arXiv:2303.05949v1 [math.HO] 10 Mar 2023

2023年3月10日

Terquem遗忘的问题

Robert G. Donnelly，[1] Molly W. Dunkum，[2]和 Rachel McCoy[3]

摘要

“Terquem问题”是二十世纪出现的一个名称，指的是对某些奇偶性交替的整数序列进行计数的问题。具体而言，该问题要求计算长度为 m 的严格递增正整数序列的数量，其中各项均不超过某个整数 n，且奇数位上的项为奇数，偶数位上的项为偶数。这个问题及其推广已得到深入研究。然而，该问题所谓的原始出处——Olry Terquem 于 1839年 发表的一篇论文——与如今归于 Terquem 名下的问题存在细微差异。本文着重指出这一区别，并探讨 Terquem 的“遗忘”问题与斐波那契数列、连分式分子、B´ézout 引理以及扩展欧几里得算法之间的联系。

数学主题分类：11A04, 11B39 关键词：Terquem问题、斐波那契数组、连分式分子多项式、B´ézout 引理、扩展欧几里得算法

§0. 引言。Olry Terquem 是十九世纪的博学家——他既是数学家、历史学家、期刊创办人和编辑、宗教改革者，也是法国荣誉军团勋章的获得者。他以在几何学方面的数学贡献而闻名；而在组合数学领域，他的名字则与一个称为“Terquem问题”的计数问题相关。如今对 Terquem问题的表述通常沿用 John Riordan 所著的经典组合数学入门教材；他似乎是从德国数学家 Eugen Netto 于二十世纪初编写的一本组合数学教材中借鉴了这个问题（见 [10]第3章§49）。以下是 Riordan 的版本（[13], 第1章问题15），其中对记号略作修改，以便更适合我们的语境：

> Terquem问题。对于由 n 个编号对象按自然（递增）顺序组成的组合，设 $\mathsf{t}(n,m)$表示满足以下条件的 m-组合的数量：奇数元素处于奇数位置，偶数元素处于偶数位置；或者等价地，设 $\mathsf{t}(n,m)$ 表示组合中奇数元素和偶数元素数量相等（当 m 为偶数时），而奇数元素比偶数元素多一个（当 m 为奇数时）的组合数量。证明 $\mathsf{t}(n,m)$ 满足递推关系 $\mathsf{t}(n,m) = \mathsf{t}(n-1,m-1)+\mathsf{t}(n-2,m)$[，其中] $\mathsf{t}(n,0) = 1$, [，且] $\mathsf{t}(n,m) = \binom{\lfloor \frac{n+m}{2} \rfloor}{m}$, [，以及] $f_{n+1} = \sum_{m=0}^{n} \mathsf{t}(n,m) = f_n + f_{n-1}$。

在 OEIS 条目 [12] 中，这一版本的 Terquem问题所要计数的对象称为“交替奇偶子集”。（例如，当 $n = 4$ 时，我们得到 $\mathsf{t}(4,0) = 1$、$\mathsf{t}(4,1) = 2$、$\mathsf{t}(4,2) = 3$、$\mathsf{t}(4,3) = 1$ 和 $\mathsf{t}(4,4) = 1$，从而得到斐波那契

[1]默里州立大学数学与统计学系，肯塔基州默里 42071 电子邮箱：rob.donnelly@murraystate.edu[2]西肯塔基大学数学系，肯塔基州鲍灵格林 42101 电子邮箱：molly.dunkum@wku.edu[3]西肯塔基大学数学系，肯塔基州鲍灵格林 42101 电子邮箱：mccoy.800@osu.edu

数 8 的划分。）这类交替奇偶子集已得到深入研究和推广；近期的一个例子可参见 Toufik Mansour 和 Augustine O. Munagi 的论文 [9] 及其中的参考文献。

然而，上述版本的 Terquem问题省略了他在1839年的论文中提出的一项要求 [15].[4] 这项要求是关于他所考察的交替奇偶子集长度的奇偶性条件。Terquem 原始问题中这一颇为微妙却已被遗忘的差异，实际上使该问题与一些非常经典的组合计数和数论现象密切相关，即一个右三角形的斐波那契型数组、连分式分子多项式、B´ézout 引理以及欧几里得扩展算法。本文的主要目标是重新审视 Terquem 的原始问题，并展示这些联系。

§1. 斐波那契型数组。众所周知，帕斯卡三角形某些对角线上的数之和构成的数列恰好就是斐波那契数列 $f_0 = 1$, $f_1 = 1$, $f_2 = 2$, $f_3 = 3$, $f_4 = 5$, 等等。[5]事实上，我们可以像下图所示那样将帕斯卡三角形倾斜，从而把斐波那契对角线看作图1.1所示右三角形数组中的各行。

1
1
1 1
1 2
1 3 1
1 4 3
1 5 6 1
1 6 10 4
1 7 15 10 1
1 8 21 20 5
1 9 28 35 15 1
1 10 36 56 35 6
1 11 45 84 70 21 1
1 12 55 120 126 56 7
1 13 66 165 210 126 28 1
1 14 78 220 330 252 84 8
1 15 91 286 495 462 210 36 1
1 16 105 364 715 792 462 120 9
ETC.

图1.1

我们称其为斐波那契直角三角数组，或简称斐波那契数组。我们用记号 $\boldsymbol{F}$ 表示这个三角数组，并将第 n^{th} 行的 k^{th} 项记为 $f_{n,k}$，于是

$$\boldsymbol{F} = (f_{n,k})_{n\in\{0,1,2,\ldots\},k\in\{0,1,\ldots,\lfloor\frac{n}{2}\rfloor\}}.$$

[4]在研究这一主题期间，排名第三的作者热心地翻译了Terquem于1839年发表的论文 [15] （原文为法语），以及Netto在1901年的著作中对Terquem问题的表述 [10] （原文为德语）。[5]这一观察被归功于爱德华·卢卡斯，参见Thomas Koshy的著作 [7]。

形式上，我们通过定义 $f_{0,0} := f_{1,0} := 1$ 来构造 $\boldsymbol{F}$，然后应用递推关系

$$f_{n,k} := f_{n-1,k} + f_{n-2,k-1}$$

对于整数 k和 n，其中 $n \geqslant 2$，并约定 $f_{n,\,k} := 0$当 $k < 0$或$k > \lfloor \frac{n}{2} \rfloor$时。根据这个定义递推关系，可以很容易验证，对于任意满足 $0 \leqslant k \leqslant \lfloor \frac{n}{2} \rfloor$的整数 n和 k，有

$$f_{n,k} = \binom{n-k}{k} \qquad \text{and} \qquad \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} f_{n,i} = f_n.$$

因此，$\boldsymbol{F}$ 的第 n^{th} 行中的项序列可以看作是 n^{th}斐波那契数的细化。事实上，有些多项式族，例如卢卡斯[6] （见[8]）和恩斯特·雅各布斯塔尔（见 [7] 第 39 章）研究的多项式，其系数取自$\boldsymbol{F}$的各行。这些细化所包含的数也有许多计数解释。接下来，我们将介绍两种这样的解释——一种广为人知，另一种由 Olry Terquem 提出，似乎已被遗忘。

解释 1.1：斐波那契数组的一种经典计数解释。固定一个正整数 n和一个非负整数 m。由 n 严格界定的无连续项序列 $S = (S_1, S_2, \ldots, S_m)$，是由 m 个正整数组成的严格递增序列，其中 $S_m < n$ 且对任意 $i \in \{1, 2, \ldots, m-1\}$，都有$S_{i+1} - S_i \geqslant 2$。我们称 S的长度为 m。当 $m = 0$ 时， S是空序列，记作 ()，其长度视为零，并且也视为无连续项序列。令 $\mathcal{CF}(n)$ 为由n严格界定的无连续项序列集合。例如，

$$\begin{aligned} \mathcal{CF}(5) &= \{(), (1), (2), (3), (4), (13), (14), (24)\} \\ \mathcal{CF}(6) &= \{(), (1), (2), (3), (4), (5), (13), (14), (15), (24), (25), (35), (135)\} \end{aligned}$$

此外，设 $\mathcal{CF}(n,k)$表示 $\mathcal{CF}(n)$中长度为 k的序列集合，其中 k是非负整数。根据在线整数数列百科全书条目 A011973 [11],，我们有 $|\mathcal{CF}(n,k)| = f_{n,\,k}$，对所有正整数$n$以及满足 $0 \leqslant k \leqslant \lfloor \frac{n}{2} \rfloor$的所有整数 k均成立。特别地， $|\mathcal{CF}(n)| = f_n$是第 n^{th}个斐波那契数。 □

解释 1.2：Olry Terquem 遗忘的问题。再次假设 n 是一个正整数，且 m 是一个非负整数。由 n 界定的奇偶交替序列 $T := (T_1, T_2, \ldots, T_m)$ 是一个由 m 个正整数组成的严格递增序列，其中 m 和 n 具有相同的奇偶性， T_1 为奇数， $T_m \leqslant n$，并且对于任意 $i \in \{1, 2, \ldots, m-1\}$， T_i 和 T_{i+1} 具有相反的奇偶性。（在此定义中，前缀“oe”意在表示奇偶交替序列的奇偶交替模式。）我们称 T 的长度为 m，并记作 $\ell(T) = m$。当 $m = 0$ 时， T 是空序列，记作 ()，其长度视为零，且视为一个奇偶交替序列。令 $\mathcal{OE}(n)$ 为由 n 界定的奇偶交替序列集合。出于稍后将显而易见的原因，我们设 $\mathcal{OE}(-1) := \varnothing$

[6]在 [8], 第 186 页，量 U_n （其中 n 是正整数）是关于整数变量 P和 Q的多项式，其系数符号交替，来自 $\boldsymbol{F}$ 的第 $n-1$ 行。

并且 $\mathcal{OE}(0) := \{()\}$。例如，

$$\begin{aligned}\mathcal{OE}(5) &= \{(1),(3),(5),(123),(125),(145),(345),(12345)\}\\ \mathcal{OE}(6) &= \{(),(12),(14),(16),(34),(36),(56),(1234),(1236),(1256),(1456),(3456),(123456)\}\end{aligned}$$

进一步，对于 $0 \leqslant k \leqslant \lfloor \frac{n}{2} \rfloor$，令 $\mathcal{OE}(n,k)$ 为 $\mathcal{OE}(n)$ 中满足 $\ell(T) = n - 2k$ 的序列集合 T。Terquem遗忘的问题是证明 $|\mathcal{OE}(n,k)| = f_{n,\ k}$。在下文的命题 1.3 中，我们通过证明 $\mathcal{CF}(n,k)$ 与 $\mathcal{OE}(n,k)$ 之间存在双射来解决这个问题。

同样，偶奇序列具有奇偶交替序列的所有性质，不同之处在于它以偶数而非奇数开头，且其长度的奇偶性与 n 相反；于是我们将 $\mathcal{EO}(n)$ 定义为以 n 为界的偶奇序列集合。这次我们设 $\mathcal{EO}(-1) := \{()\}$，且 $\mathcal{EO}(0) := \varnothing$。例如，

$$\begin{aligned}\mathcal{EO}(5) &= \{(),(23),(25),(45),(2345)\}\\ \mathcal{EO}(6) &= \{(2),(4),(6),(234),(236),(256),(456),(23456)\}\end{aligned}$$

从这里开始，我们统称奇偶交替序列和偶奇序列为 oereo 序列（读作“OH-ree-oh”）。对于 $0 \leqslant k \leqslant \lfloor \frac{n-1}{2} \rfloor$，令 $\mathcal{EO}(n,k)$ 为满足 $\ell(T) = (n-1) - 2k$ 的 $T \in \mathcal{EO}(n)$ 集合。在下文的命题 1.3 中，我们证明 $\mathcal{EO}(n,k)$ 与 $\mathcal{OE}(n-1,k)$ 之间存在双射，并由此得出 $|\mathcal{EO}(n,k)| = f_{n-1,\ k}$。

□

为了在命题 1.3 中构建对 Terquem遗忘的问题的解答，我们需要以下思路。当给定序列中的各项互不相同时，我们可以将该序列视为集合，并进行集合运算。因此，当 n 是正整数时，我们注意到，整数的严格递增序列 $(T_1, \ldots, T_m)$，若满足 $1 \leqslant T_1$ 和 $T_m \leqslant n$，则它是奇偶交替序列，当且仅当$\{1, 2, \ldots, n\} \backslash \{T_1, \ldots, T_m\}$ 是由连续整数的偶数长度子序列组成的并集。

对于非负整数 $k \leqslant \lfloor \frac{n}{2} \rfloor$，我们按以下方式定义函数 $\phi\colon \mathcal{CF}(n,k) \longrightarrow \mathcal{OE}(n,k)$。给定 $S = (S_1, \ldots, S_k) \in \mathcal{CF}(n,k)$，令

$$T := \phi(S) := \Big\{1, 2, \ldots, n-1, n\Big\} \setminus \left(\bigcup_{i=1}^{k} \{S_i, S_i + 1\} \right).$$

显然 $\ell(T) = n - 2k$，因此 $\ell(T)$ 与 n具有相同的奇偶性。由于 T是通过从$\{1, 2, \ldots, n\}$ 中删去连续整数对得到的，因此 T 任意两个相邻项之间的数构成一个偶数长度（也可能长度为零）的连续整数串；所以，正如上一段所观察到的，T 是奇偶交替序列。接下来，我们按如下方式定义函数 $\psi : \mathcal{EO}(n,k) \longrightarrow \mathcal{OE}(n-1,k)$。规定 $() \xmapsto{\psi} ()$。否则，当 $T = (T_1, \ldots, T_m)$且满足 $m = \ell(T) > 0$时，令 $\psi(T) := (T_1 - 1, T_2 - 1, \ldots, T_m - 1)$。显然，$\psi(T) \in \mathcal{OE}(n-1,k)$。

命题 1.3 设 n和 k是整数，且 n为正，并且$0 \leqslant k \leqslant \lfloor \frac{n}{2} \rfloor$。那么函数$\phi\colon \mathcal{CF}(n,k) \longrightarrow \mathcal{OE}(n,k)$和 $\psi\colon \mathcal{EO}(n,k) \longrightarrow \mathcal{OE}(n-1,k)$ 都是双射。因此 $|\mathcal{OE}(n,k)| = f_{n,k}$ 和 $|\mathcal{EO}(n,k)| = f_{n-1,k}$。

证明。上文已经指出， ϕ 和 ψ 各自的值域都包含在所声明的目标集合中。由于 ϕ 和 ψ 各自采用的过程显然都是可逆的，因此我们得出这些函数都是双射。其余结论由以下事实推出：$|\mathcal{CF}(n,k)| = f_{n,k}$，参见上文解释 1.1。

□

§2. 连分式分子多项式的组合刻画。现在，我们将某些多元多项式 g_n 和 h_n 定义为某些 oereo 序列集合上的“生成函数”。这些定义基于以下一般概念：对于任意严格递增的正整数序列 $T = (T_1, \ldots, T_m)$，令 $\mathsf{x}_T := x_{T_1} x_{T_2} \cdots x_{T_m}$（其中每个 x_i 都是不定元），空序列对应 $\mathsf{x}_() := 1$。对于任意整数 $n \geqslant -1$，令

$$g_n := \sum_{T \in \mathcal{EO}(n)} \mathsf{x}_T \qquad \text{and} \qquad h_n := \sum_{T \in \mathcal{OE}(n)} \mathsf{x}_T,$$

当然，空和为零。注意， g_n 和 h_n 都是关于 $x_1, \ldots, x_n$ 的多项式，且系数均为 1。称 g_n 为 eo 多项式， h_n 为 oe 多项式；统称为 oereo 多项式。现列出最初的几个 eo 多项式和 oe 多项式：

$$\begin{aligned}
g_{-1} &= 1 \\
g_0 &= 0 \\
g_1 &= 1 \\
g_2 &= x_2 \\
g_3 &= 1 + x_2x_3 \\
g_4 &= x_2 + x_4 + x_2x_3x_4 \\
g_5 &= 1 + x_2x_3 + x_2x_5 + x_4x_5 + x_2x_3x_4x_5
\end{aligned}
\qquad\qquad
\begin{aligned}
h_{-1} &= 0 \\
h_0 &= 1 \\
h_1 &= x_1 \\
h_2 &= 1 + x_1x_2 \\
h_3 &= x_1 + x_3 + x_1x_2x_3 \\
h_4 &= 1 + x_1x_2 + x_1x_4 + x_3x_4 + x_1x_2x_3x_4 \\
h_5 &= x_1 + x_3 + x_5 + x_1x_2x_3 + x_1x_2x_5 \\
&\quad + x_1x_4x_5 + x_3x_4x_5 + x_1x_2x_3x_4x_5
\end{aligned}$$

命题 1.3 的一个推论是，当 $n \geqslant 1$ 时，斐波那契数 f_{n-1} 统计多项式 g_n 中项的数量，而斐波那契数 f_n 统计 h_n 中项的数量。此外，在 g_n（分别为 h_n）中， $0 \leqslant k \leqslant \lfloor \frac{n-1}{2} \rfloor$（分别为 $0 \leqslant k \leqslant \lfloor \frac{n}{2} \rfloor$）的次数为 $(n-1)-2k$（分别为 $n-2k$）的项数为 $f_{n-1,\,k}$（分别为 $f_{n,\,k}$）。鉴于这些多项式具有内在的类斐波那契结构，它们可以通过简单的递推关系构造出来也就不足为奇了，下一条结果将展示这一点。我们用记号 $g_n(c_1, \ldots, c_n)$ 表示每个 x_j 都已取定为某个整数值 c_j， h_n 的记法也类似。

命题 2.1 eo 多项式 $\{g_n\}_{n \geqslant -1}$ 由递推关系$g_{-1} = 1$、 $g_0 = 0$和 $g_{n+1} = g_{n-1} + g_n x_{n+1}$ 对于 $n \geqslant 0$唯一确定。同样，oe 多项式 $\{h_n\}_{n \geqslant -1}$ 由递推关系 $h_{-1} = 0$、 $h_0 = 1$和 $h_{n+1} = h_{n-1} + h_n x_{n+1}$ 对于 $n \geqslant 0$ 唯一确定。对于正整数 n 和实数 c_1、……、 c_n，我们有 $h_{n-1}(c_2$、……、 $c_n) = g_n(c_1$、 c_2、……、 $c_n)$以及 $c_1 h_{n-1}(c_2$、……、 $c_n) + g_{n-1}(c_2$、……、 $c_n) = h_n(c_1$、 c_2、……、 $c_n)$。

证明。命题前两句中的断言可通过常规的归纳论证得出，这里留给读者完成。最后一句中的断言则可由 g_n 和 h_n 关于 eo 序列与 oe 序列的定义得出。

□

前一个命题中的递推关系使我们能够将 oe 多项式认作 [6] 第 4.5.3 节中的“连续式多项式”。在那里，Knuth 展示了这类多项式与连分数（因此得名）以及欧几里得算法之间的关系。Knuth 将以下对 oe 多项式 h_n 各项的刻画归功于欧拉（大概指的是 [4]）：这些项可由 $x_1x_2\cdots x_n$ 中“删除零个或多个互不重叠的连续变量对 x_jx_{j+1}”得到。正如上文第 1 节所述，这些恰好是以 n 为界的 oe 序列。

§3. B´ezout 引理——一个非构造性结果？传统上称为 B´ezout 引理的结果如下：

引理 3.1 给定整数 a和 b，其中不全为零，则存在整数 s 和 t，使得 $\gcd(a,b) = as + bt$。

尽管这一结果归功于 B´ezout [2],，但 Claude Gaspard Bachet [1]早在一个多世纪前就发现了它的一个版本。Bachet 在欧几里得《几何原本》第七卷中的欧几里得算法框架下，运用符号代数描述了丢番图方程 $ax - by = 1$ 在 a 和 b 互素（即 $\gcd(a,b) = 1$）时的一般解，方法是沿着算法各步骤产生的商和余数逆向追溯。不过，正是通过 B´ezout 的工作，人们才认识到，在整数范围内求解 $ax + by = \gcd(a,b)$ 这一更一般的问题，是初等数论中的一项重要结果（例如，Maarten Bullynck 对高斯之前几个世纪欧洲史上此类余数问题的精彩易读论述，见 [3]）。

不过，贝祖引理有什么实际用途呢？这里给出一个现代应用。密码系统常使用模运算，尤其可能需要在这一运算体系中计算乘法逆元。例如，假设我们知道 a 和 b 互素，并希望在商环 $\mathbb{Z}_a := \mathbb{Z}/a\mathbb{Z}$, 中计算 $\overline{b}^{-1}$ ——如果这样的逆元确实存在的话。（这里，$\overline{x}$ 表示 $\mathbb{Z}_a$中的陪集 $x + a\mathbb{Z}$。）那么，写作 $1 = as + bt$，其中 (s,t) 是一对整数“贝祖系数”。于是 $\overline{1} = \overline{as + bt} = \overline{a}\,\overline{s} + \overline{b}\,\overline{t} = \overline{b}\,\overline{t}$, 因此 $\overline{b}\,\overline{t} = \overline{1}$。也就是说， $\overline{b}$在 $\mathbb{Z}_a$中有乘法逆元，而且 $\overline{b}^{-1} = \overline{t}$。

鉴于这类计算场景，当代关于贝祖引理的论述有时采用非构造性证明，并且先于（如 [14] 的 §3.3），甚至完全绕过（如 [5] 的第 0 章）欧几里得算法，这一点颇为令人好奇。在这类方法中，贝祖引理是利用正整数的（非构造性）良序原理证明的；该原理断言，任何非空的正整数集合都包含一个最小整数。[7] 证明如下：假设a和 b不同时为零，那么 $\{ax + by \,|\, x、\ y \in \mathbb{Z}$和 $ax + by > 0\}$构成一个非空集合。根据良序原理，我们可以认定 d 是该集合中的最小元素。显然

[7]值得注意的是，在这些相同的参考文献中，带余除法算法也被视为一个非构造性结果，其存在性是良序原理的推论（见 [5] 第 0 章和 [14]第 1.5 节）。特别是，当 a和 b为满足 $b \neq 0$的整数时， $\{a - bk \,|\, k \in \mathbb{Z}$和 $a - bk \geqslant 0\}$非空，并且包含一个形如 $a - bq$的最小元素 r，由此我们很容易推出 $0 \leqslant r < |b|$。当然，要确立带余除法算法的存在性结论，完全不必采用这种非构造性推理。

$\gcd(a,b)|d$，所以 $\gcd(a,b) \leqslant d$。为证明 d 是 a的一个因数，设 $a = dq + r$，其中 $0 \leqslant r < d$，由此 $r = dq - a = a(xq-1) + b(yq)$，从而必有 $r = 0$。同理可得 $d|b$，现在可以得出结论： $d \leqslant \gcd(a, b)$。因此， $d = \gcd(a,b)$。

接下来，我们将说明，oereo 多项式结合欧几里得算法提供的数据，可以得出贝祖系数的显式非递归公式。

§4. 扩展欧几里得算法的一种形式。欧几里得算法是一种古老的程序，可在不对两个整数进行因数分解的情况下求出它们的最大公约数。这一算法之所以归于欧几里得，是因为它著名地出现在他的巨著《几何原本》中，作为第七卷的命题 2。然而，这一结果很可能早在欧几里得之前就已为人所知，或许为毕达哥拉斯学派所知；数学家兼历史学家巴特尔·伦德特·范德瓦尔登等人曾提出这一观点[8]，见 [16]。唐纳德·克努特在其经典著作《计算机程序设计艺术》中写道，欧几里得算法是"所有算法的鼻祖，因为它是流传至今最古老的非平凡算法"（见 [6]的§4.5.2）。

扩展欧几里得算法（例如 [14] 的 §3.4）会在求出最大公约数的同时确定贝祖系数。这里，我们将传统的（未扩展的）欧几里得算法表述为一个逐步推进的伪代码过程，从而探讨它与贝祖引理以及我们对 Terquem遗忘的问题的解答之间的联系。我们以一对满足 $a \geqslant b$ 的正整数 a 和 b 为输入。该过程逐步应用带余除法算法，每一步都产生一个商和一个余数，并将最后一个非零余数作为最大公约数返回。我们还将返回该过程提供的其他数据，尤其是过程中得到的完整商列表和完整余数列表。借助 oereo 多项式，我们将看到如何利用这些数据恢复扩展欧几里得算法所能提供的所有信息。

EUCLIDEAN ALGORITHM (EA)

INPUT: 满足 $a \geqslant b$ 的正整数 a 和 b。

INITIALIZATION: 令 $r_{-1} := a$ 和 $r_0 := b$分别视为实际余数。令 i 为步数计数索引，初始值为 $i := 1$。

STEP 1: 应用带余除法算法，我们得到唯一的整数 q_i 和 r_i，满足 $0 \leqslant r_i < r_{i-1}$和

$$r_{i-2} = r_{i-1}q_i + r_i.$$

STEP 2: 若 $r_i = 0$，则 RETURN 以下数据： GCD:= r_{i-1}， NUM_STEPS := i， REM_LIST :=(r_{-1}, r_0, ..., r_i)，以及 QUO_LIST := (q_1, ..., q_i)。

STEP 3: 否则，令 $r_i > 0$，用 $i+1$ 替换 i，然后返回 STEP 1。

OUTPUT:一个正整数 GCD （稍后将证明它是 a 和 b的最大公约数），

[8]摘自 [16]第 115 页："……第七卷并非后世重构之作，而是古代数学的一部分。……由此我们获得了一项重要的认识： *Book VII was a textbook on the elements of the Theory of Numbers, in use inthe Pythagorean school.*"[9]为简便起见，假定其为正。

一个正整数 NUM_STEPS，用于记录我们应用带余除法算法的次数；非负整数余数列表 REM_LIST，其索引从 -1 到 NUM_STEPS；以及正整数商列表 QUO_LIST，其索引从 1 到 NUM_STEPS。

对于满足 $a \geqslant b$的正整数 a 和 b，我们用记号 $\mathrm{EA}(a,b)[\mathrm{GCD}]$ 表示算法返回的最大公约数，用$\mathrm{EA}(a,b)[\mathrm{NUM_STEPS}]$ 表示欧几里得算法应用带余除法算法的次数，用$\mathrm{EA}(a,b)[\mathrm{REM_LIST}]$ 表示余数列表，用$\mathrm{EA}(a,b)[\mathrm{QUO_LIST}]$ 表示商列表。

例4.1 为了说明这个版本的欧几里得算法，我们寻找了输入数 a 和 b，使算法恰好在7步后终止，也就是应用带余除法算法7次。我们如何找到这样的 a 和 b ——以及为什么需要恰好这么多步——很快就会揭晓。带着这个想法，来看 $a = 4449$ 和 $b = 935$。下面是$\mathrm{EA}(a、\ b)$ 的运算过程：

$$\begin{aligned} 4449 &= 935 \cdot 4 + 709 \\ 935 &= 709 \cdot 1 + 226 \\ 709 &= 226 \cdot 3 + 31 \\ 226 &= 31 \cdot 7 + 9 \end{aligned} \qquad \begin{aligned} 31 &= 9 \cdot 3 + 4 \\ 9 &= 4 \cdot 2 + 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned}$$

欧几里得算法的输出如下：$\mathrm{EA}(a,b)[\mathrm{GCD}] = 1$、$\mathrm{EA}(a,b)[\mathrm{NUM_STEPS}] = 7$、$\mathrm{EA}(a,b)[\mathrm{REM_LIST}] =$(4449、935、709、226、31、9、4、1、0)，以及$\mathrm{EA}(a,b)[\mathrm{QUO_LIST}] = (4$、1、3、7、3、2、4)。事实上，我们可以通过回溯前面的等式来构造贝祖系数：$1 = 9 + 4 \cdot {}^{-}2 = 31 \cdot {}^{-}2 + 9 \cdot 7 = 226 \cdot 7 + 31 \cdot {}^{-}51 = 709 \cdot {}^{-}51 + 226 \cdot 160 = 935 \cdot 160 + 709 \cdot {}^{-}211 = 4449 \cdot {}^{-}211 + 935 \cdot 1004$，因此我们的贝祖系数为 $s = {}^{-}211$ 和 $t = 1004$。 □

定理4.2（欧几里得算法定理）设 a 和 b 为正整数，且 $a \geqslant b$。

（0）对于此输入，欧几里得算法会终止。在定理陈述的其余部分，我们令

$$G := \mathrm{EA}(a,b)[\mathrm{GCD}],\ n := \mathrm{EA}(a,b)[\mathrm{NUM_STEPS}],$$
$$(r_{-1},\ r_0,\ \ldots r_n) := \mathrm{EA}(a,b)[\mathrm{REM_LIST}],\ \text{且}\ (q_1,\ \ldots,\ q_n) := \mathrm{EA}(a,b)[\mathrm{QUO_LIST}],$$

其中（如算法结束时所述），输出 $G = r_{n-1}$ 是一个正整数，r_{-1} 和 r_0 分别是正整数 a 和 b，n 记录欧几里得算法应用带余除法算法的次数，而 $(r_1,\ \ldots r_n)$ 是非负整数余数序列，$(q_1,\ \ldots,\ q_n)$ 是通过这 n 次带余除法算法应用得到的正整数商序列。

（1）（一个贝祖型结果）对于任意 $i \in \{-1,\ 0,\ \ldots,\ n\}$，令 $\overrightarrow{g_i} := g_i(q_1,\ \ldots,\ q_i)$，$\overleftarrow{g_i} := g_i(q_{n+1-i},\ \ldots,\ q_n)$，$\overrightarrow{h_i} := h_i(q_1,\ \ldots,\ q_i)$，且 $\overleftarrow{h_i} := h_i(q_{n+1-i},\ \ldots,\ q_n)$，并暂且允许$r_{n+1} := G$。对于每个这样的 i，$r_i = (-1)^{i+1}\overrightarrow{g_i}\, a + (-1)^i \overrightarrow{h_i}\, b$，$r_{n-i} = \overleftarrow{g_i}\, G$，以及 $r_{n-1-i} = \overleftarrow{h_i}\, G$。

(2) 对任意 $i \in \{0、1、\ldots\ldots、n\}$，如果 c 是 r_{i-1} 和 r_i 的因数，那么 c 整除 r_{-1}、r_0、……、r_n 中的每一个。

(3) a 和 b 的最大公约数是 G，即 $G = \gcd(a、b)$。此外，集合 $\{ax + by \mid x、y \in \mathbb{Z}\}$ 恰好由 $\gcd(a、b)$ 的整数倍组成。特别地，$\gcd(a、b)$ 是可表示为 a 和 b 的整数线性组合的最小正整数。此外，$\gcd(a、b) = (-1)^n g_{n-1}(q_1、\ldots\ldots、q_{n-1})a + (-1)^{n-1}h_{n-1}(q_1、\ldots\ldots、q_{n-1})b$，$b = g_n(q_1、\ldots\ldots、q_n)\gcd(a、b)$，以及 $a = h_n(q_1、\ldots\ldots、q_n)\gcd(a、b)$。

证明。对于（0），考虑余数序列 $r_{-1} \geqslant r_0 > r_1 > \cdots$。现在，$b = r_0 > 0$、$b-1 \geqslant r_1 \geqslant 0$、$b-2 \geqslant r_2 \geqslant 0$，等等。由于 $b - b = 0$，余数序列的最大可能索引为 b，因此算法至多经过 b 步便会终止。这证明了欧几里得算法会终止。定理陈述中（0）部分所声称的关于 G、n、$(r_1、\ldots r_n)$、$(q_1，\ldots\ldots，q_n)$ 的每一项的记录内容，均可由算法终止步骤的描述得出。

对于（1），我们对 i 进行归纳，以此说明每个余数 r_i 都能表示为 a 和 b 的整数线性组合。当 $i = -1$ 时，我们有 $r_{-1} = a = (-1)^0 \cdot 1 \cdot a + (-1)^{-1} \cdot 0 \cdot b$；当 $i = 0$ 时，我们有 $r_0 = b = (-1)^1 \cdot 0 \cdot a + (-1)^0 \cdot 1 \cdot b$。现在假设对于某个 $j \in \{0，1，\ldots\ldots，n-1\}$，对每个 $i \in \{-1，0，\ldots\ldots，j\}$，都有 $r_i = (-1)^{i+1}\overrightarrow{g_i}\,a + (-1)^i\overrightarrow{h_i}\,b$。由 $r_{j-1} = r_j q_{j+1} + r_{j+1}$ 可知

$$\begin{aligned} r_{j+1} &= r_{j-1} - q_{j+1}r_j \\ &= \left((-1)^j\overrightarrow{g_{j-1}}\,a + (-1)^{j-1}\overrightarrow{h_{j-1}}\,b\right) + q_{j+1}\left((-1)^j\overrightarrow{g_j}\,a + (-1)^{j-1}\overrightarrow{h_j}\,b\right) \\ &= (-1)^j\left(\overrightarrow{g_{j-1}} + \overrightarrow{g_j}q_{j+1}\right)a + (-1)^{j-1}\left(\overrightarrow{h_{j-1}} + \overrightarrow{h_j}q_{j+1}\right)b \\ &= (-1)^{j+2}\overrightarrow{g_{j+1}}\,a + (-1)^{j+1}\overrightarrow{h_{j+1}}\,b, \end{aligned}$$

如所需（其中，后一个等式由应用命题 2.1 得出）。

为证明第 (1) 部分的最后几个结论，我们用归纳法证明：对于每个 $i \in \{-1, 0, \ldots, n+1\}$，都有 $r_{n-i} = \overleftarrow{g_i}\,G$ and $r_{n-1-i} = \overleftarrow{h_i}\,G$，其中 $G = r_{n-1} =$ 最大公因数(a, b)。当 $i = -1$ 时，显然有 $r_{n+1} = G = \overleftarrow{g_{-1}}\,G$ and $r_n = 0 = \overleftarrow{h_{-1}}\,G$。现在假设对于某个 $j \in \{-1, 0, \ldots, n\}$，对每个 $i \in \{-1, 0, \ldots, j\}$，都有 $r_{n-i} = \overleftarrow{g_i}\,G$ and $r_{n-1-i} = \overleftarrow{h_i}\,G$。根据归纳假设，$r_{n-(j+1)} = r_{n-1-j} = h_j(q_{n+1-j}, \ldots, q_n)\,G = g_{j+1}(q_{n-j}, \ldots, q_n)\,G$，其中后一个等式由命题 2.1 得出。类似地，我们得到 $r_{n-1-(j+1)} = r_{n-(j+1)}q_{n-j} + r_{n-j} = q_{n-j}h_j(q_{n+1-j}, \ldots, q_n)\,G + g_j(q_{n+1-j}, \ldots, q_n)\,G = h_{j+1}(q_{n-j}, \ldots, q_n)\,G$。至此，归纳论证以及 (1) 的证明均告完成。

对于（2），注意如果 $c|r_i$ 和 $c|r_{i-1}$，那么 $c|(r_{i-1}q_i + r_i)$，所以 $c|r_{i-2}$。重复这一推理可知 $c|r_{i-3}$、$c|r_{i-4}$ 等等，最终得到 $c|b$ 和 $c|a$。由于 c 是 a 和 b的公因数，因此根据（1），$c \,\Big|\, \left((-1)^{i+1}\overrightarrow{g_i}\,a + (-1)^i\overrightarrow{h_i}\,b\right)$，所以 c 是每个 r_i的因数。对于（3），由于 $r_n = 0$ 和 $r_{n-1} = G$，那么 $G|r_n$ 和 $G|r_{n-1}$，因此根据（2），对于每个 $i \in \{-1，0，\ldots，n\}$，都有 $G|r_i$。特别地，G 是 $a = r_{-1}$ 和 $b = r_0$的公因数，因此根据（2），$\gcd(a, b) \geqslant G$。由于 $\gcd(a, b)$ 也是 $a = r_{-1}$ 和 $b = r_0$的公因数，因此再次根据（2），$\gcd(a, b)|r_{n-1}$，并且特别地 $\gcd(a, b) \leqslant G$。所以，$\gcd(a, b) = G$。于是，集合 $\{ax + by \mid x, y \in \mathbb{Z}\}$ 中的每个元素都是

G的倍数；如果我们能证明 G 是 a 和 b的整数线性组合，那么这个集合就包含 G 的所有倍数。当然，后一个事实正是（1）的 $i = n - 1$ 情形。 □

§5. 结束语。作为讨论的总结，我们回想一下早先例4.1中的一个问题：我们是如何找到整数 a 和 b，使欧几里得算法恰好在 $n = 7$ 步后终止的？为什么是 $n = 7$？其实，为了给离散数学课程的学生寻找示例来说明算法，我们认为，让学生进行涉及 g_7 和 h_7 的计算——它们分别有13项和21项——就足以有力地表明我们提出的欧几里得算法、贝祖引理与斐波那契数组之间的联系。根据定理4.2.1，只需选取一个由商组成的序列 $q_1, q_2, \ldots, q_7$，然后取 $b := g_7(q_1, q_2, \ldots, q_7)$ 和 $a := h_7(q_1, q_2, \ldots, q_7)$，就能找到这样的 a 和 b。我们把验证留作练习：对于例4.1中的商序列 4, 1, 3, 7, 3, 2, 4，我们确实得到 $b = 935 = g_7(4, 1, 3, 7, 3, 2, 4)$ 和 $a = 4449 = h_7(4, 1, 3, 7, 3, 2, 4)$。请读者思考：定理4.2的哪个方面使我们能够得出结论，认为这些数 a 和 b 互素？

在 [3], Bullynck 的 §3.1 中，他指出，莱昂哈德·欧拉和亚伯拉罕·戈特赫尔夫·卡斯特纳在18世纪后期分别撰写的某些数论论述，都用输入整数演示了欧几里得算法：最多只需应用带余除法算法五六次，就能求出最大公因数；不过，卡斯特纳提到了这样一种情况："必须进行54次除法，才能找到最大公约数。"Bullynck 还指出，后一个问题是一个经典趣味问题，最初由莱昂纳多·斐波那契提出（至于他的别名是什么，就留给读者去辨认了）。因此，我们邀请读者运用本文的成果，找出一对使欧几里得算法恰好经过54步才终止的最小正整数输入 a 和 b（例如，可用它们的和 $a + b$来衡量"大小"）。在这种情况下，最大公因数是多少？

为了更好地理解有关 Terquem问题的历史记载，我们将他的思想与斐波那契数、连分式分子、贝祖引理以及欧几里得算法联系起来。尤其是，我们如今对斐波那契数组中的数有了新的诠释，至少可以说，这种诠释如今已不再被遗忘。由此可以直接得到与连分式分子相关的某些多项式的组合式显式描述。并且，给定正整数 a 和 b，还可直接得到贝祖系数以及整数 a/最大公因数(a、b) 和 b/最大公因数(a、b)的显式公式。所有这些思想在文献中都能找到先例；不过，我们相信，将它们按照本文的方式结合起来，便能对这些初等数论概念作出明确且在组合意义上颇具说服力的阐释，也可能适合纳入有关这些主题的入门论述中。

参考文献

[1] C. G. Bachet deM´eziriac，《趣味数学问题集》，分为两部分：一部分辑录自不同作者，另一部分为新作，并附有证明，第二版增订版，Rigaud，里昂，1624。

[2] E. B´ezout, 《数学教程》，供皇家卫队和海军使用。第三部分：代数，Musier，巴黎，1766年。[3] M. Bullynck, “高斯之前的模算术：18世纪德国对余数问题的系统化与讨论”, 《数学史》（爱思唯尔）36（2009年），48–72。[4] L. Euler, “特殊算法样本”, 《彼得堡帝国科学院新纪事》9（1764年），53–69。[5] J. A. Gallian, 《当代抽象代数》， 9th 版，圣智学习，波士顿，2015年。[6] D. E. Knuth, 《计算机程序设计艺术》，第2卷：半数值算法， 3^{rd}版，Addison–Wesley Professional，1997年。（数学科学出版社制作的授权 PDF 版本可在 www.informit.com 获取）[7] T. Koshy, 《斐波那契数与卢卡斯数及其应用》，第1卷， 2nd 版，约翰·威立父子公司，霍博肯，新泽西州，2018年。[8] E. Lucas, “简单周期数值函数理论”, 《美国数学杂志》1（1878年），184–196。[9] T. Mansour 和 A. O. Munagi, “模 m的交错子集”, 《落基山数学杂志》42（2012年），1313–1325。[10] E. Netto, 《组合学教程》，B. G. Teubner 出版社，莱比锡，1901年。[11] OEIS 基金会, 《整数数列在线百科全书》，http://oeis.org/A011973，2018年。[12] OEIS 基金会, 《整数数列在线百科全书》，http://oeis.org/A046854，2018年。[13] J. Riordan, 《组合分析导论》，约翰·威立父子公司，纽约，1958年。[14] K. H. Rosen, 《初等数论及其应用》， 6th 版，Addison–Wesley（培生旗下品牌），波士顿，2011年。[15] O. Terquem, “论欧拉的一个组合符号及其在分析中的用途”, 《纯粹与应用数学杂志》4（1839年），177–184。[16] B. L. van der Waerden, 《科学的觉醒 I》，Arnold Dresden 英译，作者补充内容，第四版，克吕维尔学术出版社，多德雷赫特，荷兰，1975年。