5.B. Sums and differences of cubes

In the main notes for this unit we mentioned a result in Diophantus' writings involving sums and differences of cubes. Specifically, the result states that

if a and b are positive rational numbers such that $a > b$ (hence $a^3 > b^3$), then there are positive rational numbers c and d such that

$$a^3 \; - \; b^3 \quad = \quad c^3 \; + \; d^3 \; .$$

Since it is not particularly easy to find a proof of this result in undergraduate level texts, we shall give one here.

PRELIMINARY REDUCTION. The following is extremely useful for simplifying the algebra in the proof.

> *If the result is true when $a = r > 1$ and $b = 1$, then it is true for all a and b such that $a/b = r$.*

If we set $c = a/b$, then $c > 1$. If we know that $c^3 - 1 = u^3 + v^3$ for suitable rational numbers u and v, it follows that

$$a^3 \; - \; b^3 \quad = \quad (bu)^3 \; + \; (bv)^3$$

and thus the special case implies the general case.

PROOF WHEN $a > \sqrt[3]{2}$ AND $b = 1$. We would like to find rational numbers t and n such that

$$(a - t)^3 \; + \; (nt - 1)^3 \quad = \quad a^3 \; - \; 1$$

where both $a - t$ and $nt - 1$ are positive. If we expand the left hand side of the displayed equation we obtain

$$a^3 - 3a^2t + 3at^2 - t^3 + n^3t^3 - 3n^2t^2 + 3nt - 1$$

and if we subtract $a^3 - 1$ from both sides of the displayed equation we then obtain the following equation in n and t:

$$(n^3 - 1)t^3 \; + \; (3a - 3n^2)t^2 \; + \; (3n - 3a^2)t \quad = \quad 0$$

This is a polynomial in n and t; the trick to solving it here will be to look for solutions in which the coefficient of t is equal to zero; in other words, we are interested in solutions for which $n = a^2$. In this case the equation reduces to

$$(a^6 - 1)t^3 \; + \; (3a - 3a^4)t^2 \quad = \quad 0$$

and the roots of this polynomial are zero and

$$t \quad = \quad \frac{3a^4 - 3a}{a^6 - 1} \quad = \quad \frac{3a}{a^3 + 1} \; .$$

Note that the right hand side is nonzero because $a > 1$.

Conversely, direct substitution and retracing the algebra in the previous paragraph show that

$$(a-t)^3 \;+\; (a^2t-1)^3 \;\;=\;\; a^3 \;-\; 1$$

so the only remaining issue is to determine whether $a - t$ and $a^2t - 1$ are both positive.

By the preceding formula for t we have

$$a \;-\; t \;\;=\;\; \frac{a^4 - 2a}{a^3 + 1}$$

and the right hand side is clearly positive if $a > \sqrt[3]{2}$. On the other hand, we also have

$$a^2t \;-\; 1 \;\;=\;\; \frac{2a^3 - 1}{a^3 + 1}$$

and this is positive provided $a > 1$. Therefore we have proven Diophantus' result when $a > \sqrt[3]{2}$.

WHAT HAPPENS WHEN $1 < a < \sqrt[3]{2}$ AND $b = 1$. In this case we still have the equation

$$(a-t)^3 \;+\; (a^2t-1)^3 \;\;=\;\; a^3 \;-\; 1$$

but now $(a - t)$ is negative while $(a^2t - 1)$ is positive. If we take

$$c \;\;=\;\; \frac{a^2t - 1}{t - a}$$

then the numerator and denominator of c are positive and it follows that

$$a^3 \;-\; 1 \;\;=\;\; (t-a)^3\big(c^3 \;-\; 1\big)$$

so that $c^3 - 1$ is positive. In fact, if we somehow know that $c > \sqrt[3]{2}$, then by the previously settled case we may write $c^3 - 1 = p^3 + q^3$ for suitable positive rational numbers p and q, and it will then follow that

$$a^3 \;-\; 1 \;\;=\;\; [(t-a)p]^3 \;+\; [(t-a)q]^3$$

proving the result in such cases. We shall use this idea to set up an induction argument. The crucial question involves the behavior of the function

$$c(a) \;\;=\;\; \frac{a^2t - 1}{t - a} \;\;=\;\; \frac{2a^3 - 1}{a(2 - a^3)}$$

when $1 < a < \sqrt[3]{2}$. Specifically, here is the main step:

CLAIM. *There is a strictly decreasing sequence of real numbers*

$$\sqrt[3]{2} \;\;=\;\; x_0 \;\;>\;\; x_1 \;\;\cdots\;\; > \;\; 1$$

such that the limit of the sequence is equal to 1 *and for all* $k > 0$ *we have*

$$x_k \;\;\leq\;\; a \;\;<\;\; \sqrt[3]{2} \qquad \Longrightarrow \qquad x_{k-1} \;\;<\;\; c(a)\ .$$

Suppose that the claim is true. We have seen that Diophantus' result is true for $a \geq x_0$, and the preceding discussion shows that if the result is true for $a \geq x_0$ then it is also true for $a \geq x_1$. Proceeding similarly, we see that if the result is true for $a \geq x_{k-1}$ then it is true for $a \geq x_k$, and therefore by induction it will follow that the result is true when $a \geq x_n$ for some nonnegative integer n. Since the sequence is decreasing and its limit is equal to 1, we know that for each $a > 1$ there is some n such that $a > x_n$, and thus it will follow that Diophantus' result will be true for all $a > 1$.

PROOF OF THE CLAIM. We shall prove the claim by using results from calculus to study the behavior of the function $c(a)$ on the half open interval $[0, \sqrt[3]{2})$. Note first that this function is positive valued on the given interval with $a(1) = 1$, and the line $x = \sqrt[3]{2}$ is a vertical asymptote at the right hand point of the interval under consideration. Standard formulas from calculus immediately yield the following formula for $c'(a)$:

$$c'(a) \quad = \quad \frac{(2a - a^4)6a^3 - (2a^3 - 1)(2 - 4a^3)}{a^2(2 - a^3)^2} \quad = \quad \frac{6a^4}{a^2(2 - a^3} \quad - \quad \frac{(2a^3 - 1)2}{a^2(2 - a^3)}$$

and since $a^4 > a^3$ when $a > 1$ the right hand side implies

$$c'(a) \quad > \quad \frac{6a^3}{a^2(2 - a^3)} \quad - \quad \frac{4a^3 - 2}{a^2(2 - a^3)} \quad = \quad \frac{2a^3}{a^2(2 - a^3)} \quad + \quad \frac{2}{a^2(2 - a^3)} \quad =$$

$$\frac{2a}{(2 - a^3)} \quad + \quad \frac{2}{a^2(2 - a^3)} \ .$$

Note that this expression is always positive if $1 \leq a < \sqrt[3]{2}$. The first summand of the right hand side is increasing for these values of a because it is a product of two functions that are increasing over this interval. Furthermore, the second summand is also increasing because the derivative of the denominator is negative for $a \geq 1$ (hence the denominator is strictly decreasing, which means the function itself is strictly increasing). The value of the right hand side is equal to 2 if $a = 1$, and therefore we conclude that $c'(a) \geq 2$ for $1 \leq a < \sqrt[3]{2}$. By the Mean Value Theorem, for these values of a we have $c(a) \ - \ 1 \ \ \geq \ \ 2 \cdot (a - 1)$. In particular, if we define x_n recursively by $x_0 = \sqrt[3]{2}$ and

$$x_{n+1} \quad = \quad \frac{1 + x_n}{2}$$

then it follows that $1 < x_{n+1} < x_n$ for all n and also

$$c(x_{n+1}) \ - \ 1 \quad \geq \quad 2 \cdot (x_{n+1} - 1) \quad = \quad x_n \ - \ 1$$

so that $c(x_{n+1}) \geq x_n$, and since c is strictly increasing it follows that $t > x_{n+1}$ implies $c(t) > x_n$.

It only remains to show that $\lim_{n\to\infty} \ x_n = 1$. This will follow immediately if we can show that

$$x_n \quad = \quad \left(\frac{1}{2}\right)^n \cdot \left(\sqrt[3]{2} \ - \ 1\right) \ + \ 1$$

for all n. By definition this is true for $n = 0$. Suppose now that the formula is true for x_n; we need to show that it is also true for x_{n+1}. Using the recursive definition we have

$$x_{n+1} \quad = \quad \frac{1}{2} \cdot (1 + x_n) \quad = \quad \frac{1}{2} \ + \ \left(\frac{1}{2}\right)^{n+1} \cdot \left(\sqrt[3]{2} \ - \ 1\right) \ + \ \frac{1}{2} \quad = \quad \left(\frac{1}{2}\right)^{n+1} \cdot \left(\sqrt[3]{2} \ - \ 1\right) \ + \ 1$$

and hence the formula is valid for x_{n+1}. This completes the proof of the claim, and by previous comments it also completes the proof of Diophantus' result.■