SELMER'S EXAMPLE

KEITH CONRAD

1. Introduction

Selmer's cubic is $3x^3 + 4y^3 + 5z^3$. It is a famous example of an irreducible polynomial that has no nontrivial rational zero (that is, no rational zero other than $(0, 0, 0)$), but it has a nontrivial real and p-adic zero for all p.

Theorem 1 (Selmer [4])**.** *The equation $3x^3 + 4y^3 + 5z^3 = 0$ has only the solution $(0, 0, 0)$ over $\mathbf{Q}$, but it has a nonzero solution over $\mathbf{R}$ and every $\mathbf{Q}_p$.*

We will first prove there is a nontrivial zero in each completion, relying for the most part on Hensel's lemma, and then use algebraic number theory to show there is no zero over $\mathbf{Q}$ other than $(0, 0, 0)$.

2. Local solutions

There is obviously a nonzero solution in $\mathbf{R}$. To show there is a solution besides $(0, 0, 0)$ in each $\mathbf{Q}_p$ we follow a method I learned from Kevin Buzzard. The basic idea is to show there is a nonzero solution modulo p and then lift that solution p-adically by Hensel's lemma. We will separately treat the cases $p = 3$, $p = 5$, and $p \neq 3$ or 5.

To find a 3-adic solution, set $x = 0$ and $z = -1$, making the equation $4y^3 - 5 = 0$, or $y^3 = 5/4$. Although $5/4 \equiv -1 \bmod 9$ and -1 is a 3-adic cube, this congruence modulo 9 isn't sharp enough to conclude by Hensel's lemma that $5/4$ is a 3-adic cube: to use Hensel's lemma (in the form $|f(\alpha)|_3 < |f'(\alpha)|_3^2$), we seek an $\alpha \in \mathbf{Z}_3^\times$ such that $|\alpha^3 - 5/4|_3 < 1/9$, i.e., $\alpha^3 \equiv 5/4 \bmod 27$. The choice $\alpha = 2$ works, so $5/4$ is a 3-adic cube and we can solve Selmer's equation in $\mathbf{Q}_3$ as $(0, y, -1)$ where $y^3 = 5/4$ in $\mathbf{Z}_3$.

If $p \neq 3$ and the p-adic integer a is a nonzero cube mod p then a is a cube in $\mathbf{Z}_p^\times$ by Hensel's lemma for $X^3 - a$. In particular, for $p = 5$, set $x = 1$ and $z = 0$ to make Selmer's equation $3 + 4y^3 = 0$, or $y^3 = -3/4$. Since $-3/4 \equiv 3 \equiv 2^3 \bmod 5$, by Hensel's lemma for $X^3 + 3/4$ with approximate solution 2 we see that $-3/4$ is a 5-adic cube. We get a 5-adic solution to Selmer's equation as $(1, y, 0)$ where $y^3 = -3/4$ in $\mathbf{Z}_5$.

From now on let p be a prime other than 3 or 5 (this includes allowing $p = 2$). Then $3, 5 \not\equiv 0 \bmod p$. We are going to look at the group $(\mathbf{Z}/(p))^\times$, which is *cyclic* of order $p - 1$. What proportion of the group is filled up by cubes?

- If $p \equiv 1 \bmod 3$ then the cubes in $(\mathbf{Z}/(p))^\times$ are a subgroup of index 3.
- If $p \not\equiv 1 \bmod 3$ then $(3, p - 1) = 1$, so every number in $(\mathbf{Z}/(p))^\times$ is a cube.

If 3 mod p is a cube then 3 is a cube in $\mathbf{Z}_p$ by Hensel's lemma for $X^3 - 3$, so we can solve Selmer's equation as $(x, 1, -1)$ where $x^3 = 1/3$ in $\mathbf{Q}_p$.

If 3 mod p is not a cube then not all numbers in $(\mathbf{Z}/(p))^\times$ are cubes. Thus $p \equiv 1 \bmod 3$, so the nonzero cubes mod p are a subgroup of $(\mathbf{Z}/(p))^\times$ that has index 3 and coset representatives $\{1, 3, 9\}$: for every $a \not\equiv 0 \bmod p$ we have $a \equiv b^3, 3b^3$, or $9b^3 \bmod p$ for some $b \not\equiv 0 \bmod p$. We will apply this with $a = 5$.

- If $5 \equiv b^3 \bmod p$ then 5 is a cube in $\mathbf{Z}_p$ by Hensel's lemma for $X^3 - 5$, and we can solve Selmer's equation as $(-y, y, -1)$ where $y^3 = 5$ in $\mathbf{Z}_p$.
- If $5 \equiv 3b^3 \bmod p$ then $5/3$ is a cube in $\mathbf{Z}_p$ by Hensel's lemma and we can solve Selmer's equation as $(x, 0, -1)$ where $x^3 = 5/3$.
- If $5 \equiv 9b^3 \bmod p$ then $5 \cdot 3 = 15$ is a cube in $\mathbf{Z}_p$ by Hensel's lemma and we can solve Selmer's equation as $(3t, 5, -7)$ where $t^3 = 15$. That is, $3a^3 + 4b^3 = 5c^3$ where $a = 3t$, $b = 5$, and $c = 7$.

This completes the proof that Selmer's equation has local solutions everywhere.

3. No global solutions

To prove $3x^3 + 4y^3 + 5z^3 = 0$ has no rational solution besides $(0, 0, 0)$, assume there is a rational solution (x, y, z). Multiplying through by 2 and rearranging terms, we get $(2y)^3 + 6x^3 = 10(-z)^3$. We will show the only rational solution to the equation

$$X^3 + 6Y^3 = 10Z^3 \tag{3.1}$$

is $(0, 0, 0)$, which implies the only rational solution to Selmer's equation is $(0, 0, 0)$.

By clearing denominators in (3.1), we can assume that X, Y, and Z are integers. They are not all 0, so in fact *none* are 0 since the coefficient ratios $6, 10$, and $10/6$ are not cubes in $\mathbf{Q}$. If a prime p divides two of X, Y, or Z then it also divides the third since the coefficients 6 and 10 in (3.1) aren't divisible by the cube of a prime. Then we can divide through all the terms in (3.1) by p^3 to get a smaller integral solution of the same equation. Hence without loss of generality X, Y, and Z are pairwise relatively prime. Since 6 and 10 are each even, necessarily $\boxed{X \text{ is even}}$. If either Y or Z were also even then both would be even (since 6 and 10 are each divisible by 2 just once), but X, Y, and Z can't all be even. Thus $\boxed{Y \text{ and } Z \text{ are both odd}}$. We can also conclude from (3.1) that $\boxed{X \text{ and } Z \text{ are not divisible by } 3}$ and $\boxed{X \text{ and } Y \text{ are not divisible by } 5}$.

Factor the left side of (3.1) in $\mathbf{Z}[\sqrt[3]{6}]$: writing $\alpha = \sqrt[3]{6}$, (3.1) is equivalent to

$$(X + Y\alpha)(X^2 - XY\alpha + Y^2\alpha^2) = 10Z^3. \tag{3.2}$$

Claim 1: $\mathbf{Z}[\alpha]$ is the ring of integers in $\mathbf{Q}[\alpha]$.

Proof of claim. For non-cube integers d,

$$\operatorname{disc}(\mathbf{Z}[\sqrt[3]{d}]) = -27d^2 = [\mathcal{O}_{\mathbf{Q}(\sqrt[3]{d})} : \mathbf{Z}[\sqrt[3]{d}]]^2 \operatorname{disc}(\mathcal{O}_{\mathbf{Q}(\sqrt[3]{d})}),$$

so the index of $\mathbf{Z}[\sqrt[3]{d}]$ in the ring of integers of $\mathbf{Q}(\sqrt[3]{d})$ divides $3d$. In particular, the index of $\mathbf{Z}[\sqrt[3]{6}]$ in the integers of $\mathbf{Q}(\sqrt[3]{6})$ divides 18. Since $T^3 - 6$ is Eisenstein at 2 and 3, the index of $\mathbf{Z}[\sqrt[3]{6}]$ in the integers of $\mathbf{Q}(\sqrt[3]{6})$ is not divisible by 2 or 3, so the index is 1.

Passing from (3.2) to an equation of principal ideals in $\mathbf{Z}[\alpha]$,

$$(X + Y\alpha)(X^2 - XY\alpha + Y^2\alpha^2) = (10)(Z)^3. \tag{3.3}$$

To derive information about the prime ideal factorization of $(X + Y\alpha)$ from this equation, we need to determine how the ideal (10) factors.

The way a prime p factors in $\mathbf{Z}[\alpha] \cong \mathbf{Z}[T]/(T^3 - 6)$ matches how $T^3 - 6$ factors mod p. The following table shows how the ideals (2) and (5) decompose, so $(10) = \mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{25}$.

p	$T^3 - 6 \bmod p$	(p)
2	T^3	$\mathfrak{p}_2^3$
5	$(T-1)(T^2+T+1)$	$\mathfrak{p}_5\mathfrak{p}_{25}$

Writing N for the field norm $\mathrm{N}_{\mathbf{Q}(\alpha)/\mathbf{Q}}$, we have for each integer k that $\mathrm{N}(\alpha+k) = k^3+6$. The table below collects a few norm values.

k	-2	-1	0	1	2	4
k^3+6	-2	5	6	7	14	70

Since there are unique prime ideals of norm 2 and 5, $\boxed{\mathfrak{p}_2 = (\alpha-2) \text{ and } \mathfrak{p}_5 = (\alpha-1)}$. We will use the other norm values later.

Claim 2: The principal ideal $(X+Y\alpha)$ decomposes in $\mathbf{Z}[\alpha]$ as

$$(X+Y\alpha) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{b}^3 = (\alpha-2)(\alpha-1)\mathfrak{b}^3 \tag{3.4}$$

for some ideal $\mathfrak{b}$.

Proof of claim. (This proof, which involves a careful analysis of ideal factorizations in $\mathbf{Z}[\alpha]$, takes a fair bit of work and could be skipped to see how the claim gets used first.)

We will show the only common prime ideal factor of $(X+Y\alpha)$ and $(X^2-XY\alpha+\alpha^2)$ is $\mathfrak{p}_2$. Since $\mathrm{N}(\alpha) = 6$, the ideal (α) is divisible by $\mathfrak{p}_2$, so X being even makes $(X+Y\alpha)$ and $(X^2-XY\alpha+Y^2\alpha^2)$ both divisible by $\mathfrak{p}_2$.

In the other direction, let $\mathfrak{p}$ be a prime ideal such that

$$\mathfrak{p} \mid (X+Y\alpha) \quad \text{and} \quad \mathfrak{p} \mid (X^2-XY\alpha+Y^2\alpha^2), \tag{3.5}$$

so

$$X+Y\alpha \equiv 0 \bmod \mathfrak{p} \quad \text{and} \quad X^2-XY\alpha+Y^2\alpha^2 \equiv 0 \bmod \mathfrak{p}.$$

Since $X^2-XY\alpha+Y^2\alpha^2 = (X+Y\alpha)^2 - 3XY\alpha$, we get $3XY\alpha \equiv 0 \bmod \mathfrak{p}$. Thus $\mathfrak{p}$ divides one of the ideals (3), (X), (Y), or (α).

- If $\mathfrak{p} \mid (3)$ then the norm of $\mathfrak{p}$ is a power of 3. Since $\mathfrak{p}$ divides $(Z)^3$ by equation (3.3), taking norms implies Z is divisible by 3, which is false.
- If $\mathfrak{p} \mid (X)$ then $Y\alpha \equiv 0 \bmod \mathfrak{p}$ since $X+Y\alpha \equiv 0 \bmod \mathfrak{p}$, which implies $\mathfrak{p} \mid (Y)(\alpha)$. From relative primality of X and Y, $\mathfrak{p}$ can't divide (Y) (otherwise X and Y would be divisible by whatever prime number $\mathfrak{p}$ divides), so $\mathfrak{p} \mid (\alpha)$.
- If $\mathfrak{p} \mid (Y)$ then $X \equiv 0 \bmod \mathfrak{p}$ since $X+Y\alpha \equiv 0 \bmod \mathfrak{p}$, but that means $\mathfrak{p} \mid (X)$, which contradicts the relative primality of X and Y.

The conclusion is that a prime ideal $\mathfrak{p}$ satisfying (3.5) is a factor of (α) and not a factor of the ideal (3). Since $(\alpha)^3 = (6) = (2)(3)$, $\mathfrak{p}$ must be a factor of the ideal (2), so $\mathfrak{p} = \mathfrak{p}_2$.

Any common ideal factor of the ideals on the left side of equation (3.3) is a power of $\mathfrak{p}_2$. How high a power can be a common divisor? Since X is even and Y is odd and (α) is divisible by $\mathfrak{p}_2$ just once, we have $X \equiv 0 \bmod \mathfrak{p}_2^3$, $Y\alpha \equiv 0 \bmod \mathfrak{p}_2$, and $Y\alpha \not\equiv 0 \bmod \mathfrak{p}_2^2$, so $(X+Y\alpha)$ is divisible by $\mathfrak{p}_2$ just once. Therefore

$$(X+Y\alpha) = \mathfrak{p}_2\mathfrak{c}, \quad (X^2-XY\alpha+Y^2\alpha^2) = \mathfrak{p}_2\mathfrak{c}'$$

where $\mathfrak{c}$ and $\mathfrak{c}'$ are relatively prime ideals in $\mathbf{Z}[\alpha]$ and $\mathfrak{p}_2$ doesn't divide $\mathfrak{c}$.

Plugging these factorizations into equation (3.3), $\mathfrak{p}_2^2\mathfrak{c}\mathfrak{c}' = (10)(Z)^3 = \mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{25}(Z)^3$, so $\mathfrak{p}_2$ is a factor of $\mathfrak{c}'$. Which of $\mathfrak{c}$ or $\mathfrak{c}'$ is divisible by $\mathfrak{p}_5$ and $\mathfrak{p}_{25}$?

From $X^3+6Y^3 = 10Z^3$ we get $X^3 \equiv (-Y)^3 \bmod 5$. Cubing is a bijection on $\mathbf{Z}/(5)$, so $X \equiv -Y \bmod 5$. Therefore $X+Y\alpha \equiv X+Y \equiv 0 \bmod \mathfrak{p}_5$, which means $\mathfrak{p}_5 \mid (X+Y\alpha)$. If $\mathfrak{p}_{25} \mid (X+Y\alpha)$ then $\mathfrak{p}_5\mathfrak{p}_{25} = (5)$ divides $(X+Y\alpha)$, so 5 is a factor of $X+Y\alpha$ in $\mathbf{Z}[\alpha]$, which implies X and Y are divisible by 5 in $\mathbf{Z}$, and that is false. Thus $\mathfrak{p}_{25}$ is not a factor of $(X+Y\alpha)$, so $\mathfrak{p}_{25}$ is a factor of $(X^2-XY\alpha+Y^2\alpha^2)$.

Write $\mathfrak{c} = \mathfrak{p}_5\mathfrak{m}$ and $\mathfrak{c}' = \mathfrak{p}_2\mathfrak{p}_{25}\mathfrak{m}'$. Then

$$(X + Y\alpha) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{m} \quad \text{and} \quad (X^2 - XY\alpha + Y^2\alpha^2) = \mathfrak{p}_2^2\mathfrak{p}_{25}\mathfrak{m}'.$$

Multiplying these together, we obtain $(X^3 + 6Y^3) = (10)\mathfrak{m}\mathfrak{m}'$ so $(10)(Z)^3 = (10)\mathfrak{m}\mathfrak{m}'$. The ideals $\mathfrak{m}$ and $\mathfrak{m}'$ are relatively prime since $\mathfrak{c}$ and $\mathfrak{c}'$ are relatively prime, so $\mathfrak{m}$ (as well as $\mathfrak{m}'$) must be a cube. This proves (3.4).

Claim 3: $\mathbf{Q}(\alpha)$ has class number 1.

Proof of claim. The Minkowski bound for $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt[3]{6})$ is

$$\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|\operatorname{disc}(\mathbf{Z}[\sqrt[3]{6}])|} = \frac{4}{\pi}\frac{6}{27}\sqrt{27 \cdot 6^2} = \frac{16\sqrt{3}}{\pi} \approx 8.82.$$

Therefore the class group is generated by the ideal classes of primes with norm at most 8. We have already seen that there is a unique prime ideal of norm 2, namely $\mathfrak{p}_2 = (\alpha - 2)$, and no prime ideal of norm 4 or 8 since $(2) = \mathfrak{p}_2^3$. To factor (3), from $T^3 - 6 \equiv T^3 \bmod 3$ we obtain $(3) = \mathfrak{p}_3^3$. Since $\mathrm{N}(\alpha) = 6$, we have $(\alpha) = \mathfrak{p}_2\mathfrak{p}_3 = (\alpha - 2)\mathfrak{p}_3$, so $\mathfrak{p}_3$ is principal. The only ideal of norm 5 is $\mathfrak{p}_5 = (\alpha - 1)$, which is principal. It remains to factor (7). Since $T^3 - 6 \equiv (T+1)(T+2)(T+4) \bmod 7$, we have $(7) = \mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7''$ where these prime ideals satisfy $\mathfrak{p}_7 \mid (\alpha + 1)$, $\mathfrak{p}_7' \mid (\alpha + 2)$, and $\mathfrak{p}_7'' \mid (\alpha + 4)$. From the table of norm values before Claim 2 we have $\mathrm{N}(\alpha + 1) = 7$, $\mathrm{N}(\alpha + 2) = 14$, and $\mathrm{N}(\alpha + 4) = 70$, so $(\alpha + 1) = \mathfrak{p}_7$, $(\alpha + 2) = \mathfrak{p}_2\mathfrak{p}_7'$, and $(\alpha + 4) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_7''$. Since $\mathfrak{p}_2$ and $\mathfrak{p}_5$ are principal, all the prime ideals of norm 7 are all principal. Thus the class number of $\mathbf{Q}(\alpha)$ is 1.

By Claim 3 the ideal $\mathfrak{b}$ in Claim 2 is principal, say $\mathfrak{b} = (\beta)$, so equation (3.4) leads to an equation of elements:

$$X + Y\alpha = (\alpha - 2)(\alpha - 1)\beta^3 u \tag{3.6}$$

for some unit u in $\mathbf{Z}[\alpha]$. In this equation the unit u only matters modulo multiplication by unit cubes since unit cubes can be absorbed into β.

Claim 4: The units in $\mathbf{Z}[\alpha]$ modulo unit cubes are represented by $(1 - 6\alpha + 3\alpha^2)^k$ for $k = 0, 1$, and 2.

Proof of claim. Since $\mathbf{Q}(\alpha)$ has $r_1 = 1$ and $r_2 = 1$ by Dirichlet's unit theorem $\mathbf{Z}[\alpha]^\times = \pm\varepsilon^{\mathbf{Z}}$ for some ε, so $\mathbf{Z}[\alpha]^\times/(\mathbf{Z}[\alpha]^\times)^3$ is cyclic of order 3. Therefore a unit that is not a cube generates the units modulo cubes. (That is, a non-identity element in a group of prime order is a generator.) To find a noncube unit, observe that $(2) = \mathfrak{p}_2^3 = (\alpha - 2)^3$, so

$$\frac{(\alpha - 2)^3}{2} = \frac{\alpha^3 - 6\alpha^2 + 12\alpha - 8}{2} = -1 + 6\alpha - 3\alpha^2 \approx -.00306$$

is a unit. Its negative $1 - 6\alpha + 3\alpha^2$ is also a unit. To check this is not a cube of a unit, we verify it is not a cube in a suitably chosen residue field. Specifically, the ideal $\mathfrak{p}_7 = (\alpha + 1)$ has norm 7 and in $\mathbf{Z}[\alpha]/\mathfrak{p}_7 \cong \mathbf{Z}/(7)$ we have

$$1 - 6\alpha + 3\alpha^2 \equiv 1 - 6(-1) + 3(1) = 10 \equiv 3 \bmod \mathfrak{p}_7,$$

and this is not a cube since 3 is not a cube in $\mathbf{Z}/(7)$.

Remark 1. The unit $1 - 6\alpha + 3\alpha^2$ is actually a generator of $\mathbf{Z}[\alpha]^\times$ (modulo ± 1), but that takes more effort to prove and Claim 4 is sufficient information for us about units in $\mathbf{Z}[\alpha]$.

Since

$$1 - 6\alpha + 3\alpha^2 = -\frac{(\alpha-2)^3}{2} = \frac{(2-\alpha)^3}{2},$$

by Claim 4 we can write u in equation (3.6) as $((2-\alpha)^3/2)^k v^3 = ((2-\alpha)^k v)^3/2^k$ where $v \in \mathbf{Z}[\alpha]^\times$ and k is 0, 1, or 2. Multiplying through equation (3.6) by 2^k, we absorb $((2-\alpha)^k v)^3$ into β^3 to get

$$2^k X + 2^k Y\alpha = (\alpha-2)(\alpha-1)\gamma^3 \tag{3.7}$$

for some $\gamma \in \mathbf{Z}[\alpha]$. Write $\gamma = A + B\alpha + C\alpha^2$, where A, B, and C are integers that are not all 0.

Compute $(\alpha-2)(\alpha-1)\gamma^3$ as a $\mathbf{Z}$-linear combination of 1, α, and α^2 and then equate the coefficients of α^2 on both sides of equation (3.7) to get

$$0 = A^3 + 6B^3 + 36C^3 + 36ABC - 9(A^2B + 6AC^2 + 6B^2C) + 6(AB^2 + A^2C + 6BC^2). \tag{3.8}$$

In this equation each term other than A^3 is a multiple of 3, so $0 \equiv A^3 \bmod 3$. Thus $3 \mid A$, which makes each term in (3.8) other than the second term $6B^3$ divisible by 9, so $0 \equiv 6B^3 \bmod 9$. That implies $3 \mid B$, which forces each term in (3.8) other than the third term $36C^3$ to be divisible by 27, so $0 \equiv 36C^3 \bmod 27$. Thus $3 \mid C$.

We have shown A, B, and C in (3.8) are each divisible by 3. The right side of (3.8) is homogeneous of degree 3 in A, B, and C, so we can remove a common factor of 27 from all the terms and obtain another equation (3.8) where A, B, and C are one-third as large. Repeating this infinitely often forces A, B, and C to equal 0, which is a contradiction. This completes the proof that Selmer's equation has no rational solution other than $(0,0,0)$.

Our treatment of Selmer's equation is based on [3, pp. 220–222], where the analogue of our equation (3.8) on the top of p. 222 has one incorrect coefficient on the right side.

Other examples of homogeneous cubics fitting the conditions of Selmer's theorem are

$$x^3 + 5y^3 + 12z^3, \quad x^3 + 4y^3 + 15z^3, \quad x^3 + 3y^3 + 20z^3, \quad x^3 + 3y^3 + 22z^3.$$

A different class of examples that are analyzed without algebraic number theory are in [1].

Remark 2. Just as counterexamples to unique factorization in number fields can acquire a positive interpretation as non-trivial elements in an ideal class group (that is, such phenomena are associated to non-principal ideals), Selmer's example has a positive interpretation: it represents a non-trivial element in the Tate-Shafarevich group of an elliptic curve over $\mathbf{Q}$, specifically the elliptic curve $x^3 + y^3 + 60z^3 = 0$. The lack of rational solutions besides $(0,0,0)$ to $3x^3 + 4y^3 + 5z^3 = 0$ can be proved more simply using the theory of elliptic curves instead of purely by algebraic number theory. See [2, pp. 86–87].

References

[1] W. Aitken and F. Lemmermeyer, Simple Counterexamples to the Local–Global Principle, at http://public.csusm.edu/aitken_html/m372/diophantine.pdf.

[2] J. W. S. Cassels, "Lectures on Elliptic Curves," Cambridge Univ. Press, Cambridge, 1991.

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

[4] E. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Mathematica **85** (1951), 203–362.