenblicke aus der* 出版社，斯坦福，加利福尼亚州。J. Suranyi, 见*Geschichte der Mathematik*，BI 曼海姆1991[29] C.M. Taisbak, *Division and Logos. A theory of equivalent couples and sets of integers*, 《自然科学与医学史学报》**25** (1971)。欧登塞大学出版社，欧登塞1971[30] C. Thaer（编）, *Euklid "Die Elemente"*。依据Heiberg文本从希腊语¨翻译并由Clemens Thaer编校；达姆施塔特，科学图书协会出版社 1980 [31] *Die Arithmetik der Pythagoreer I. II.* B.L. van der Waerden, , 《数学年刊》**120** (1947/49), 127–153；同上，676–700 [32] *On a property of pre-Schreier domains* **15** 1987 1895 1920 M. Zafrullah, [33] *Elementare Betrachtungen zur Theorie der Primzahlen* ¨ 2 **1** 《代数通讯》( ), – E. Zermelo, 《哥廷根科学院公报》( ) (1934), 43–46