AN EXAMPLE OF DESCENT BY EULER

KEITH CONRAD

As an illustration of the technique of descent where the equation has a few rational solutions, we discuss the following theorem of Euler [2, Theorem 10].

Theorem 1 (Euler, 1738)**.** *The only rational solutions to* $y^2 = x^3 + 1$ *are* $(-1, 0)$*,* $(0, \pm 1)$*, and* $(2, \pm 3)$*.*

Proof. Our proof is an elaboration on the sketch in [3, Sect. 5].

Suppose we have a rational solution (x, y). Since $y^2 \geq 0$, $x^3 + 1 = (x + 1)(x^2 - x + 1)$, and $x^2 - x + 1 = (x - 1/2)^2 + 3/4 > 0$, we must have $x \geq -1$. When $x = -1$, $y = 0$. From now on take $x > -1$.

Write $x = a/b$ where $(a, b) = 1$ and $b > 0$. From $x > -1$ we get $a + b > 0$. Since

$$x^3 + 1 = \left(\frac{a}{b}\right)^3 + 1 = \frac{b(a^3 + b^3)}{b^4},$$

$x^3 + 1$ is a rational square precisely when $b(a^3 + b^3)$ is a rational square, necessarily an integral square. To think about how $b(a^3 + b^3)$ could be a square, we will factor $a^3 + b^3$, hoping to get relatively prime factors:

$$b(a^3 + b^3) = b(a + b)(a^2 - ab + b^2).$$

What are common divisors of the three factors on the right? Since $(a, b) = 1$, b is relatively prime to $a + b$ and to $a^2 - ab + b^2$. What about $(a + b, a^2 - ab + b^2)$? Since $a^2 - ab + b^2 = (a+b)^2 - 3ab$, $(a+b, a^2-ab+b^2) = (a+b, -3ab)$ is either 1 or 3. We have $(a+b, a^2-ab+b^2) = 3$ if and only if $3|(a+b)$. Our calculations are hinting that we should be keeping track of $a+b$ and not just a and b, so let's give $a + b$ a name. Set $c = a + b$, so

$$b(a + b)(a^2 - ab + b^2) = bc(c^2 - 3bc + 3b^2).$$

Our task is to figure out when this can be a square in $\mathbf{Z}$. We know b is relatively prime to c and to $c^2 - 3bc + 3b^2$ and $(c, c^2 - 3bc + 3b^2) = (c, 3)$.

<u>Case 1</u>: $(3, c) = 1$. Now all three of b, c, and $c^2 - 3bc + 3b^2$ are pairwise relatively prime. All are positive (complete the square on $c^2 - 3bc + 3b^2$ to check this), so their product is a square only when each is a square. We will see later that, under these conditions, $b = c = 1$. Since $c = a + b$, we get $a = 0$ and therefore $(x, y) = (0, \pm 1)$.

<u>Case 2</u>: $3|c$. Write $c = 3d$, so from $(b, c) = 1$ we get $(b, 3) = 1$ and $(b, d) = 1$. Therefore

$$bc(c^2 - 3bc + 3b^2) = 9bd(3d^2 - 3bd + b^2) = 9db(b^2 - 3db + 3d^2).$$

For this to be an integral square, the square factor 9 doesn't matter, so we want to know when $db(b^2 - 3db + 3d^2)$ is a square in $\mathbf{Z}$. This is exactly the same situation as in Case 1, since $(b, d) = 1$ and $(3, b) = 1$. Therefore, granting the way Case 1 is claimed to turn out, we must have $b = d = 1$, so $c = 3d = 3$. Since $c = a + b$, $a = c - b = 2$ and $x = a/b = 2$, meaning $(x, y) = (2, \pm 3)$.

It remains to complete the analysis of Case 1: if $u, v \in \mathbf{Z}^+$ satisfy $u = \square$, $v = \square$, $u^2 - 3uv + 3v^2 = \square$, $(u, v) = 1$, and $(3, u) = 1$, then $u = v = 1$. We will prove this by descent.

Write

$$u^2 - 3uv + 3v^2 = w^2. \tag{1}$$

Since $(3, u) = 1$, also $(3, w) = 1$. We have a choice of sign on w. Since $u, w \not\equiv 0 \bmod 3$ we may *pick the sign so that* $w \equiv -u \bmod 3$.

Now pick $r \in \mathbf{Q}$ so that $u + rv = w$. That is, $r = (w - u)/v$. Since our sign convention on w forces $w - u \equiv 2w \not\equiv 0 \bmod 3$, $r \neq 0$. Write r in reduced form as $r = m/n$, where $n > 0$. Then $m|(w - u)$ and $n|v$, so $(3, m) = 1$.

Rewrite (1) using r:

$$u^2 - 3uv + 3v^2 = (u + rv)^2 = u^2 + 2ruv + r^2v^2,$$

so

$$(3 - r^2)v^2 = (2r + 3)uv.$$

The left side is not zero, so $2r + 3 \neq 0$. Collecting the r terms on one side and the u and v terms on the other,

$$\frac{u}{v} = \frac{3 - r^2}{2r + 3} = \frac{3 - (m/n)^2}{2(m/n) + 3} = \frac{3n^2 - m^2}{n(2m + 3n)}.$$

Let's show this last fraction is in reduced form. Since $(m, n) = 1$, n is prime to $3n^2 - m^2$. To show $(3n^2 - m^2, 2m + 3n) = 1$ we argue by contradiction. If some prime p divides $3n^2 - m^2$ and $2m + 3n$ then $m^2 \equiv 3n^2 \bmod p$ and $2m \equiv -3n \bmod p$. Squaring the second congruence and comparing it with the first gives $4m^2 \equiv 3m^2 \bmod p$ and $12n^2 \equiv 9n^2 \bmod p$. Thus $m^2 \equiv 0 \bmod p$ and $3n^2 \equiv 0 \bmod p$. Since $(m, n) = 1$, we get $p|m$ and $p = 3$, but $(3, m) = 1$. This is a contradiction.

Since u/v and $(3n^2 - m^2)/(n(2m + 3n))$ are equal and in reduced form, the numerators and denominators match up to the same sign:

$$u = \varepsilon(3n^2 - m^2), \quad v = \varepsilon n(2m + 3n)$$

for some $\varepsilon = \pm 1$. Reducing the first equation modulo 3, $u \equiv -\varepsilon m^2 \equiv -\varepsilon \bmod 3$. By hypothesis $u = \square$ in $\mathbf{Z}$, so $\varepsilon = -1$ since $-1 \bmod 3$ is not a square. Having identified ε,

$$u = m^2 - 3n^2, \quad v = -n(2m + 3n).$$

Since u and v are squares, we write $m^2 - 3n^2 = k^2$ for some integer k. Then $k \not\equiv 0 \bmod 3$. We are free to choose the sign on k. *Pick the sign so that* $k \equiv -m \bmod 3$.

Now choose $s \in \mathbf{Q}$ so that $m + sn = k$. That is, $s = (k - m)/n$. From our sign convention on k, $k - m \equiv 2k \not\equiv 0 \bmod 3$, so $s \neq 0$. Write s in reduced form as $s = u'/v'$, where $v' > 0$. Then $u'|(k - m)$ and $v'|n$, so $(3, u') = 1$. (Our choice of notation u' and v' is deliberate. They will be the pair to replace u and v in the descent step.)

Since $m^2 - 3n^2 = k^2 = (m + sn)^2 = m^2 + 2mns + s^2n^2$, $2mns = -(3 + s^2)n^2$. Collecting the s-terms on one side,

$$\frac{2m}{n} = -\frac{3 + s^2}{s}.$$

Now $v = -n(2m+3n) = -n^2(2m/n+3)$, so

$$\begin{aligned} v &= -n^2\left(-\frac{3+s^2}{s}+3\right) \\ &= n^2\left(\frac{s^2-3s+3}{s}\right) \\ &= n^2\frac{u'^2-3u'v'+3v'^2}{u'v'}. \end{aligned}$$

Since $v = \square$ in $\mathbf{Z}$, multiplying through by $(u'v')^2$ shows

$$u'v'(u'^2-3u'v'+3v'^2) = \square. \tag{2}$$

Since $(u',v') = 1$ and $(3,u') = 1$, u' and v' are both relatively prime to $u'^2-3u'v'+3v'^2$. Since $v' > 0$ and $u'^2-3u'v'+3v'^2 = (u'-(3/2)v')^2+(3/4)v'^2 > 0$, from (2) we must have $u' > 0$. The three terms on the left side of (2) are positive are pairwise relatively prime, so each is a square:

$$u' = \square, \quad v' = \square, \quad u'^2-3u'v'+3v'^2 = \square.$$

Now all the hypotheses on u and v have been checked on u' and v'. Let's find a sense in which the pair u' and v' is smaller than the pair u and v.

Since $n|v$ and

$$\frac{v}{n} = \frac{n(u'^2-3u'v'+3v'^2)}{u'v'},$$

we have $u'v'|n$ because u' and v' are prime to $u'^2-3u'v'+3v'^2$. Therefore $u'v'|v$, so from positivity $0 < u'v' \le v$, which implies $0 < v' \le v$.

As long as $v' < v$ we can repeat this construction, getting u'' and v'' with $0 < v'' \le v'$, and so on. This can't continue forever, so at some point we will have $v = v'$, where now we write u and v for the pair that occur at the step where the construction doesn't produce a smaller solution. Since $u'v'|n$ and $n|v'$, from $v = v'$ we get $v' = n$ and $u' = 1$.

Now

$$s = \frac{k-m}{n} = \frac{u'}{v'} = \frac{1}{n},$$

so $k = m+1$. Then $m^2-3n^2 = k^2 = m^2+2m+1$, so $2m+1 = -3n^2$. Then

$$n = v = -n(2m+3n) \Longrightarrow 2m+3n = -1 \Longrightarrow 2m+1 = -3n,$$

so $-3n^2 = -3n$. Since $n \neq 0$, $n = 1$ and therefore $v' = n = 1$. That means $s = 1$ and $2m+1 = -3$, so $m = -2$ and $u = m^2-3n^2 = 4-3 = 1$.

We have proved that at some point this iterative construction of smaller pairs (measuring size by the size of v) will have to lead to the pair $(1,1)$. We also showed that at the step before we reached $(1,1)$, the pair was also $(1,1)$. Since $(1,1)$ only lifts back to $(1,1)$, the only possible choice for u and v is $u = 1$ and $v = 1$. $\square$

Corollary 2. *The only rational solution to the equation $x^3+y^3 = 2$ is $(1,1)$ and the only rational solutions to $a^3-2b^3 = 1$ are $(1,0)$ and $(-1,-1)$.*

Proof. Suppose (x,y) is a rational solution of $x^3+y^3 = 2$, so x and y are both nonzero. Then the pair

$$(u,v) = \left(\frac{2x}{y^2}, 1-\frac{4}{y^3}\right)$$

satisfies $v^2 = u^3 + 1$, as a simple check confirms. Since u are v are both nonzero, we must have $(u, v) = (2, \pm 3)$ by Theorem 1. Therefore $x = y^2$ and $1 - 4/y^3 = \pm 3$. In the second equation the + sign leads to $y^3 = -2$, which is impossible. The − sign leads to $y^3 = 1$, so $y = 1$ and then $x = y^2 = 1$.

If $a^3 - 2b^3 = 1$ with rational a and b, and $b \neq 0$, then $2 = (a/b)^3 + (-1/b)^3$. Therefore $a/b = 1$ and $-1/b = 1$, making $b = -1$ and $a = b = -1$. If instead $b = 0$ then of course $a = 1$. □

Remark 3. To prove Theorem 1 for solutions in $\mathbf{Z}$ rather than in $\mathbf{Q}$ does not make things much easier. That is, proving the *integral* solutions to $y^2 = x^3 + 1$ are $(-1, 0)$, $(0, \pm 1)$, and $(2, \pm 3)$ is not simple. Let's show this is equivalent to the *integral* solutions to $a^3 - 2b^3 = 1$ being $(1, 0)$ and $(-1, -1)$.

- Suppose the integral solutions to $y^2 = x^3 + 1$ are the five known examples. Then if $a^3 - 2b^3 = 1$ in $\mathbf{Z}$, the pair $(x, y) = (2ab, 4b^3 + 1)$ satisfies $y^2 = x^3 + 1$ with $y \equiv 1 \bmod 4$, so $(2ab, 4b^3 + 1) = (0, 1)$ or $(2, -3)$ and therefore $(a, b) = (1, 0)$ or $(-1, -1)$.
- Suppose the integral solutions to $a^3 - 2b^3 = 1$ are $(1, 0)$ and $(-1, -1)$. Then if $y^2 = x^3 + 1$ in $\mathbf{Z}$, arguments with unique factorization in $\mathbf{Z}$ imply $(x, y) = (-1, 0)$ if y is even. For odd y, choose the sign on y to make $y \equiv 1 \bmod 4$. Then it can be shown with unique factorization in $\mathbf{Z}$ that $(y + 1)/2$ and $(y - 1)/4$ are both cubes: $(y + 1)/2 = a^3$ and $(y - 1)/4 = b^3$,[1] so $y = 2a^3 - 1 = 4b^3 + 1$, which implies $a^3 - 2b^3 = 1$. Setting $(a, b) = (1, 0)$ and $(-1, -1)$ we get $y = 1$ and -3. If $y = 1$ then $x^3 = y^2 - 1 = 0$ so $(x, y) = (0, 1)$, and if $y = -3$ the $x^3 = y^2 - 1 = 8$ so $(x, y) = (2, -3)$. Recalling we had adjusted the sign on y to force $y \equiv 1 \bmod 4$, allowing sign changes gives us $(x, y) = (0, -1)$ and $(2, 3)$ too.

For comparison to $x^3 + y^3 = 2$, the equation $x^3 + y^3 = 6$ has no integral solutions, but it has infinitely many rational solutions, the smallest one being $(17/21, 37/21)$.

The equation $x^3 + y^3 = 9$ has only two integral solutions, the obvious ones: $(1, 2)$ and $(2, 1)$. A rational solution is $(20/7, -17/7)$, with $y < 0$. If you want a non-integral rational solution (x, y) with $x > 0$ and $y > 0$, then you have to deal with fractions having very large numerators and denominators. The positive rational solution to $x^3 + y^3 = 9$ besides $(1, 2)$ and $(2, 1)$ with smallest denominator is

$$\left(\frac{415280564497}{348671682660}, \frac{676702467503}{348671682660}\right) \approx (1.191036, 1.940801)$$

Here is an interesting application of Corollary 2. There are infinitely many 3-term arithmetic progressions of perfect squares, with the simplest being 1, 24, and 49 What about 3-term arithmetic progressions of perfect cubes? Well, there are two trivial constructions: n^3, n^3, n^3 and $(-n)^3, 0^3, n^3$.

Corollary 4. *A 3-term arithmetic progressions of nonzero cubes in* $\mathbf{Z}$ *has all terms equal.*

Proof. Say the progression is a^3, b^3, c^3, with $a^3 \leq b^3 \leq c^3$. As an arithmetic progression, $b^3 - a^3 = c^3 - b^3$, so $2b^3 = a^3 + c^3$. Since $b \neq 0$, $2 = (a/b)^3 + (c/b)^3$. By Corollary 2, $a/b = 1$ and $c/b = 1$, so $a = b = c$. □

[1]See Example 3.6 in `https://kconrad.math.uconn.edu/blurbs/gradnumthy/mordelleqn1.pdf` for details of these arguments involving unique factorization in $\mathbf{Z}$ when y is even or odd.

What about higher powers? A 3-term arithmetic progression of nth powers in $\mathbf{Z}$ corresponds to an integral solution of the equation $x^n + y^n = 2z^n$. It can be proved that any such solution has all terms equal or one term equal to 0. This is proved by the same techniques used to prove Fermat's Last Theorem. See [1] and [4].

References

[1] H. Darmon and L. Merel, "Winding quotients and some variants of Fermat's last theorem," J. Reine Angew. Math. **490** (1997), 81–100.

[2] L. Euler, *Theorematum quorundam arithmeticorum demonstrationes*, Comm. Acad. Sci. Petrop. **10** (1738), 125–146. English translation online at https://scholarlycommons.pacific.edu/euler-works/98/.

[3] F. Lemmermeyer, "A note on Pépin's counterexamples to the Hasse principle for curves of genus 1," Abh. Math. Sem. Hamburg **69** (1999), 335–345. Online at http://www.fen.bilkent.edu.tr/∼franz/publ.html.

[4] K. Ribet, "On the Equation $a^p + 2^\alpha b^p + c^p = 0$," Acta Arith. **79** (1997), 7–16.