INTEGRAL SOLUTIONS OF $x^3 - 2y^3 = 1$

KEITH CONRAD

1. Introduction

For each positive integer d that is not a perfect square, Pell's equation $x^2 - dy^2 = 1$ has infinitely many solutions in integers. For example, the integral solutions of $x^2 - 2y^2 = 1$ are $(\pm x_n, \pm y_n)$ where $x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n$ for $n \in \mathbf{Z}$. Values of x_n and y_n for small $|n|$ are in Table 1.

n	0	1	2	3	-1	-2	-3
x_n	1	3	17	99	3	17	99
y_n	0	2	12	70	-2	-12	-70

Table 1. Coefficients of $(3 + 2\sqrt{2})^n$.

If the exponent in Pell's equation is increased from 2 to 3, so we are looking at $x^3 - dy^3 = 1$, then the description of its integral solutions changes dramatically.

Theorem 1.1 (Delaunay, Nagell)**.** *For nonzero $d \in \mathbf{Z}$, $x^3 - dy^3 = 1$ has at most one solution in $\mathbf{Z}$ besides $(1, 0)$.*

Table 2 lists small $d > 0$ for which there is a solution besides $(1, 0)$. Replacing d with $-d$ has no real effect on solutions, since $x^3 + dy^3 = x^3 - d(-y)^3$.

d	2	7	17	19	20	26	28	37	43	63
x	-1	2	18	-8	-19	3	-3	10	-7	4
y	-1	1	7	-3	-7	1	-1	3	-2	1

Table 2. Ten d for which $x^3 - dy^3 = 1$ has an integral solution besides $(1, 0)$.

Remark 1.2. Theorem 1.1 is about integral solutions, not rational solutions. The equation $x^3 - 7y^3 = 1$ has infinitely many rational solutions besides $(1, 0)$ and $(2, 1)$, such as $(1/2, -1/2)$ and $(17/73, -38/73)$. In contrast to this, the only rational solutions to $x^3 - 2y^3 = 1$ are its two integral solutions $(1, 0)$ and $(-1, -1)$. That is due to Euler [4, Part II, Sect. II, § 247], who showed the integral solutions to $a^3 - b^3 = 2c^3$ are $(a, a, 0)$ and $(a, -a, a)$ (take $x = a/b$ and $y = c/b$ if $b \neq 0$) in connection with his work [4, Part II, Sect. II, § 243] on Fermat's Last Theorem for exponent 3.

That $x^3 - dy^3 = 1$ has finitely many integral solutions was first proved by Thue (1909) using an approximation theorem for irrational algebraic numbers by rational numbers, and his proof in fact shows $x^3 - dy^3 = m$ has finitely many integral solutions for each nonzero integer m. See Section A. That $x^3 - dy^3 = 1$ has at most one integral solution besides $(1, 0)$ is due independently to Delaunay[1] [2] and Nagell [6]. Their proofs are largely algebraic,

[1]Delaunay also wrote his name as Delone. He was Russian and the CIA prepared a once-classified list of his work up to 1950. See https://www.cia.gov/library/readingroom/docs/CIA-RDP82-00039R000100090012-9.pdf.

and such a proof of Theorem 1.1 is in [3, Sect. VII.3] and [5, Sect. 3-9]. A proof of Theorem 1.1 using both algebraic and p-adic arguments, due to Skolem, is in [1, pp. 223–226]. We will use Skolem's ideas to prove Theorem 1.1 in the special case $d = 2$, based partly on [7, pp. 34–35]. Here is our goal.

Theorem 1.3. *The only integral solutions to $x^3 - 2y^3 = 1$ are $(1, 0)$ and $(-1, -1)$.*

2. Reducing Theorem 1.3 to the vanishing of an exponential expression

Theorem 2.1. *Let $u = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ and ω be a nontrivial cube root of unity. The $\mathbf{Q}$-conjugates of u are $u_1 = u$, $u_2 = 1 + \sqrt[3]{2}\omega + \sqrt[3]{4}\omega^2$, and $u_3 = 1 + \sqrt[3]{2}\omega^2 + \sqrt[3]{4}\omega$.*

For $x, y \in \mathbf{Z}$, $x^3 - 2y^3 = 1$ if and only if $x - y\sqrt[3]{2} = u^n$, where the integer n satisfies

$$u_1^n + \omega u_2^n + \omega^2 u_3^n = 0. \tag{2.1}$$

Proof. There are three embeddings of $\mathbf{Q}(\sqrt[3]{2})$ into $\mathbf{C}$, determined by $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$, and $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$. Under these embeddings, the corresponding images of u are u_1, u_2, and u_3 as in the statement of the theorem, so these are the $\mathbf{Q}$-conjugates of u. By a calculation, $u_1u_2u_3 = 1$.

If $x^3 - 2y^3 = 1$ then

$$(x - y\sqrt[3]{2})(x^2 + xy\sqrt[3]{2} + y^2\sqrt[3]{4}) = 1, \tag{2.2}$$

so $x - y\sqrt[3]{2}$ is a unit in $\mathbf{Z}[\sqrt[3]{2}]$. Since $x^2 + xy\sqrt[3]{2} + y^2\sqrt[3]{4} = (x + y\sqrt[3]{2}/2)^2 + (3/4)(y\sqrt[3]{2})^2 > 0$, $x - y\sqrt[3]{2} > 0$ by (2.2).

It can be shown using algebraic number theory that the units in $\mathbf{Z}[\sqrt[3]{2}]$ are the powers of u up to sign: $\mathbf{Z}[\sqrt[3]{2}]^\times = \pm u^{\mathbf{Z}}$. Therefore $x - y\sqrt[3]{2} = \pm u^n$ for some $n \in \mathbf{Z}$. Since the left side is positive and $u > 0$, the sign on the right side is $+$, so $x - y\sqrt[3]{2} = u^n$.

Conversely, suppose $x - y\sqrt[3]{2} = u^n$ for some $n \in \mathbf{Z}$. Applying to this equation the three embeddings of $\mathbf{Q}(\sqrt[3]{2})$ into $\mathbf{C}$, we get $x - y\sqrt[3]{2} = u_1^n$, $x - y\sqrt[3]{2}\omega = u_2^n$ and $x - y\sqrt[3]{2}\omega^2 = u_3^n$. Therefore

$$x^3 - 2y^3 = (x - y\sqrt[3]{2})(x - y\sqrt[3]{2}\omega)(x - y\sqrt[3]{2}\omega^2) = u_1^n u_2^n u_3^n = (u_1u_2u_3)^n = 1.$$

It remains to determine which powers u^n have the form $x - y\sqrt[3]{2}$. The key point is that $\mathbf{Z}[\sqrt[3]{2}] = \mathbf{Z} + \mathbf{Z}\sqrt[3]{2} + \mathbf{Z}\sqrt[3]{4}$ has a $\mathbf{Z}$-basis of size 3, so for all $n \in \mathbf{Z}$,

$$u^n = a_n + b_n\sqrt[3]{2} + c_n\sqrt[3]{4} \tag{2.3}$$

where $a_n, b_n, c_n \in \mathbf{Z}$. To have u^n of the form $x - y\sqrt[3]{2}$ means $c_n = 0$ (and $x = a_n, y = -b_n$). We seek a formula for c_n. Apply to (2.3) each embedding of $\mathbf{Q}(\sqrt[3]{2})$ into $\mathbf{C}$:

$$\begin{aligned} u_1^n &= a_n + b_n\sqrt[3]{2} + c_n\sqrt[3]{4}, \\ u_2^n &= a_n + b_n\sqrt[3]{2}\omega + c_n\sqrt[3]{4}\omega^2, \\ u_3^n &= a_n + b_n\sqrt[3]{2}\omega^2 + c_n\sqrt[3]{4}\omega. \end{aligned}$$

Therefore

$$\begin{pmatrix} u_1^n \\ u_2^n \\ u_3^n \end{pmatrix} = \begin{pmatrix} 1 & \sqrt[3]{2} & \sqrt[3]{4} \\ 1 & \sqrt[3]{2}\omega & \sqrt[3]{4}\omega^2 \\ 1 & \sqrt[3]{2}\omega^2 & \sqrt[3]{4}\omega \end{pmatrix} \begin{pmatrix} a_n \\ b_n \\ c_n \end{pmatrix}.$$

Inverting the 3×3 matrix,

$$\begin{pmatrix} a_n \\ b_n \\ c_n \end{pmatrix} = \begin{pmatrix} 1/3 & 1/3 & 1/3 \\ 1/(3\sqrt[3]{2}) & 1/(3\sqrt[3]{2}\omega) & 1/(3\sqrt[3]{2}\omega^2) \\ 1/(3\sqrt[3]{4}) & 1/(3\sqrt[3]{4}\omega) & 1/(3\sqrt[3]{4}\omega^2) \end{pmatrix} \begin{pmatrix} u_1^n \\ u_2^n \\ u_3^n \end{pmatrix},$$

so

$$c_n = \frac{u_1^n + \omega u_2^n + \omega^2 u_3^n}{3\sqrt[3]{4}}.$$

Therefore $c_n = 0$ if and only if $u_1^n + \omega u_2^n + \omega^2 u_3^n = 0$. □

We now want to find every integer n such that (2.1) is satisfied. Since $u_1 \approx 3.847$ and $|u_2| = |u_3| \approx .5098$, when $n \geq 1$ we can't have $u_1^n = -\omega u_2^n - \omega^2 u_3^n$ since the left side is greater than 3 while the right side is smaller by the triangle inequality. If $n = 0$ and $n = -1$ then (2.1) is true and we have $x^3 - 2y^3 = 1$ where $x - y\sqrt[3]{2} = u^0 = 1$ or $x - y\sqrt[3]{2} = u^{-1} = -1 + \sqrt[3]{2}$: (x, y) is $(1, 0)$ or $(-1, -1)$. We don't expect (2.1) to hold for integers $n \leq -2$, but this is not easy to see because when $n < 0$, (2.1) involves positive powers of $1/u_1$, $1/u_2$, and $1/u_3$ where $1/u_1 \approx .259$ while $|1/u_2| = |1/u_3| \approx 1.96$: if $n < 0$ then there are *two* dominant terms of equal absolute value on the left side of (2.1), so we need to rule out the possibility that there is a nearly total cancellation of dominant terms that could make (2.1) hold for $n < -1$. To achieve this, instead of looking at (2.1) in $\mathbf{C}$, we will look at it in $\mathbf{Q}_p$ for a suitable choice of p. Since (2.1) is a purely algebraic equation, it can be viewed in an arbitrary field of characteristic 0 containing a cube root of 2 and nontrivial cube roots of unity, or equivalently three different cube roots of 2.

To interpret $\sqrt[3]{2}$ and ω as p-adic numbers means the polynomial $T^3 - 2$ has to split completely in $\mathbf{Q}_p$. For $p > 3$, Hensel's lemma tells us that $T^3 - 2$ splits completely in $\mathbf{Q}_p$ if $T^3 - 2$ splits completely mod p.[2] The first few such p are 31, 43, and 109. For example,

$$T^3 - 2 \equiv (T - 4)(T - 7)(T - 20) \bmod 31$$

and in $\mathbf{Q}_{31}$ the polynomial $T^3 - 2$ has roots r_1, r_2, and r_3 where

$$r_1 = 4 + 9 \cdot 31 + 4 \cdot 31^2 + \cdots, r_2 = 7 + 13 \cdot 31 + 29 \cdot 31^2 + \cdots, r_3 = 20 + 8 \cdot 31 + 28 \cdot 31^2 + \cdots.$$

In $\mathbf{Q}_{31}$ the nontrivial cube roots of unity are $r_2/r_1 = 25 + 16 \cdot 31 + 6 \cdot 31^2 + \cdots$ and $r_3/r_1 = 5 + 14 \cdot 31 + 24 \cdot 31^2 + \cdots$. If we denote r_1 by $\sqrt[3]{2}$ and r_2/r_1 by ω then $r_2 = \sqrt[3]{2}\omega$ and $r_3 = \sqrt[3]{2}\omega^2$ in $\mathbf{Z}_{31}$.

3. A finiteness theorem on linear combinations of powers in $\mathbf{Z}_p$

We have shown the only integral solutions to $x^3 - 2y^3 = 1$ are $(x, y) = (1, 0)$ and $(x, y) = (-1, -1)$ when the only $n \in \mathbf{Z}$ satisfying the exponential relation (2.1) are $n = 0$ and $n = -1$. The following theorem uses p-adic power series to give conditions under which such an exponential relation has finitely many solutions.

Theorem 3.1. *Let p be an odd prime. Fix $u_1, \ldots, u_k \in \mathbf{Z}_p^\times$ and $c_1, \ldots, c_k, b \in \mathbf{Z}_p$. The equation*

$$c_1 u_1^n + c_2 u_2^n + \cdots + c_k u_k^n = b \tag{3.1}$$

is true for only finitely many integers n if, for each $r \in \{0, 1, \ldots, p-2\}$, the left side of (3.1) is not b for some $n \equiv r \bmod p-1$.

Proof. For $a \in \mathbf{Z}_p^\times$ with $a \equiv 1 \bmod p\mathbf{Z}_p$, the powers a^n for $n \in \mathbf{Z}$ interpolate to a p-adic analytic function a^x for $x \in \mathbf{Z}_p$: $a^x = e^{x \log a} = \sum_{j \geq 0} (\log a)^j / j!) x^j$. For $u \in \mathbf{Z}_p^\times$ with $u \not\equiv 1 \bmod p$, the sequence u^n for $n \in \mathbf{Z}$ does *not* p-adically interpolate (it is not p-adically continuous in n), but if we focus on exponents in one congruence class mod $p - 1$ then the problem goes away: $u^{p-1} \equiv 1 \bmod p$, so when $n = (p-1)m + r$ for a fixed remainder $r \in \{0, 1, \ldots, p-2\}$,

$$u^n = u^{(p-1)m} u^r = u^r (u^{p-1})^m,$$

[2]The polynomial $T^3 - 2$ is irreducible over $\mathbf{Q}_2$ and $\mathbf{Q}_3$.

and we can p-adically interpolate the right side as a function of m since $u^{p-1} \equiv 1 \bmod p$.

For $r = 0, 1, \dots, p-2$, set

$$f_r(m) = c_1 u_1^r (u_1^{p-1})^m + c_2 u_2^r (u_2^{p-1})^m + \cdots + c_k u_k^r (u_k^{p-1})^m - b.$$

This extends to a p-adic analytic function $f_r(x)$ for $x \in \mathbf{Z}_p$, and the integers $n \equiv r \bmod p-1$ that satisfy (3.1) are of the form $(p-1)m + r$ where m is an integer such that $f_r(m) = 0$.

A p-adic analytic function on $\mathbf{Z}_p$ is either identically zero on $\mathbf{Z}_p$ or has finitely many zeros on $\mathbf{Z}_p$. Therefore if, for each $r \in \{0, 1, \dots, p-2\}$, $f_r(m) \neq 0$ for some integer m, which means (3.1) is not true for some $n \equiv r \bmod p-1$, then each $f_r(x)$ has finitely many zeros in $\mathbf{Z}_p$, so (3.1) is true for only finitely many integers n (check separately for the integers in each congruence class modulo $p-1$). □

Example 3.2. For an integer $n \geq 0$, the sum $(1+\sqrt{-2})^n + (1-\sqrt{-2})^n$ is an even number (terms associated to odd powers of $\sqrt{-2}$ from the binomial theorem cancel out in the sum). How often can this sum be 2? Small n where this happens are $n = 0, 1$, and 5. In $\mathbf{C}$, since $|1+\sqrt{-2}| = |1-\sqrt{-2}| = \sqrt{3} > 1$, the terms $(1+\sqrt{-2})^n$ and $(1-\sqrt{-2})^n$ are equally large for every n, and it's not obvious that the terms couldn't have a near-cancellation and add up to 2 again for some $n > 5$. To investigate this, we want to interpret $1 \pm \sqrt{-2}$ in $\mathbf{Z}_p^\times$ as a first step towards p-adically interpolating their powers, so we need -2 to be a square in $\mathbf{Z}_p$.

The first two primes p for which -2 is a square in $\mathbf{Z}_p^\times$ are 3 and 11. In $\mathbf{Z}_3^\times$, we can take $\sqrt{-2} = 1 + 3 + 2 \cdot 3^2 + \cdots$ using Hensel's lemma. Then $1+\sqrt{-2} \in \mathbf{Z}_3^\times$ but $1-\sqrt{-2} \in 3\mathbf{Z}_3$, which is bad. In $\mathbf{Z}_{11}^\times$ we can take $\sqrt{-2} = 3 + 9 \cdot 11 + 4 \cdot 11^2 + \cdots$, so $1+\sqrt{-2} \equiv 4 \not\equiv 0 \bmod 11$ and $1-\sqrt{-2} \equiv 9 \not\equiv 0 \bmod 11$. Therefore we have 11-adic analytic functions

$$f_r(x) = (1+\sqrt{-2})^r((1+\sqrt{-2})^{10})^x + (1-\sqrt{-2})^r((1-\sqrt{-2})^{10})^x - 2$$

for $r = 0, \dots, 9$.[3] A direct calculation for each r shows $f_r(0) \neq f_r(1)$ (*e.g.*, $f_3(0) = -12$ and $f_3(1) = 2496$). Therefore, qualitatively, each $f_r(x)$ has finitely many zeros in $\mathbf{Z}_{11}$, so the equation $(1+\sqrt{-2})^n + (1-\sqrt{-2})^n = 2$ has only finitely many solutions in nonnegative integers n.

Using Strassmann's theorem about zeros of p-adic analytic functions for $f_0(x), \dots, f_9(x)$ on $\mathbf{Z}_{11}$, it can be shown that $f_0(x)$, $f_1(x)$, and $f_5(x)$ each have $x = 0$ as their only zero in $\mathbf{Z}_{11}$ while $f_r(x)$ has no zero in $\mathbf{Z}_{11}$ for $r \in \{2, 3, 4, 6, 7, 8, 9\}$, so the only solutions of $(1+\sqrt{-2})^n + (1-\sqrt{-2})^n = 2$ in nonnegative integers are $n = 0$, 1, and 5. See Theorem 1.1 in `https://kconrad.math.uconn.edu/blurbs/gradnumthy/strassmannapplication.pdf`.

There is an analogue of Theorem 3.1 in $\mathbf{Z}_2$ by looking separately at the exponents $n \bmod 2$ since $u \in \mathbf{Z}_2^\times \Rightarrow u^2 \equiv 1 \bmod 8$ and a^x is a 2-adic analytic function of x when $a \equiv 1 \bmod 4\mathbf{Z}_2$.

4. Theorem 1.3 using $\mathbf{Q}_{31}$

Let's return to (2.1):

$$u_1^n + \omega u_2^n + \omega^2 u_3^n = 0,$$

where $u_1 = 1 + \sqrt[3]{2} + \sqrt[3]{4}$, $u_2 = 1 + \sqrt[3]{2}\omega + \sqrt[3]{4}\omega^2$, and $u_3 = 1 + \sqrt[3]{2}\omega^2 + \sqrt[3]{4}\omega$. Our goal is to show the only solutions to this in integers is $n = 0$ and $n = -1$.

View the equation in $\mathbf{Q}_{31}$ where $\sqrt[3]{2}$ is the cube root of 2 in $\mathbf{Z}_{31}$ with $\sqrt[3]{2} \equiv 4 \bmod 31$ and ω is the cube root of unity in $\mathbf{Z}_{31}$ with $\omega \equiv 25 \bmod 31$. Then calculations show

$$u_1 \equiv 21 \bmod 31, \quad u_2 \equiv 26 \bmod 31, \quad u_3 \equiv 18 \bmod 31.$$

[3]Since 4 mod 11 and 9 mod 11 have order 5, we could take 11-adic powers of $(1 \pm \sqrt{-2})^5$ and thereby cut down the number of 11-adic analytic functions under consideration from 10 down to 5.

To study $u_1^n + \omega u_2^n + \omega^2 u_3^n$ using 31-adic analytic functions, pick $r \in \{0, 1, \ldots, 29\}$ and look at $u_1^n + \omega u_2^n + \omega^2 u_3^n$ for $n = 30m + r$: define

$$f_r(x) = u_1^r (u_1^{30})^x + \omega u_2^r (u_2^{30})^x + \omega^2 u_3^r (u_3^{30})^x$$

for $x \in \mathbf{Z}_{31}$.[4] We want to study the zeros of each $f_r(x)$ in $\mathbf{Z}_{31}$.

For odd prime p and $a \in 1 + p\mathbf{Z}_p$, $a^x = e^{(\log a)x} = \sum_{j \geq 0} ((\log a)^j / j!) x^j$ is p-adic analytic on $\mathbf{Z}_p$ with $\log a \in p\mathbf{Z}_p$ since $|\log a|_p = |a - 1|_p \leq 1/p$. Therefore $f_r(x)$ is a $\mathbf{Z}_{31}$-linear combination of three 31-adic analytic functions, so $f_r(x)$ is 31-adic analytic. The function $f_r(x)$ is not identically 0 since $f_0(1) \neq 0$ and $f_r(0) \neq 0$ for $1 \leq r \leq 29$, so Strassmann's theorem provides an upper bound on the number of zeros of $f_r(x)$ in $\mathbf{Z}_{31}$: $f_r(x)$ has at most N zeros in $\mathbf{Z}_{31}$ where the Nth power series coefficient of $f_r(x)$ has maximal 31-adic absolute value (minimal 31-adic valuation) and N is as large as possible. For example, if the constant term of $f_r(x)$ has larger 31-adic absolute value than the other coefficients, $N = 0$ so $f_r(x)$ has no zero in $\mathbf{Z}_{31}$.

For odd prime p and $a \in 1 + p\mathbf{Z}_p$, $\log a \in p\mathbf{Z}_p$ and $p^j / j! \in p\mathbf{Z}_p$ for $j \geq 1$, so every nonconstant coefficient of the p-adic power series for a^x is in $p\mathbf{Z}_p$. Therefore the nonconstant coefficients of $f_r(x)$ are all in $31\mathbf{Z}_{31}$. The constant term of $f_r(x)$ is

$$f_r(0) = u_1^r + \omega u_2^r + \omega^2 u_3^r \equiv 21^r + 25 \cdot 26^r + 25^2 18^r \bmod 31$$

Using a computer, $f_r(0) \not\equiv 0 \bmod 31$ except when $r = 0, 9, 10, 19, 20, 29$. Therefore by Strassmann's theorem, $f_r(x)$ has no zero in $\mathbf{Z}_{31}$ if $r \neq 0, 9, 10, 19, 20, 29$. What if r is 0, 9, 10, 19, 20, or 29?

Since $f_0(0) = 1 + \omega + \omega^2 = 0$, $f_0(x)$ has a zero at $x = 0$. When r is 9, 10, 19, 20, and 29, a calculation shows <u>the constant term $f_r(0)$ is divisible by 31 precisely once</u>. The linear coefficient of $f_r(x)$ is

$$u_1^r \log(u_1^{30}) + \omega u_2^r \log(u_2^{30}) + \omega^2 u_3^r \log(u_3^{30}). \tag{4.1}$$

For odd prime p and $a \in 1 + p\mathbf{Z}_p$, $\log a = (a - 1) + \sum_{j \geq 2} (-1)^{j-1} (a - 1)^j / j$ and $(a - 1)^j / j \in p^2\mathbf{Z}_p$ for $j \geq 2$, so $\log a \equiv a - 1 \bmod p^2\mathbf{Z}_p$. Therefore (4.1) is congruent to

$$u_1^r (u_1^{30} - 1) + \omega u_2^r (u_2^{30} - 1) + \omega^2 u_3^r (u_3^{30} - 1) \bmod 31^2\mathbf{Z}_{31}. \tag{4.2}$$

For $r = 0, 9, 10, 19, 20, 29$, calculations show (4.2) is divisible by 31 but is not 0 mod 31^2, so <u>$f_r(x)$ has linear coefficient divisible by 31 precisely once</u>.

For odd prime p and $a \in 1 + p\mathbf{Z}_p$, $\log a \in p\mathbf{Z}_p$ and $p^j / j! \in p^2\mathbf{Z}_p$ for $j \geq 2$, so $(\log a)^j / j! \in p^2\mathbf{Z}_p$ for $j \geq 2$. Thus <u>the coefficients of every $f_r(x)$ in degree 2 and higher are in $31^2\mathbf{Z}_{31}$</u>.

Combining the underlined information about 31-divisibility of power series coefficients with Strassmann's theorem, $f_r(x)$ has at most one zero in $\mathbf{Z}_{31}$ for $r = 0, 9, 10, 19, 20, 29$. Using Hensel's lemma for power series converging on $\mathbf{Z}_{31}$ instead of Strassmann's theorem for power series converging on $\mathbf{Z}_{31}$, $f_r(x)$ has a unique zero in $\mathbf{Z}_{31}$ for $r = 0, 9, 10, 19, 20, 29$. The zero of $f_0(x)$ is $x = 0$ (corresponding to (2.1) being zero at $n = 0 = 30(0) + 0$) and the zero of $f_{29}(x)$ is $x = -1$ (corresponding to (2.1) being zero at $n = -1 = 30(-1) + 29$). We don't expect the zeros of $f_r(x)$ in $\mathbf{Z}_{31}$ for $r = 9, 10, 19$, or 20 to be integers, but that possibility can't be ruled out from the reasoning presented so far. Therefore by working in $\mathbf{Z}_{31}$, we have shown (2.1) is true for at most 6 integers n. To cut down the upper bound further, we will work in a p-adic completion for $p \neq 31$.

[4]Since 21 mod 31 has order 30, we can't use an exponent smaller than 30 in the terms of $f_r(x)$.

5. Theorem 1.3 using 3-adic powers

There is no cube root of 2 in $\mathbf{Q}_3$: if $\alpha^3 = 2$ then $|\alpha|_3^3 = |2|_3 = 1$, so $|\alpha|_3 = 1$: α is in $\mathbf{Z}_3^\times$. Therefore we can reduce the equation $\alpha^3 = 2$ modulo 9 to get $\alpha^3 \equiv 2 \bmod 9\mathbf{Z}_3$. The cubes mod 9 are 0, 1, and 8, so we have a contradiction. Thus $T^3 - 2$ is a cubic polynomial with no root in $\mathbf{Q}_3$, so $\mathbf{Q}_3(\sqrt[3]{2})$ is a cubic extension of $\mathbf{Q}_3$ with basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. There are no nontrivial cube roots of unity in $\mathbf{Q}_3(\sqrt[3]{2})$ since $\mathbf{Q}_3(\omega) = \mathbf{Q}_3(\sqrt{-3})$ is a quadratic extension of $\mathbf{Q}_3$, which can't lie in a cubic extension.

Just as the absolute value on $\mathbf{R}$ has a unique extension to an absolute value on its quadratic extension $\mathbf{C}$, which is complete, the 3-adic absolute value on $\mathbf{Q}_3$ has a unique extension to an absolute value on its cubic extension $\mathbf{Q}_3(\sqrt[3]{2})$, which is complete. It is possible to give a formula for $|a + b\sqrt[3]{2} + c\sqrt[3]{4}|_3$, where $a, b, c \in \mathbf{Q}_3$, that is analogous to the formula $|a + bi| = \sqrt{a^2 + b^2}$ for the absolute value of complex numbers. Here it is:

$$|a + b\sqrt[3]{2} + c\sqrt[3]{4}|_3 = \sqrt[3]{|a^3 + 2b^3 + 4c^3 - 6abc|_3}.$$

We will not discuss how to derive this formula or why it is an absolute value on $\mathbf{Q}_3(\sqrt[3]{2})$. The formula reveals a new phenomenon compared to absolute values on $\mathbf{Q}_3$: some numbers in $\mathbf{Q}_3(\sqrt[3]{2})$ have absolute value that is not an integral power of $1/3$: the nonzero numbers have 3-adic absolute value $(1/3)^{n/3} = (1/\sqrt[3]{3})^n$ for some $n \in \mathbf{Z}$.

Example 5.1. Let $\pi = \sqrt[3]{2} + 1$. Since $|\sqrt[3]{2}^3|_3 = |2|_3 = 1$, $|\sqrt[3]{2}|_3^3 = 1$, so $|\sqrt[3]{2}|_3 = 1$. From the ultrametric inequality, $|\pi|_3 \le \max(|\sqrt[3]{2}|_3, |1|_3) = 1$. Expanding the left side of the equation $(\pi - 1)^3 = 2$ and rearranging terms, we get $\pi^3 - 3\pi^2 + 3\pi - 3 = 0$. Rewrite this as

$$\pi^3 = 3(\pi^2 - \pi + 1).$$

Therefore $|\pi|_3^3 = (1/3)|\pi^2 - \pi + 1|_3 \le 1/3 < 1$, so $|\pi|_3 < 1$. Therefore $|\pi^2 - \pi + 1|_3 = 1$ by the ultrametric inequality, so $|\pi|_3^3 = 1/3$, which implies $|\pi|_3 = 1/\sqrt[3]{3}$. Here $1/\sqrt[3]{3}$ is a real number: absolute values live in $\mathbf{R}$, not in a 3-adic field.

It can be shown that the closed unit ball in $\mathbf{Q}_3(\sqrt[3]{2})$, which is $\{y \in \mathbf{Q}_3(\sqrt[3]{2}) : |y|_3 \le 1\}$, equals $\mathbf{Z}_3[\sqrt[3]{2}]$. We'll be using this later.

In $\mathbf{Z}[\sqrt[3]{2}]$, the unit $u = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ has inverse $v = \sqrt[3]{2} - 1$, so by working with powers of v we can reformulate Theorem 2.1 as follows: for $x, y \in \mathbf{Z}$, $x^3 - 2y^3 = 1$ if and only if $x - y\sqrt[3]{2} = v^n$ for some $n \in \mathbf{Z}$. We want to find the integers n such that v^n written in the $\mathbf{Q}_3$-basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ has $\sqrt[3]{4}$-coefficient equal to 0. We expect the only such n are $n = 0$ (so $(x, y) = (1, 0)$) and $n = 1$ (so $(x, y) = (-1, -1)$). To prove this, we will 3-adically interpolate the powers of v in $\mathbf{Q}_3(\sqrt[3]{2})$ and use Strassmann's theorem.

To interpolate powers a^n where a is in a p-adic field, we need $|a - 1|_p < 1$. Using Example 5.1 in the field $\mathbf{Q}_3(\sqrt[3]{2})$,

$$v = \sqrt[3]{2} - 1 = \pi - 2 = 1 + (\pi - 3)$$

and $|\pi - 3|_3 = \max(1/\sqrt[3]{3}, 1/3) = 1/\sqrt[3]{3} < 1$, so $|v - 1|_3 = |\pi - 3|_3 < 1$. Thus there is a 3-adically continuous function

$$v^x = \sum_{k \ge 0} (v - 1)^k \binom{x}{k}$$

where $x \in \mathbf{Z}_3$. However, v^x is *not* a 3-adic analytic function $\mathbf{Z}_3 \to \mathbf{Q}_3(\sqrt[3]{2})$. When $|a - 1|_p < 1$, the condition for $a^x = \sum_{k \ge 0} (a - 1)^k \binom{x}{k}$ to be p-adic analytic in x, not just p-adically continuous in x, is that $|a - 1|_p < (1/p)^{1/(p-1)}$. For our example, where $a = v$ in $\mathbf{Q}_3(\sqrt[3]{2})$,

$|a-1|_3 = |v-1|_3 = |\pi - 3|_3 = (1/3)^{1/3} > (1/3)^{1/2}$. Taking a 3rd power of v will improve the situation:

$$(5.1)\quad v^3 = (\sqrt[3]{2}-1)^3 = 2-3\sqrt[3]{4}+3\sqrt[3]{2}-1 = 1+3(\sqrt[3]{2}-\sqrt[3]{4}) = 1-3\sqrt[3]{2}v \Longrightarrow |v^3-1|_3 = \frac{1}{3}.$$

Therefore $(v^3)^x$ is 3-adic analytic in x, so we'll look at the powers v^n with n restricted to a congruence class mod 3: For $r \in \{0,1,2\}$, set $f_r(x) = v^r(v^3)^x$ where $x \in \mathbf{Z}_3$. This is 3-adic analytic in x, and for $m \in \mathbf{Z}$ we have $f_r(m) = v^r(v^3)^m = v^{3m+r}$.

We will study v^n for $n \in \mathbf{Z}$ by studying the three 3-adic analytic functions $f_r \colon \mathbf{Z}_3 \to \mathbf{Q}_3(\sqrt[3]{2})$, which each interpolate one of the sequences v^{3m+r} (r being fixed). Write $f_r(x)$ as a power series in x:

$$(5.2)\qquad f_r(x) = v^r(v^3)^x = v^r e^{x\log(v^3)} = v^r \sum_{k\geq 0} \frac{(\log(v^3))^k}{k!} x^k.$$

Write $(\log(v^3))^k/k!$ in terms of its coefficients in the $\mathbf{Q}_3$-basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ of $\mathbf{Q}_3(\sqrt[3]{2})$:

$$\frac{(\log(v^3))^k}{k!} = a_k + b_k\sqrt[3]{2} + c_k\sqrt[3]{4},$$

where $a_k, b_k, c_k \in \mathbf{Q}_3$. Plugging this into (5.2),

$$\begin{aligned} f_r(x) &= v^r \sum_{k\geq 0}(a_k + b_k\sqrt[3]{2} + c_k\sqrt[3]{4})x^k \\ &= v^r \sum_{k\geq 0}\left(a_k x^k + b_k x^k\sqrt[3]{2} + c_k x^k\sqrt[3]{4}\right) \\ &= v^r\left(\left(\sum_{k\geq 0} a_k x^k\right) + \left(\sum_{k\geq 0} b_k x^k\right)\sqrt[3]{2} + \left(\sum_{k\geq 0} c_k x^k\right)\sqrt[3]{4}\right). \end{aligned}$$

(In $\mathbf{Q}_3(\sqrt[3]{2})$, a sequence tends to 0 if and only if its 3 sequences of coefficients in the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ each tend to 0 in $\mathbf{Q}_3$. That justifies splitting up the power series into a sum of three power series multiplied by the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.) Since v^r is either 1, $-1+\sqrt[3]{2}$, or $1-2\sqrt[3]{2}+\sqrt[3]{4}$, the coefficients of $f_r(x)$ in the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ are each 3-adic analytic functions. Therefore $f_r(x) \in \mathbf{Q}_3 + \mathbf{Q}_3\sqrt[3]{2}$ for an x if and only if its $\sqrt[3]{4}$-coefficient is 0, which is equivalent to the vanishing of a 3-adic analytic function $\mathbf{Z}_3 \to \mathbf{Q}_3$ at x.

Since $|v^3-1|_3 = 1/3$, in the 3-adic power series

$$(v^3)^x = e^{x\log(v^3)} = 1 + (\log(v^3))x + \sum_{k\geq 2}\frac{(\log(v^3))^k}{k!}x^k$$

for $x \in \mathbf{Z}_3$, we have $|\log(v^3)|_3 = |v^3-1|_3 = 1/3$, so the coefficient of x^k is divisible by 9 when $k \geq 2$. Therefore

$$(5.3)\qquad (v^3)^x = 1 + (\log(v^3))x + 9x^2 g(x)$$

where $g(x)$ is a power series converging on $\mathbf{Z}_3$ with coefficients in $\mathbf{Q}_3(\sqrt[3]{2})$ of absolute value at most 1 that tend to 0. Also

$$\log(v^3) = (v^3-1) + \sum_{k\geq 2}(-1)^{k-1}\frac{(v^3-1)^k}{k},$$

and $|v^3-1|_3 = 1/3 \Rightarrow |(v^3-1)^k/k|_3 \leq 1/9$ for $k \geq 2$, so $\log(v^3) \equiv v^3 - 1 \bmod 9$. Plugging this into (5.3),

$$(v^3)^x = 1 + (v^3-1)x + 9xh(x),$$

where $h(x)$ is a power series converging on $\mathbf{Z}_3$ with coefficients in $\mathbf{Q}_3(\sqrt[3]{2})$ of absolute value at most 1 that tend to 0. Since $\{y \in \mathbf{Q}_3(\sqrt[3]{2}) : |y|_3 \leq 1\} = \mathbf{Z}_3[\sqrt[3]{2}]$, which was mentioned earlier, the coefficients of $h(x)$ are all in $\mathbf{Z}_3[\sqrt[3]{2}]$. From (5.1), $v^3 - 1 = 3(\sqrt[3]{2} - \sqrt[3]{4})$, so

$$(v^3)^x = 1 + 3(\sqrt[3]{2} - \sqrt[3]{4})x + 9xh(x) = 1 + 3x\sqrt[3]{2} - 3x\sqrt[3]{4} + 9xh(x). \tag{5.4}$$

We will use (5.4) to bound the number of zeros in $\mathbf{Z}_3$ of the $\sqrt[3]{4}$-coefficient of the function $f_r(x) = v^r(v^3)^x$ when $r = 0$, 1, and 2.

Case 1: $r = 0$.

By (5.4), the $\sqrt[3]{4}$-coefficient of the power series for $f_0(x) = (v^3)^x$ is $-3x + 9xk_0(x)$ for a power series $k_0(x)$ on $\mathbf{Z}_3$ with $\mathbf{Z}_3$-coefficients that tend to 0. By Strassmann's theorem, $-3x + 9xk_0(x)$ has at most one zero in $\mathbf{Z}_3$. The choice $x = 0$ works, so it is the only zero in $\mathbf{Z}_3$.

Case 2: $r = 1$.

Since $f_1(x) = v(v^3)^x$, multiply (5.4) by v:

$$\begin{aligned} v(1 + 3x\sqrt[3]{2} - 3x\sqrt[3]{4} + 9xh(x)) &= (\sqrt[3]{2} - 1)(1 + 3x\sqrt[3]{2} - 3x\sqrt[3]{4} + 9xh(x)) \\ &= (-1 - 6x) + (1 - 3x)\sqrt[3]{2} + (6x)\sqrt[3]{4} + 9vxh(x), \end{aligned}$$

so the $\sqrt[3]{4}$-coefficient of the power series for $f_1(x)$ is $6x + 9xk_1(x)$ for a power series $k_1(x)$ on $\mathbf{Z}_3$ with $\mathbf{Z}_3$-coefficients that tend to 0. By Strassmann's theorem, $6x + 9xk_1(x)$ has at most one zero in $\mathbf{Z}_3$. The choice $x = 0$ works, so it is the only zero in $\mathbf{Z}_3$.

Case 3: $r = 2$.

Since $f_2(x) = v^2(v^3)^x$, multiply (5.4) by v^2:

$$\begin{aligned} v^2(1 + 3x\sqrt[3]{2} - 3x\sqrt[3]{4} + 9xh(x)) &= (\sqrt[3]{2} - 1)^2(1 + 3x\sqrt[3]{2} - 3x\sqrt[3]{4} + 9xh(x)) \\ &= (1 - 2\sqrt[3]{2} + \sqrt[3]{4})(1 + 3x\sqrt[3]{2} - 3x\sqrt[3]{4} + 9xh(x)) \\ &= (1 + 18x) + (-2 - 3x)\sqrt[3]{2} + (1 - 9x)\sqrt[3]{4} + 9v^2xh(x), \end{aligned}$$

so the $\sqrt[3]{4}$-coefficient of the power series for $f_2(x)$ is $1 - 9xk_2(x)$ for a power series $k_2(x)$ on $\mathbf{Z}_3$ with $\mathbf{Z}_3$-coefficients that tend to 0. By Strassmann's theorem, $1 - 9xk_2(x)$ has no zero in $\mathbf{Z}_3$.

From all three cases, $f_0(x)$ and $f_1(x)$ each have a zero in $\mathbf{Z}_3$ only at $x = 0$ and $f_2(x)$ has no zero in $\mathbf{Z}_3$. That implies the only (r, x) with $r \in \{0, 1, 2\}$ and $x \in \mathbf{Z}_3$ such that $v^r(v^3)^x$ has its $\sqrt[3]{4}$-coefficient equal to 0 are $(r, x) = (0, 0)$ and $(1, 0)$, so $3m + x$ is 0 and 1. Therefore the only positive units in $\mathbf{Z}[\sqrt[3]{2}]$ with $\sqrt[3]{4}$-coefficient 0 are $v^0 = 1$ and $v^1 = v = -1 + \sqrt[3]{2}$, which proves Theorem 1.3.

Appendix A. Thue's theorem

In this appendix we describe a different approach to the integral solutions of $x^3 - dy^3 = 1$, which historically was the original method and it goes back to Thue.

Theorem A.1 (Thue, 1909)**.** *Let d be a nonzero integer. For each nonzero $m \in \mathbf{Z}$, the equation $x^3 - dy^3 = m$ has finitely many integral solutions (x, y).*

Thue's actual theorem is a general finiteness theorem for integral solutions of certain two-variable polynomial equations $f(x, y) = m$ where $\deg f \geq 3$. We focus on the special case $f(x, y) = x^3 - dy^3$ for simplicity.

Proof. If $y = 0$ then $x^3 = m$, which has at most one solution for x, so we can now assume $y \neq 0$.

If d is a perfect cube in $\mathbf{Z}$, say $d = c^3$, then $x^3 - (cy)^3 = m$, so $(x - cy)(x^2 + cxy + c^2y^2) = m$. This makes $x - cy$ a factor of m. For each factor f, $x = cy + f$, so $(cy + f)^3 - dy^3 = m$. This equation simplifies to $(3c^2f)y^2 + (3cf^2)y + (f^3 - m) = 0$ since $c^3 = d$, and this quadratic equation has at most two solutions y for each f. Thus $x^3 - dy^3 = m$ has finitely many integral solutions if d is a perfect cube.

Now suppose d is not a perfect cube, so $\sqrt[3]{d}$ is irrational in $\mathbf{R}$. Factor $x^3 - dy^3$ as $(x - \sqrt[3]{d}y)(x - \sqrt[3]{d}\omega y)(x - \sqrt[3]{d}\omega^2 y)$, so

$$x^3 - dy^3 = m \Longrightarrow \left(\frac{x}{y} - \sqrt[3]{d}\right)\left(\frac{x}{y} - \sqrt[3]{d}\omega\right)\left(\frac{x}{y} - \sqrt[3]{d}\omega^2\right) = \frac{m}{y^3}.$$

Taking absolute values,

$$\left|\frac{x}{y} - \sqrt[3]{d}\right|\left|\frac{x}{y} - \sqrt[3]{d}\omega\right|\left|\frac{x}{y} - \sqrt[3]{d}\omega^2\right| = \frac{|m|}{|y|^3}.$$

On the left side, the second and third factors have positive lower bounds since x/y does not interact with the imaginary parts of $\sqrt[3]{d}\omega = \sqrt[3]{d}(-1/2 + \sqrt{3}i/2)$ and $\sqrt[3]{d}\omega^2 = \sqrt[3]{d}(-1/2 - \sqrt{3}i/2)$, so

$$\left|\frac{x}{y} - \sqrt[3]{d}\right|\frac{3\sqrt[3]{d}^2}{4} \leq \frac{|m|}{|y|^3}.$$

Thus

$$\left|\frac{x}{y} - \sqrt[3]{d}\right| \leq \frac{(4/3)|m|/\sqrt[3]{d}^2}{|y|^3} = \frac{K}{|y|^3},$$

where $K = (4/3)|m|/\sqrt[3]{d}^2$ depends on d and m but not on x or y.

Thue proved that for every $\varepsilon > 0$ and real algebraic irrational α of degree $n \geq 3$, there is $C = C_{\alpha,\varepsilon} > 0$ such that $|x/y - \alpha| \geq C/|y|^{n/2+1+\varepsilon}$ for all rational x/y. Taking $\alpha = \sqrt[3]{d}$, so $n = 3$, the exponent $n/2 + 1 + \varepsilon = 2.5 + \varepsilon$ is less than 3 if $\varepsilon < 1/2$. In this case, if $x^3 - dy^3 = m$ then $C/|y|^{2.5+\varepsilon} \leq |x/y - \sqrt[3]{d}| \leq K/|y|^3$, so $|y|^{.5-\varepsilon} \leq K/C$, which has finitely many solutions in y. For each y there is at most one x such that $x^3 - dy^3 = m$, so the equation $x^3 - dy^3 = m$ has finitely many integral solutions. $\square$

Thue's proof does not give upper bounds on the magnitude of $|x|$ or $|y|$ in an integral solution of $x^3 - dy^3 = m$ (when d is not a perfect cube) since the constant $C_{\alpha,\varepsilon}$ at the end of the proof is not explicit. Therefore Thue's work is fundamentally ineffective: it proved an equation has finitely many solutions in $\mathbf{Z}$ but gives no method of finding all the solutions in $\mathbf{Z}$. Decades later, work of Baker and Coates on linear forms in logarithms led to upper bounds on $|x|$ and $|y|$ that are explicit, but the size of the bounds in terms of $|d|$ and $|m|$ often makes them impractical. The p-adic method leads to more practical bounds when it can be applied.

References

[1] J. W. S. Cassels, "Local Fields," Cambridge Univ. Press, 1986.

[2] B. N. Delaunay, La solution générale de l'équation $X^3\rho + Y^3 = 1$, Comptes Rendus Acad. Sci. Paris **162** (1916), 150–151. Online at https://www.biodiversitylibrary.org/item/30710#page/156/mode/1up.[5]

[3] A. Fröhlich and M. J. Taylor, "Algebraic Number Theory," Cambridge Univ. Press, 1993.

[4] L. Euler, "Elements of Algebra," 1770. English translation online at http://www.17centurymaths.com/contents/euleralgebra.htm.

[5] W. J. Leveque, "Topics in Number Theory, Volume II," Addison-Wesley, 1956.

[6] T. Nagell, Solution complète de quelques équations cubiques à deux indéterminées, J. Math. Pures et Appl. **4** (1925), 209–270. Online at http://sites.mathdoc.fr/JMPA/PDF/JMPA_1925_9_4_A6_0.pdf.

[7] N. P. Smart, "The Algorithmic Resolution of Diophantine Equations," Cambridge Univ. Press, 1998.

[5]This is a short announcement of the result. Details were given earlier in several papers in Russian. See papers 37, 38, 39, and 40 at http://www.mathnet.ru/php/person.phtml?personid=25811&option_lang=eng.