COUNTEREXAMPLE TO THE LOCAL–GLOBAL PRINCIPLE

KEITH CONRAD

The local–global principle, in its simplest form, is the idea that an equation over $\mathbf{Q}$ should have a rational solution if and only if it has solutions in each completion $\mathbf{Q}_v$. (More generally, the same idea can be formulated over any global field and its family of completions, not just $\mathbf{Q}$.) If the equation is homogeneous, so the zero solution is automatic, then one is interested in whether a *nonzero* (= not all coordinates are zero) rational solution exists if and only if there is a nonzero solution in each completion. The first strong piece of evidence in favor of the local–global principle comes from Hasse's work on quadratic forms, building on earlier work of Minkowski.

Theorem 1 (Hasse, 1921)**.** *If $Q(x_1, \ldots, x_n)$ is a quadratic form over $\mathbf{Q}$ then the equation $Q(x_1, \ldots, x_n) = 0$ has a nonzero solution over $\mathbf{Q}$ if and only if it has a nonzero solution over every $\mathbf{Q}_v$.*

The local–global principle is also true in other situations (*e.g.*, two central simple algebras over $\mathbf{Q}$ are isomorphic if and only if they are isomorphic over every $\mathbf{Q}_v$), but for higher-degree equations it need not hold. Selmer famously gave a counterexample to the local–global principle among cubic forms, and we will verify such an example as an illustration of techniques from algebraic number theory. For simpler counterexamples to the local–global principle, not requiring algebraic number theory, see [1].

Theorem 2 (Selmer, 1951)**.** *The equation $3x^3 + 4y^3 + 5z^3 = 0$ has only the zero solution over $\mathbf{Q}$, but there is a nonzero solution over every completion $\mathbf{Q}_v$.*

Proof. First we treat the local case. Over $\mathbf{Q}_\infty = \mathbf{R}$, it is obvious there is a solution besides $(0, 0, 0)$. To handle p-adic fields, roughly speaking the idea is to show there is a nonzero solution modulo p and then lift it p-adically by Hensel's lemma. We use Hensel's lemma to detect cubes. To show by Hensel's lemma that some $\alpha \in \mathbf{Z}_p^\times$ is a p-adic cube, we need to find a $\beta \in \mathbf{Z}_p^\times$ such that $|\beta^3 - \alpha|_p < |3\beta^2|_p^2 = |3|_p^2$. In particular, for $p \neq 3$ any element of $\mathbf{Z}_p^\times$ which is a cube modulo p is a cube in $\mathbf{Z}_p^\times$. In particular, when $p \equiv 2 \bmod 3$ every element of $\mathbf{Z}/(p)$ is a cube, so every element of $\mathbf{Z}_p^\times$ is a cube.

To get a 2-adic solution to Selmer's equation $3x^3 + 4y^3 + 5z^3 = 0$, set $x = 1$ and $y = 0$, making the equation $3 + 5z^3 = 0$, or $z^3 = -3/5$. Every element of $\mathbf{Z}_2^\times$ is a cube by Hensel's lemma, so there is a 2-adic choice for z.

For a 3-adic solution, set $x = 0$ and $y = 1$, making Selmer's equation $4 + 5z^3 = 0$, or $z^3 = -4/5$. Is $-4/5$ a cube in $\mathbf{Q}_3$? By Hensel's lemma, we seek a $\beta \in \mathbf{Z}_3^\times$ such that $|\beta^3 + 4/5|_3 < 1/9$. The choice $\beta = 1$ doesn't quite work, but the refinement $\beta = 1 + 9 = 10$ does: $|10^3 + 4/5|_3 = 1/27 < 1/9$. So $-4/5$ is a 3-adic cube and we can make a 3-adic choice for z.

For a 5-adic solution, set $x = 1$ and $z = 0$, making Selmer's equation $3 + 4y^3 = 0$, or $y^3 = -3/4$. Since $5 \equiv 2 \bmod 3$, every element of $\mathbf{Z}_5^\times$ is a cube, so $-3/4$ is a 5-adic cube.

Now let $p \geq 7$, so the coefficients 3, 4, and 5 are all p-adic units. When $p \equiv 2 \bmod 3$, so every element of $\mathbf{Z}_p^\times$ is a p-adic cube by Hensel's lemma, let $x = 1$ and $y = 0$. Now Selmer's equation is $3 + 5z^3 = 0$, which has a p-adic solution since $-3/5 \in \mathbf{Z}_p^\times = (\mathbf{Z}_p^\times)^3$.

When $p \equiv 1 \bmod 3$, not every element of $\mathbf{F}_p^\times$ is a cube (in fact, only $1/3$ of the nonzero numbers modulo p are cubes), so not every element of $\mathbf{Z}_p^\times$ is a cube and we need to take a different approach to solve Selmer's equation p-adically than we did for $p = 2$, 3, and 5. Using character sums over finite fields it can be shown [4, Thm. 5, p. 103] that for any prime $p \equiv 1 \bmod 3$ and $c_1, c_2, c_3 \in \mathbf{F}_p^\times$, the number N_p of solutions over $\mathbf{F}_p$ to the congruence $c_1x^3 + c_2y^3 + c_3z^3 \equiv 0 \bmod p$ satisfies

$$|N_p - p^2| \leq 2(p-1)\sqrt{p}.$$

There is always the solution $(0, 0, 0)$, so $N_p \geq 1$. Could $N_p = 1$? We will show it is not, by contradiction. If $N_p = 1$ then the above inequality becomes $p^2 - 1 \leq 2(p-1)\sqrt{p}$, so $p + 1 \leq 2\sqrt{p}$, which is the same as $(\sqrt{p} - 1)^2 \leq 0$. This is impossible for prime p, so in fact $N_p \geq 2$: there is a solution to $c_1x_0^3 + c_2y_0^3 + c_3z_0^3 \equiv 0 \bmod p$ with at least one of x_0, y_0, or z_0 being nonzero modulo p.

In particular, the congruence $3x_0^3 + 4y_0^3 + 5z_0^3 \equiv 0 \bmod p$ has a solution other than $(0, 0, 0)$ for any $p \equiv 1 \bmod 3$. Treating x_0, y_0, and z_0 as p-adic integers, at least one of them is in $\mathbf{Z}_p^\times$. If $x_0 \not\equiv 0 \bmod p$ then from

$$x_0^3 \equiv -\frac{4}{3}y_0^3 - \frac{5}{3}z_0^3 \bmod p$$

we obtain that $-(4/3)y_0^3 - (5/3)z_0^3$ is a nonzero cube modulo p, so by Hensel's lemma it is a p-adic cube: there is a solution to $x^3 = -(4/3)y_0^3 - (5/3)z_0^3$ with $x \in \mathbf{Z}_p^\times$, so $(x, y_0, z_0) \neq (0, 0, 0)$ is a p-adic solution to $3x^3 + 4y^3 + 5z^3 = 0$. A similar argument goes through if $y_0 \not\equiv 0 \bmod p$ or if $z_0 \not\equiv 0 \bmod p$.

This concludes the proof that Selmer's equation has solutions everywhere locally.

Now we turn to the global case: $3x^3 + 4y^3 + 5z^3 = 0$ has no rational solution besides $(0, 0, 0)$. Our proof is based on [3, pp. 220-222], with a few minor changes and (typographical) corrections.

If there is a rational solution to Selmer's equation besides $(0, 0, 0)$ then there is a rational solution besides $(0, 0, 0)$ to the cubic equation

$$a^3 + 6b^3 = 10c^3$$

(use $a = 2y$, $b = x$, and $c = -z$), and *vice-versa*. Assume we can solve $a^3 + 6b^3 = 10c^3$ with $(a, b, c) \neq (0, 0, 0)$. We will reach a contradiction.

Since 6, 10, and $10/6 = 5/2$ are not cubes in $\mathbf{Q}$, none of a, b, and c are 0. Clearing denominators, we may assume $(a, b, c) \in \mathbf{Z}^3$. Since 6 and 10 are cube-free, if any two of a, b, and c have a common prime factor p then so does the third. We can then remove the common p^3 throughout, so without loss of generality a, b, and c are *pairwise relatively prime*. In particular,

- b and c are odd since a is even,
- $(3, a) = 1$ and $(5, a) = 1$.

Let $K = \mathbf{Q}(\sqrt[3]{6})$, so $\mathrm{N}_{K/\mathbf{Q}}(a + b\sqrt[3]{6}) = a^3 + 6b^3$. Thus the equation $a^3 + 6b^3 = 10c^3$ is the same as

$$\mathrm{N}_{K/\mathbf{Q}}(a + b\sqrt[3]{6}) = 10c^3,$$

and in $\mathbf{Z}[\sqrt[3]{6}]$

$$(a+b\sqrt[3]{6})(a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36})=10c^3.$$

Step 1: $\mathcal{O}_K=\mathbf{Z}[\sqrt[3]{6}]$.

For any non-cube $d\in\mathbf{Z}$, $\operatorname{disc}(\mathbf{Z}[\sqrt[3]{d}])=-27d^2$, so $\operatorname{disc}(\mathbf{Z}[\sqrt[3]{6}])=-2^2\cdot 3^5$. Since X^3-6 is Eisenstein at 2 and 3, the index $[\mathcal{O}_K:\mathbf{Z}[\sqrt[3]{6}]]$ is not divisible by 2 or 3, so the index is 1.

Step 2: $h(K)=1$.

The Minkowski bound is

$$\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\operatorname{disc}(\mathbf{Z}[\sqrt[3]{6}])|}=\frac{32\sqrt{3}}{\pi}\approx 5.61.$$

A prime p factors in $\mathbf{Z}[\sqrt[3]{6}]$ the same way X^3-6 factors in $(\mathbf{Z}/p\mathbf{Z})[X]$. Therefore $(2)=\mathfrak{p}_2^3$, $(3)=\mathfrak{p}_3^3$, and $(5)=\mathfrak{p}_5\mathfrak{p}_{25}$. The class group is generated by $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_5$. Since

$$\mathrm{N}_{K/\mathbf{Q}}(2-\sqrt[3]{6})=2^3+6(-1)^3=2,\quad \mathrm{N}_{K/\mathbf{Q}}(1-\sqrt[3]{6})=1^3+6(-1)^3=-5,$$

we must have $\mathfrak{p}_2=(2-\sqrt[3]{6})$ and $\mathfrak{p}_5=(1-\sqrt[3]{6})$, so these ideals are principal. Since $\mathrm{N}(\sqrt[3]{6})=6$, we must have $(\sqrt[3]{6})=\mathfrak{p}_2\mathfrak{p}_3$, so $\mathfrak{p}_3$ is principal. Hence $h=1$.

Step 3: As ideals, $(a+b\sqrt[3]{6},a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36})=\mathfrak{p}_2$.

First, we observe that $\mathfrak{p}_2$ is a common factor of $a+b\sqrt[3]{6}$ and $a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{6}$ since $a,\sqrt[3]{6}\in\mathfrak{p}_2$.

Let $\mathfrak{p}$ be a common prime ideal factor of $(a+b\sqrt[3]{6})$ and $(a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36})$. We want to show $\mathfrak{p}=\mathfrak{p}_2$. In $\mathbf{Z}[\sqrt[3]{6}]/\mathfrak{p}$ we have $a\equiv -b\sqrt[3]{6}$, so

$$0\equiv a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36}\equiv 3b^2\sqrt[3]{36}\equiv 3a^2 \bmod \mathfrak{p}.$$

Thus $\mathfrak{p}|(3)(a)^2$ and $\mathfrak{p}|(3)(b)^2(\sqrt[3]{6})^2$. If $\mathfrak{p}|(3)$ then $\mathfrak{p}=\mathfrak{p}_3$, but then $\mathfrak{p}|(\sqrt[3]{6})$, so $a\equiv -b\sqrt[3]{6}\equiv 0 \bmod \mathfrak{p}_3$. This is not true, as a is not divisible by 3. Therefore $\mathfrak{p}\neq\mathfrak{p}_3$, so $\mathfrak{p}|(a)$ and $\mathfrak{p}|(b)^2\mathfrak{p}_2^2$. Since (a) and (b) are relatively prime, $\mathfrak{p}=\mathfrak{p}_2$.

Now we know $(a+b\sqrt[3]{6},a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36})$ is a power of $\mathfrak{p}_2$. To show it is the first power, we show $\mathfrak{p}_2^2$ doesn't divide $(a+b\sqrt[3]{6})$. If $\mathfrak{p}_2^2|(a+b\sqrt[3]{6})$, then taking ideal norms shows $4|(10c^3)$, so c is even. But c is odd. We are done with Step 3.

Step 4: As ideals, $(a+b\sqrt[3]{6})=\mathfrak{p}_2\mathfrak{p}_5\mathfrak{a}$ and $(a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36})=\mathfrak{p}_2^2\mathfrak{p}_{25}\mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime ideals.

We have

$$(a+b\sqrt[3]{6})(a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36})=(a^3+6b^3)=(10c^3)=(2)(5)(c)^3=\mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{25}(c)^3.$$

Previously we saw $\mathfrak{p}_2$ divides $(a+b\sqrt[3]{6})$ precisely once, so $\mathfrak{p}_2^2$ divides $(a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36})$. Modulo $\mathfrak{p}_5=(1-\sqrt[3]{6})$ we have $a+b\sqrt[3]{6}\equiv a+b$. From $a^3+6b^3=10c^3$, $a^3+b^3\equiv 0 \bmod 5$, so $a^3\equiv(-b)^3 \bmod 5$. Since cubing is injective on $\mathbf{Z}/(5)$, $a\equiv -b \bmod 5$. Therefore $a+b\sqrt[3]{6}\equiv 0 \bmod \mathfrak{p}_5$. Since $a+b\sqrt[3]{6}$ is not divisible by 5 in $\mathbf{Z}[\sqrt[3]{6}]$ (for instance, the coefficient a is not divisible by 5), $\mathfrak{p}_{25}$ doesn't divide $(a+b\sqrt[3]{6})$, so it must divide $(a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36})$. So far we know that $(a+b\sqrt[3]{6})$ is divisible by $\mathfrak{p}_2$ and $\mathfrak{p}_5$ while $(a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36})$ is divisible by $\mathfrak{p}_2^2$ and $\mathfrak{p}_{25}$, so we can write

$$(a+b\sqrt[3]{6})=\mathfrak{p}_2\mathfrak{p}_5\mathfrak{a},\quad (a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36})=\mathfrak{p}_2^2\mathfrak{p}_{25}\mathfrak{b}$$

for some ideals $\mathfrak{a}$ and $\mathfrak{b}$. (Multiplying the two equations, we get $(c)^3=\mathfrak{a}\mathfrak{b}$, which we will use later.) The ideals $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime since we know $(a+b\sqrt[3]{6},a^2-ab\sqrt[3]{6}+b^2\sqrt[3]{36})=\mathfrak{p}_2$ and we have already extracted a factor of $\mathfrak{p}_2$ from both principal ideals.

Step 5: There is a nonzero $\alpha \in \mathbf{Z}[\sqrt[3]{6}]$ such that $a + b\sqrt[3]{6}$ and $(2 - \sqrt[3]{6})(1 - \sqrt[3]{6})\alpha^3$ are unit multiples.

Since $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime and $\mathfrak{a}\mathfrak{b} = (c)^3$ is a cube, both $\mathfrak{a}$ and $\mathfrak{b}$ are cubes. The class number $h(K)$ is 1, so $\mathfrak{a} = (\alpha)^3$ for some nonzero $\alpha \in \mathbf{Z}[\sqrt[3]{6}]$. Therefore the ideal factorization $(a + b\sqrt[3]{6}) = \mathfrak{p}_2\mathfrak{p}_5(\alpha)^3 = (2 - \sqrt[3]{6})(1 - \sqrt[3]{6})(\alpha^3)$ implies the elements $a + b\sqrt[3]{6}$ and $(2 - \sqrt[3]{6})(1 - \sqrt[3]{6})\alpha^3$ are unit multiples of each other. Since α shows up through its cube and we have not pinned down α specifically, the unspecified unit factor only matters modulo cubes of units.

Step 6: Find representatives for the unit group $\mathbf{Z}[\sqrt[3]{6}]^\times$ modulo cubes.

Since $\mathbf{Q}(\sqrt[3]{6})$ has $r_1 = 1$ and $r_2 = 1$, the unit group has rank 1: $\mathbf{Z}[\sqrt[3]{6}]^\times = \pm\varepsilon^{\mathbf{Z}}$ for some ε, so $\mathbf{Z}[\sqrt[3]{6}]^\times/(\mathbf{Z}[\sqrt[3]{6}]^\times)^3$ is cyclic of order 3. Therefore any unit which is not a cube generates the units modulo cubes. To find a unit, we observe that $(2) = \mathfrak{p}_2^3 = (2 - \sqrt[3]{6})^3$, so the ratio

$$u := \frac{(2 - \sqrt[3]{6})^3}{2} = 1 - 6\sqrt[3]{6} + 3\sqrt[3]{36} \approx .00306$$

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

$$u = 1 - 6\sqrt[3]{6} + 3\sqrt[3]{36} \equiv 1 - 6(-1) + 3(1) = 10 \equiv 3 \bmod \mathfrak{p}_7,$$

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

Remark 1. It is true that u is a generator of the unit group (modulo ± 1), but that would take more effort to prove and what we did in Step 6 is all we need.

Step 7: Wrapping things up.

By Step 6, any unit in $\mathbf{Z}[\sqrt[3]{6}]$ is equal to 1, u, or u^2 modulo cubes, so after changing α in Step 5 by a unit factor if necessary we can write

$$a + b\sqrt[3]{6} = (2 - \sqrt[3]{6})(1 - \sqrt[3]{6})u^j\alpha^3, \quad j \in \{0, 1, 2\}.$$

Since $u = (2 - \sqrt[3]{6})^3/2$, multiplying by 2^j shows

$$2^j(a + b\sqrt[3]{6}) = (2 - \sqrt[3]{6})(1 - \sqrt[3]{6})\beta^3. \tag{1}$$

where $\beta = (2 - \sqrt[3]{6})^j\alpha$. The coefficient of $\sqrt[3]{36}$ on the left is 0. Writing $\beta = k + \ell\sqrt[3]{6} + m\sqrt[3]{36}$ with $k, \ell, m \in \mathbf{Z}$, equating coefficients of $\sqrt[3]{36}$ on both sides of (1) gives (after rather tedious algebra)

$$0 = k^3 + 6\ell^3 + 36m^3 + 36k\ell m + 2(3k\ell^2 + 3k^2m + 18\ell m^2) - 3(3k^2\ell + 18km^2 + 18\ell^2 m).$$

Reducing both sides modulo 3 shows $k^3 \equiv 0 \bmod 3$, so $3|k$. But then reducing both sides modulo 9 shows $6\ell^2 \equiv 0 \bmod 9$, so $3|\ell$. Finally, reducing both sides modulo 27 now implies $36m^2 \equiv 0 \bmod 27$, so $3|m$. Since the right side is homogeneous of degree 3, the common factor of 3 in k, ℓ, and m can be removed and then repeat the above reduction process again. This can be done *ad infinitum*, so $k = \ell = m = 0$, a contradiction. □

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 counterexample 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] K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," 2nd ed., Springer–Verlag, New York, 1990.

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