解决 33 问题

ANDREW R. BOOKER

摘要受到 Tim Browning 和 Brady Haran 的 Numberphile 视频 ``未解决的 33 问题'' 的启发，我们研究了方程 $x^3+y^3+z^3=k$ 在一些小的 k 值的解。我们找到了 $k=33$ 的第一个已知解。

1. 简介

令 k 为正整数，其中 $k \equiv \pm 4 (\mathrm{mod} 9)$。然后 Heath-Brown [HB92] 推测有无限多的三元组 $(x,y,z) \in \mathbb{Z}^3$ 满足

$$k = x^3+y^3+z^3. \quad (1)$$

早在 1954 年就开始对（1）进行各种数值研究[MW55]；请参阅[BPTYJ07]，了解截至 2000 年的这些研究的历史。自那时起进行的计算由于 Elkies [Elk00] 而被算法所主导。我们所知道的最新内容是 Huisman [Hui16] 的论文，该论文确定了（1）的所有解，其中 $k \leq 1000$ 且 $\max\{|x|,|y|,|z|\} \leq 10^15$。特别是，Huisman 报告说除了 13 个 $k \leq 1000$ 的值以外的所有解决方案都是已知的：

$$33, 42, 114, 165, 390, 579, 627, 633, 732, 795, 906, 921, 975. \quad (2)$$

Elkies 的算法通过使用格基减少（lattice basis reduction）在 Fermat 曲线 $X^3+Y^3=1$ 附近寻找有理点来工作；它非常适合同时找到许多 k 值的解。在本文中，我们描述了一种在 k 值确定时更有效的不同方法。它的优点是可以找到所有具有 最小坐标界限的解，而不是 Elkies 算法中的最大坐标。这总是产生搜索范围的非平凡的扩张（nontrivial expansion），因为除了可以单独考虑的有限多个例外之外，还有

$$\max\{|x|,|y|,|z|\} > \sqrt[3]{2} \min\{|x|,|y|,|z|\}$$

此外，根据经验，通常情况是其中一个变量比其他变量小得多，因此我们希望实际上增益更大。

我们的策略类似于一些早期的方法（特别参见[HBLtR93]，[Bre95]，[KTS97]和[BPTYJ07]），并且基于观察：$k-z^3=x^3+y^3$ 的任何解都具有 $x+y$ 作为一个因子。相对于早期研究，我们的主要贡献是注意到，通过一些时间空间权衡，运行时间在高度边界内非常接近线性，并且在现代 64 位计算机上实现时非常实用。

更详细地说，假设 (x,y,z) 是（1）的解，并且不失一般性，假设 $|x|\geq|y|\geq|z|$。然后我们有

$$k-z^3=x^3+y^3=(x+y)(x^2-xy+y^2)$$

如果 $k-z^3=0$ 则 $y=-x$，并且 x 的每个值都产生一个解。否则，设 $d=|x+y|=|x|+y\operatorname{sgn}x$，我们看到 d 可以除 $|k-z^3|$ 并且

$$\begin{aligned}\frac{|k-z^3|}{d}&=x^2-xy+y^2=x(2x-(x+y))+y^2\\&=|x|(2|x|-d)+(d-|x|)^2=3x^2-3d|x|+d^2\end{aligned}$$

得到

$$\{x,y\}=\left\{\frac{1}{2}\operatorname{sgn}(k-z^3)\left(d\pm\sqrt{\frac{4|k-z^3|-d^3}{3d}}\right)\right\}$$

因此，给定 z 的候选值，通过遍历 $|k-z^3|$ 的所有除数，有一个有效的程序来查找 x 和 y 的所有相应值。这个基本算法在假设整数分解的时间复杂度的标准启发式（standard heuristics）下，已经能在时间 $O(B^{1+\varepsilon})$ 内找到满足 $\min\{|x|,|y|,|z|\}\geq B$ 的所有解。在下一节中，我们将解释如何避免因子分解并更有效地实现相同目的。

感谢感谢 Roger Heath-Brown 提供了有用的意见和建议。

2. 方法

为了便于表示，我们假设 $k\equiv\pm3(\mathrm{mod}9)$；请注意，这适用于（2）中的所有 k。由于上述基本算法对于寻找小解是合理的，因此我们将假设 $|z|>\sqrt{k}$。此外，如果我们将（1）专门用于 $y=z$ 的解，那么我们得到 Thue 方程 $x^3+2y^3=k$，这是有效可解的。使用 PARI/GP [The18] 中的 Thue 求解器，我们验证了（2）中的 k 不存在这样的解。因此，我们可以进一步假设 $y\neq z$。

由于 $|z|>\sqrt{k}\geq\sqrt[3]{k}$，我们有

$$\operatorname{sgn}z=-\operatorname{sgn}(k-z^3)=-\operatorname{sgn}(x^3+y^3)=-\operatorname{sgn}x.$$

同样，因为 $x^3+z^3=k-y^3$ 和 $|y|\geq|z|$，我们有 $\operatorname{sgn}y=-\operatorname{sgn}x=\operatorname{sgn}z$。将（1）的两边乘以 $-\operatorname{sgn}z$，我们得到

$$|x|^3-|y|^3-|z|^3=-k\operatorname{sgn} z \quad (4)$$

令 $\alpha=\sqrt[3]{2}-1$，并且 $d=|x+y|=|x|-|y|$。如果 $d\geq\alpha|z|$ 则

$$\begin{aligned}-k\operatorname{sgn} z&=|x|^3-|y|^3-|z|^3\geq(|y|+\alpha|z|)^3-|y|^3-|z|^3\\&=3\alpha(\alpha+2)(|y|-|z|)z^2+3\alpha(|y|-|z|)^2|z|\\&\geq 3\alpha(\alpha+2)|y-z|z^2\end{aligned}$$

由于 $3\alpha(\alpha+2)>1$，这与我们的假设不相容，即 $y\neq z$ 和 $|z|>\sqrt{k}$。因此我们必然有 $0<d<\alpha|z|$。

接下来，减少（4）模 3 并回想我们的假设 $k\equiv\pm 3(\bmod 9)$，我们有

$$d=|x|-|y|\equiv|z|\pmod 3.$$

设 $\epsilon\in\{\pm 1\}$ 使得 $k\equiv 3\epsilon(\bmod 9)$。然后，由于每个立方数都与 0 或 $\pm 1(mod9)$ 相等，我们必然有 $x\equiv y\equiv z\equiv\epsilon(\bmod 3)$，因此 $\operatorname{sgn} z=\epsilon(\frac{|z|}{3})=\epsilon(\frac{d}{3})$。基于（3），当且仅当 $d|z^3-k$ 以及 $3d(4|z^3-k|-d^3)=3d(4\epsilon(\frac{d}{3})(z^3-k)-d^3)$ 是平方数时，我们得到（1）的解。

总之，找到（1）的所有解并且满足 $|x|\geq|y|\geq|z|>\sqrt{k}$，$y\neq z$ 和 $|z|\leq B$，对于每个与 3 互质的 $d\in\mathbb{Z}\cap(0,\alpha B)$，解决以下系统就足够了：

$$\begin{aligned}&\frac{d}{\sqrt[3]{2}-1}<|z|\leq B,\quad \operatorname{sgn} z=\epsilon\left(\frac{d}{3}\right),\quad z^3\equiv k\pmod d\\&3d\left(4\epsilon\left(\frac{d}{3}\right)(z^3-k)-d^3\right)=\square \qquad (5)\end{aligned}$$

我们解决这个问题的方法很简单：我们通过它们的主要因子分解递归地计算 d 的值，并应用中国剩余定理来将 $z^3\equiv k(\bmod d)$ 的解减少到素数模幂的情况下，其中标准算法可以适用。设 $r_d(k)=\#\{z(\bmod d):z^3\equiv k(\bmod d)\}$ 表示 k 模 d 的立方根数。通过标准分析估计，由于 k 不是立方数，我们有

$$\sum_{d\leq\alpha B}r_d(k)\ll_k B$$

启发式地，计算对所有素数 $p\leq\alpha B$ 的 $z^3\equiv k(\bmod p)$ 的解可以用 $[0,\alpha B]$ 上的整数在 $O(B)$ 算术运算来完成；见例如 [[NZM91]，§2.9，练习 8] 中描述的算法。假设这一点，可以看出，使用 Montgomery 的批量反转技巧 [[Mon87]，§10.3.1]，计算对所有正整数 $p\leq\alpha B$ 的 $z^3\equiv k(\bmod p)$ 的根的剩余工作可以再次用 $O(B)$ 算术运算完成。

因此，我们可以在线性时间内计算满足（5）的第一行的所有 z，作为算术进展（arithmetic progressions）的并集。为了检测最后一行的解，有一个快速的方

法来确定 $\Delta := 3d\left(4\epsilon(\frac{d}{3})(z^3-k)-d^3\right)$ 是一个平方数至关重要。我们首先注意到对于固定 d, 这种情况减少到在椭圆曲线上找到积分点; 特别是, 令 $X=12d|z|$ 和 $Y=(6d^2|x-y|$，从（3）中我们看到（X，Y）位于 Mordell 曲线上

$$Y^2=X^3-2(6d)^3\left(d^3+4\epsilon\left(\frac{d}{3}\right)k\right). \quad (6)$$

因此，对于固定 d，存在至多有限多个解，并且它们可以被有效地约束。对于 d 的一些小值，找到（6）上的所有积分点并检查是否产生任何满足（1）的解是切实可行的。例如，使用 Magma[[BCFS18]，§128.2.8] 中的积分点函数（functionality），我们验证了如（2）中的 k 和 $d\leq 40$ 情况下没有解，除了 $(k,d)\in\{(579,29),(579,34),(975,22)\}$。

接下来我们自然注意到一些同余和可分性约束:

引理设 z 为（5）的解，设 p 为素数，设 $s=ord_p d$，$t=ord_p(z^3-k)$。则

(i) $z\equiv\frac{4}{3}k\left(2-d^2\right)+9(k+d)(\bmod 18)$;
(ii) 如果 $p\equiv 2(\bmod 3)$ 则 $t\leq 3s$;
(iii) 如果 $t\leq 3s$ 则 $s\equiv t(\bmod 2)$;
(iv) 如果 $ord_p k\in\{1,2\}$ 则 $s\in\{0,ord_p k\}$。

证明令 $\Delta=3d\left(4\epsilon(\frac{d}{3})(z^3-k)-d^3\right)$，令 $\delta=(\frac{d}{3})$，我们有 $|z|\equiv d\equiv\delta(\bmod 3)$，观察到 $(\delta+3n)^3\equiv\delta+9n(\bmod 27)$，模 27，我们有

$$\begin{aligned}\frac{\Delta}{3d}&=4\epsilon\delta\left(z^3-k\right)-d^3=4|z|^3-d^3-4\epsilon\delta k\\&\equiv 4[\delta+3(|z|-\delta)]-[\delta+3(d-\delta)]-4\epsilon\delta k=3(4|z|-d)-\delta[18+4(\epsilon k-3)]\\&\equiv 3(4|z|-d)-d[18+4(\epsilon k-3)]=12|z|-9d-4\epsilon dk\\&\equiv 3|z|-4\epsilon dk\end{aligned}$$

这消失了模 9，所以为了使 Δ 成为平方数，它也必须消除 mod 27。于是

$$z=\epsilon\delta|z|\equiv\frac{4\delta dk}{3}\equiv\frac{4(2-d^2)k}{3}\quad(\bmod 9)$$

减少（1）模 2 我们得到 $z\equiv k+d(\bmod 2)$，这得到（i）。

接下来设 $u=p^{-s}d$ 和 $v=p^{-t}\epsilon\delta(z^3-k)$，这样就有

$$\Delta=3\left(4p^{s+t}uv-p^{4s}u^4\right)$$

如果 $3s<t$ 则 $p^{-4s}\Delta\equiv-3u^4(\bmod 4p)$，但是当 $p\equiv 2(\bmod 3)$ 时这是不可能的，因为 -3 不是 $4p$ 的平方模。因此，在这种情况下我们必须 $t<3s$。

接下来假设 $t<3s$。我们考虑以下情况，涵盖所有可能性:

- 若 $p=3$ 则 $s=t=0$，那么 $s\equiv t(\bmod 2)$。
- 若 $p\neq 3$ 且 $3s>t+2\operatorname{ord}_p 2$，则 $\operatorname{ord}_p\Delta=s+t+2\operatorname{ord}_p 2$，那么 $s\equiv t(\bmod 2)$。
- 若 $3s\in\{t,t+2\}$ 则 $s\equiv t(\bmod 2)$。
- 如果 $p=2$ 且 $3s=t+1$ 则 $2^{-4s}\Delta=3(2uv-u^4)\equiv 3(\bmod 4)$，这是不可能的。

因此，在任何情况我们得出结论 $s\equiv t(\bmod 2)$。

最后，假设 $p|k$ 和 $p\nmid 3k$。如果 $s=0$ 则无需证明的，所以假设不然。由于 $d|z^3-k$，我们必须有 $d|k$，因为

$$0<s\le t=\operatorname{ord}_p(z^3-k)=\operatorname{ord}_p k<3s$$

通过部分（`iii`）得出 $s\equiv\operatorname{ord}_p k(\bmod 2)$，因此 $s=\operatorname{ord}_p k$。

因此，一旦 $z(\bmod d)$ 的残差类（`residue class`）固定，则其残差模 $lcm(d,18)$ 是确定的。还要注意，条件（`ii`）和（`iii`）对于测试 $p=2$ 是有效的。

然而，即使有这些优化，也有 $\ll B\log B$ 对 d,z 满足（5）的第一行和引理的结论（`i`）和（`iv`）。因此，为了实现比 $O(B\log B)$ 更好的运行时间，需要从一开始就消除一些 z 值。我们通过标准的时间空间交换来实现这一目标。确切地说，设置 $P=3(\log\log B)(\log\log\log B)$，并且让 $M=\prod_{5\le p\le P}p$ 是区间 $[5,P]$ 之间的素数的乘积。根据素数定理，我们得到 $\log M=(1+o(1))P$。如果 Δ 是平方数，那么对于任意素数 $p|M$ 我们有

$$\left(\frac{\Delta}{p}\right)=\left(\frac{3d}{p}\right)\left(\frac{|z|^3-c}{p}\right)\in\{0,1\}\quad (7)$$

其中 $c\equiv\epsilon\left(\frac{d}{3}\right)k+\frac{d^3}{4}$。当 $\operatorname{lcm}(d,18)\le\alpha B/M$ 时，我们首先为每个残差类 $|z|(\bmod M)$ 计算该函数，并且仅选择对于每个 $p|M$ 满足（7）的那些残基。由 `Hasse` 约束，允许的残差的数量最多为

$$\frac{M}{2^{\omega(M/(M,d))}}\prod_{p|\frac{M}{(M,d)}}\left(1+O\left(\frac{1}{\sqrt{p}}\right)\right)=\frac{M}{2^{\omega(M/(M,d))}}e^{O(\sqrt{P}/\log P)}$$

因此，要考虑的 z 值的总数最多为

$$\begin{aligned}
&\textstyle\sum_{lcm(d,18)\le\frac{\alpha B}{M}}r_d(k)\left[M+\frac{e^{O(\sqrt{P}/\log P)}}{2^{\omega(M/(M,d))}}\frac{\alpha B}{d}\right]+\sum_{d\le\alpha B,lcm(d,18)\le\frac{\alpha B}{M}}\frac{r_d(k)\alpha B}{d}\\
&\ll_k B\log M+\frac{e^{O(\sqrt{P}/\log P)}}{2^{\omega(M)}}\textstyle\sum_{g|M}\frac{2^{\omega(g)}r_g(k)}{g}\sum_{d'\le\frac{\alpha B}{9gM}}\frac{r_{d'}(k)\alpha B}{d'}\\
&\ll_k B\log M+B\log B\frac{e^{O(\sqrt{P}/\log P)}}{2^{\omega(M)}}\textstyle\prod_{p|M}\left(1+\frac{2r_p(k)}{p}\right)\\
&\ll BP+\frac{B\log B}{2^{(1+o(1))P/\log P}}\ll B(\log\log B)(\log\log\log B)
\end{aligned}$$

对于没有以这种方式消除的 z，我们遵循类似的策略，其中一些其他辅助模 M' 由较大的素数组成，以加速平方测试。我们预先计算模为 M' 的立方数表和 Legendre 符号模 $p|M'$，因此将测试（7）简化为了表查找。只有当所有这些测试都通过时，我们才能在多精度算术中计算 Δ 并应用一般的平方检验，这种情况对于一小部分候选值来说都是如此。事实上，我们期望 Legendre 测试的数量平均有限，所以总的来说，找到所有解决方案的 $|z| \leq B$ 应该要求不超过 $O_k(B(\log\log B)(\log\log\log B))$ 次表查找和对 $[0, B]$ 中整数的算术运算。

因此，当 B 符合机器字大小时，我们预计运行时间几乎是线性的，这就是我们在实践中观察到的 $B < 2^{64}$。

3. 实现

我们在 C 中实现了上述算法，其中有一些内联汇编程序来源于由 Ben Buhrow [Buh19] 编写的 Montgomery 算法[Mon85]，以及 Kim Walisch 的用于枚举素数的 **primesieve** 库[Wal19]。

该算法自然地在具有超过 $\sqrt{\alpha B}$ 的素因子和具有 $\sqrt{\alpha B}$ -平滑的素数的 d 的值之间分配。前一组 d 消耗超过运行时间的三分之二，但更容易并行化。我们在布里斯托大学高级计算研究中心的大规模并行集群 Bluecrystal Phase 3 上运行了这一部分。对于平滑的 d，我们使用了一个单独的 32 核和 64 核节点的小集群。

我们搜索了满足 $k \in \{33, 42\}$ 和 $\min\{|x|, |y|, |z|\} \leq 10^16$ 的（1）的解，找到了以下结果：

$$33 = 8866128975287528^3 + (-8778405442862239)^3 + (-2736111468807040)^3$$

总计算在三个星期的实际时间中大约使用了 15 个核年。

参考文献

School of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, United Kingdom

E-mail address: andrew.booker@bristol.ac.uk

BCFS18 Wieb Bosma, John Cannon, Claus Fieker, and Allan Steel, *Handbook of Magma functions*, Sydney, 2.24 ed., 2018.

BPTYJ07 Michael Beck, Eric Pine, Wayne Tarrant, and Kim Yarbrough Jensen, *New integer representations as the sum of three cubes*, Math. Comp. 76 (2007), no. 259, 1683--1690. MR 2299795

Bre95 Andrew Bremner, *On sums of three cubes*, Number theory (Halifax, NS, 1994), CMS Conf. Proc., vol. 15, Amer. Math. Soc., Providence, RI, 1995, pp. 87--91. MR 1353923

Buh19 Ben Buhrow, *YAFU*, 2019, https://sourceforge.net/projects/yafu/.

Elk00 Noam D. Elkies, *Rational points near curves and small nonzero* $|x^3 - y^2|$ *via lattice reduction*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 33--63. MR 1850598

HB92 D. R. Heath- Brown, *The density of zeros of forms for which weak approximation fails*, Math. Comp. **59** (1992), no. 200, 613--623. MR 1146835

HBLtR93 D. R. Heath- Brown, W. M. Lioen, and H. J. J. te Riele, *On solving the Diophantine equation* $x^3 + y^3 + z^3 = k$ *on a vector computer*, Math. Comp. **61** (1993), no. 203, 235--244. MR 1202610

Hui16 Sander G. Huisman, *Newer sums of three cubes*, arXiv:1604.07746, 2016.

KTS97 Kenji Koyama, Yukio Tsuruoka, and Hiroshi Sekigawa, *On searching for solutions of the Diophantine equation* $x^3 + y3 + z3 = n$, Math. Comp. **66** (1997), no. 218, 841--851. MR 1401942

MW55 J. C. P. Miller and M. F. C. Woollett, *Solutions of the Diophantine equation* $x^3 + y^3 + z^3 = k$, J. London Math. Soc. **30** (1955), 101--110. MR 0067916

Mon85 Peter L. Montgomery, *Modular multiplication without trial division*, Math. Comp. **44** (1985), no. 170, 519--521. MR 777282

Mon87 ---, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), no. 177, 243--264. MR 866113

NZM91 Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An introduction to the theory of numbers*, fifth ed., John Wiley & Sons, Inc., New York, 1991. MR 1083765

The18 The PARI Group, Univ. Bordeaux, *PARI/ GP version* 2.11.0, 2018, available from http://pari.math.u-bordeaux.fr/.

Wal19 Kim Walisch, *primesieve*, 2019, https://primesieve.org.