SOME EXCEPTIONS TO THE LOCAL-GLOBAL PRINCIPLE

LUIS MODES

ABSTRACT. We prove that the curve $3x^3+4y^3+5z^3=0$ does not satisfy the local-global principle, i.e. it has a nontrivial solution in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p, but it has no nontrivial solution in $\mathbb{Q}$, and introduce the ideas to show that neither does the family of curves $5x^3+9y^3+10z^3+12\left(\frac{t^2+82}{t^2+22}\right)^3(x+y+z)^3=0$.

1. INTRODUCTION

The local-global principle, also called the Hasse principle, is the idea that if a diophantine equation has a solution locally "for all the possible definitions of local", then it has a solution globally. As a more concrete example, we can say that a curve satisfies the local-global principle if the fact that it has solutions in $\mathbb{Q}_p$ for all primes $p \leq \infty$ implies that it also has solutions in $\mathbb{Q}$. Here, the solutions in the completions $\mathbb{Q}_p$ are the local solutions, and the solution in $\mathbb{Q}$ is the global solution. We have already seen an example of this. Namely, the Hasse-Minkowski Theorem.

Theorem 1.1 (Hasse-Minkowski)**.** *If $a,b,c \in \mathbb{Q}$, the equation $ax^2+by^2+cz^2=0$ has nontrivial solutions in $\mathbb{Q}$ if and only if it has nontrivial solutions in $\mathbb{Q}_p$ for all primes $p \leq \infty$.*

However, this remarkable principle does not always hold in general, as one's fear might have expected. In particular, we are going to show that the curve $3x^3+4y^3+5z^3=0$ does not satisfy the local-global principle. This curve is called Selmer's example, as Ernst Selmer proved in 1954 that this curve has a nontrivial solution in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p, but it has no nontrivial solution in $\mathbb{Q}$. Our main inspiration is Conrad's paper [1].

First, we use Hensel's lemma to show that this equation has a nontrivial solution in $\mathbb{Q}_p$ for each prime p. The case $p=\infty$ is clearly true. Then, we use algebraic number theory show that this equation does not have any solution in $\mathbb{Q}$.

Finally, we show the main ideas in the proof of the fact that the family of curves $5x^3+9y^3+10z^3+12\left(\frac{t^2+82}{t^2+22}\right)^3(x+y+z)^3=0$ does not satisfy the local-global principle either. This was proven by Bjorn Poonen in [2] for the sake of giving an explicit family of curves violating this principle. In fact, it was already known that several curves do not satisfy this principle, but finding an explicit family of examples was more challenging.

2. LOCAL SOLUTIONS TO SELMER'S EXAMPLE

Let us show that Selmer's example, the curve $3x^3+4y^3+5z^3=0$, has a solution in all the completions of $\mathbb{Q}$, namely $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes $p<\infty$. We are going to divide the proof in four cases: a solution in $\mathbb{R}$, a solution in $\mathbb{Q}_3$, a solution in $\mathbb{Q}_5$, and a solution in $\mathbb{Q}_p$, for $p \neq 3,5,\infty$.

First, let us show that there is a solution in $\mathbb{R}$. In fact, this is not hard to do. Take, for example, $(x,y,z)=\left(-\sqrt[3]{\frac{4}{3}},1,0\right)$. This clearly works. To show that there is a solution in $\mathbb{Q}_p$ for $p<\infty$, we are going to use the following version of Hensel's lemma:

Lemma 2.1 (Hensel's lemma)**.** *Let $f \in \mathbb{Z}_p[x]$, and suppose $|f(a)|_p < |f'(a)|_p^2$ for some $a \in \mathbb{Z}_p$. Then, there exists some $b \in \mathbb{Z}_p$ such that $f(b)=0$.*

A proof of this version of Hensel's lemma can be found in [3].

Now, let us show our curve has a solution in $\mathbb{Q}_3$. Consider the function $f(y) = 4y^3 - 5$, with derivative $f'(y) = 12y^2$. Note that, for $a = 2$,

$$|f(a)|_3 = |27|_3 = 3^{-3} < (3^{-1})^2 = |48|_3^2 = |f'(a)|_3^2 \tag{2.1}$$

Thus, by Hensel's lemma, there exists a $b \in \mathbb{Z}_3 \subseteq \mathbb{Q}_3$ such that $4b^3 - 5 = 0$. Hence, $(x, y, z) = (0, b, -1)$ is a solution for Selmer's example in $\mathbb{Q}_3$:

$$3x^3 + 4y^3 + 5z^3 = 0 + 4b^3 - 5 = 0 \tag{2.2}$$

Let us show our curve also has a solution in $\mathbb{Q}_5$. If $f(y) = 4y^3 + 3$, with derivative $f'(y) = 12y^2$, note that, for $a = 2$,

$$|f(a)|_5 = |35|_5 = 5^{-1} < 1^2 = |48|_5^2 = |f'(a)|_5^2 \tag{2.3}$$

Thus, by Hensel's lemma, there exists a $b \in \mathbb{Q}_5$ such that $4b^3 + 3 = 0$. Hence, $(x, y, z) = (1, b, 0)$ is a solution in $\mathbb{Q}_5$.

Finally, it remains to show there is also a solution for $\mathbb{Q}_p$ with $p \neq 3, 5, \infty$. Assume p is none of these primes. We will use the following lemma.

Lemma 2.2. *Let $(\mathbb{Z}/p\mathbb{Z})^{\times 3}$ be the set of cubes of $(\mathbb{Z}/p\mathbb{Z})^{\times}$. If $p \equiv 1 \bmod 3$, $(\mathbb{Z}/p\mathbb{Z})^{\times 3}$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^{\times}$ of index 3, and if $p \not\equiv 1 \bmod 3$, then $(\mathbb{Z}/p\mathbb{Z})^{\times 3} = (\mathbb{Z}/p\mathbb{Z})^{\times}$.*

Proof. As $(\mathbb{Z}/p\mathbb{Z})^{\times}$ is a cyclic group of order $p - 1$, there exists an element g of order $p - 1$ generating the group. Hence, as $g^{\gcd(3,p-1)}$ is a generator for $(\mathbb{Z}/p\mathbb{Z})^{\times 3}$, we get the desired result. □

Now, if 3 is a cube $\bmod p$, i.e. $a^3 = 3 \bmod p$, consider the function $f(x) = x^3 - 3$. By Hensel's lemma, as $|f(a)|_p < |f'(a)|_p^2$, we get $b \in \mathbb{Z}_p$ such that $b^3 - 3 = 0$, so $\left(\frac{1}{b}, 1, -1\right)$ is a solution in $\mathbb{Q}_p$ for Selmer's example.

On the other hand, if 3 is not a cube $\bmod p$, by Lemma 2.2 the only possibility is that $p \equiv 1 \bmod 3$, and that

$$(\mathbb{Z}/p\mathbb{Z})/(\mathbb{Z}/p\mathbb{Z})^{\times 3} = \{(\mathbb{Z}/p\mathbb{Z})^{\times 3}, 3(\mathbb{Z}/p\mathbb{Z})^{\times 3}, 9(\mathbb{Z}/p\mathbb{Z})^{\times 3}\} \tag{2.4}$$

because as 3 is not a cube, $1, 3, 9$ belong to distinct residue classes. Thus, depending on which residue class 5 mod p belongs to, we have three cases. If $5 \equiv c^3 \bmod p$ for some p, considering $a = c$ and $f(x) = x^3 - 5$, by Hensel's lemma, there exists $b \in \mathbb{Z}_p$ such that $b^3 - 5 = 0$, so $(-b, b, -1)$ is a solution in $\mathbb{Q}_p$ for Selmer's example. If $5 \equiv 3c^3 \bmod p$ for some p, considering $a = c$ and $f(x) = 3x^3 - 5$, by Hensel's lemma, there exists $b \in \mathbb{Z}_p$ such that $3b^3 - 5 = 0$, so $(b, 0, -1)$ is a solution in $\mathbb{Q}_p$ for Selmer's example. Finally, if $5 \equiv 9c^3 \bmod p$ for some p, considering $a = 3c$ and $f(x) = x^3 - 15$, by Hensel's lemma, there exists $b \in \mathbb{Z}_p$ such that $b^3 - 15 = 0$, so $(3b, 5, -7)$ is a solution in $\mathbb{Q}_p$ for Selmer's example:

$$3(3b)^3 + 4(5)^3 + 5(-7)^3 = 81b^3 + 500 - 1715 = 1215 - 1215 = 0 \tag{2.5}$$

Hence, this concludes our prove that the curve $3x^3 + 4y^3 + 5z^3 = 0$ has local solutions in $\mathbb{Q}_p$ for all $p \leq \infty$.

3. No global solutions to Selmer's Example

Now, let us prove that Selmer's example does not have any rational solution apart from $(0, 0, 0)$. First, note that the curve $3x^3 + 4y^3 + 5z^3 = 0$ is equivalent to the curve $X^3 + 6Y^3 = Z^3$. Indeed, by multiplying both sides of Selmer's example by 2 and rearranging, we get

$$(2y)^3 + 6x^3 = 10(-z)^3 \tag{3.1}$$

so we can make the substitution $X = 2y$, $Y = x$, and $Z = -z$. Also, as the resulting equation is still homogeneous, by multiplying everything by a suitable integer N^3, we can get rid of the denominators, and thus assume without loss of generality that X, Y, and Z are integers. Furthermore, we can also divide everything by $\gcd(X, Y, Z)$, so we can assume without loss of generality that X, Y, Z are relatively prime. Thus, our problem is equivalent to showing that the equation

$$X^3 + 6Y^3 = Z^3 \tag{3.2}$$

where X, Y, and Z are integers with $\gcd(X, Y, Z) = 1$ has no solutions apart from $(0, 0, 0)$. Our strategy will be to consider the prime factorization of the ideals of both sides of equation (3.2) in $\mathbb{Z}[\sqrt[3]{6}]$. In order to do this, we will invoke several claims. We will only prove some of them, but the complete proof of all can be found in [1]. First, if we let $\sqrt[3]{6} = \alpha$, we can factor (3.2) as

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

Claim 3.1. *$\mathbb{Z}[\alpha]$ is the ring of integers of $\mathbb{Q}(\alpha)$.*

Proof. Note that

$$\operatorname{disc}(\mathbb{Z}[\sqrt[3]{6}]) = -27 \cdot 6^2 = [\mathcal{O}_{\mathbb{Q}(\sqrt[3]{6})} : \mathbb{Z}[\sqrt[3]{6}]]^2 \operatorname{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt[3]{6})})$$

From here, $[\mathcal{O}_{\mathbb{Q}(\sqrt[3]{6})} : \mathbb{Z}[\sqrt[3]{6}]]^2$ divides $-27 \cdot 6^2 = -3^5 \cdot 2^2$, so we must have that $[\mathcal{O}_{\mathbb{Q}(\sqrt[3]{6})} : \mathbb{Z}[\sqrt[3]{6}]]$ divides $3^2 \cdot 2 = 18$. Now, as the polynomial $T^3 - 6$ is Eisenstein in 2 and 3, it follows that neither 2 nor 3 divide $[\mathcal{O}_{\mathbb{Q}(\sqrt[3]{6})} : \mathbb{Z}[\sqrt[3]{6}]]$. However, the only positive divisor of 18 not divisible by 2 or 3 is 1, so $[\mathcal{O}_{\mathbb{Q}(\sqrt[3]{6})} : \mathbb{Z}[\sqrt[3]{6}]] = 1$, and thus $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{6})} = \mathbb{Z}[\sqrt[3]{6}]$ as desired. □

By Claim 3.1, we can pass from the equation of elements (3.3) to the equation of ideals

$$(X + Y\alpha)(X^2 - XY\alpha + Y^2\alpha^2) = (10)(Z)^3 \tag{3.4}$$

Claim 3.2. *We can factor the ideal (10) as $(10) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_{25}$*

Proof. First, we factor (10) as $(10) = (2)(5)$. It remains to factor (2) and (5). For this, recall that $\mathbb{Z}[\sqrt[3]{6}] \cong \mathbb{Z}[T]/(T^3 - 6)$, so the factorization of p in $\mathbb{Z}[\sqrt[3]{6}]$ matches the factorization of $T^3 - 6 \bmod p$. Note that $T^3 - 6$ factors as $T^3 \bmod 2$ and factors as $(T - 1)(T^2 + T + 1) \bmod 5$. Hence, (2) factors as $\mathfrak{p}_2^3$ and (5) factors as $\mathfrak{p}_5\mathfrak{p}_{25}$, as desired. □

Claim 3.3. *$(X + Y\alpha) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{b}^3 = (\alpha - 1)(\alpha - 2)\mathfrak{b}^3$ for some ideal $\mathfrak{b}$.*

Sketch. Since there are the unique prime ideals of norm 2 and 5, we have that $\mathfrak{p}_2 = (\alpha - 2)$ and $\mathfrak{p}_5 = (\alpha - 1)$. Now, from (3.4) and Claim 3.2, after some work with ideals, we can deduce that $\mathfrak{p}_2$ and $\mathfrak{p}_5$ divide $(X + Y\alpha)$.

Claim 3.4. *$\mathbb{Z}[\alpha]$ is a principal ideal domain.*

Sketch. This is equivalent to proving that $\mathbb{Q}(\alpha)$ has class number 1. Note that the Minkowski bound for $\mathbb{Q}(\alpha)$ is

$$\left(\frac{4}{\pi}\right)^{r^2} \frac{n!}{n^n}\sqrt{|\operatorname{disc}(\mathbb{Z}[\sqrt[3]{6}])|} = \frac{4}{\pi} \cdot \frac{6}{27}\sqrt{27 \cdot 6^2} = \frac{16\sqrt{3}}{\pi} < 9$$

Thus, it suffices to check that the ideals with norm at most 8 are principal.

Claim 3.5. *The units if $\mathbb{Z}[\alpha]$ modulo units cubes are of the form $(1 - 6\alpha + 3\alpha^2)^k$ for $k = 0, 1$ or 2.*

Proof. As $r_1 = r_2 = 1$ for $\mathbb{Q}(\alpha)$, by Dirichlet's unit theorem, it follows that $\mathbb{Z}[\alpha]^\times$ is generated by $1 + 1 - 1 = 1$ element. In particular, it follows that $\mathbb{Z}[\alpha]^\times/\mathbb{Z}[\alpha]^{\times 3} \cong \mathbb{Z}/3\mathbb{Z}$. Thus, any unit that is not a

cube will be a generator for the group of units modulo cubes. In particular, consider the unit $1-6\alpha+3\alpha^2$. We can verify this is a unit because $(2)=\mathfrak{p}_2^3=(\alpha-2)^3$, $\alpha-2$ has norm 2, and

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

Furthermore, it is not a cube because it is not a cube $\mod 7$. Indeed, $\mathfrak{p}_7=(\alpha+1)$ and $\mathbb{Z}[\alpha]/\mathfrak{p}_7\cong\mathbb{Z}/(7)$, so $\alpha\equiv -1 \mod 7$, but then

$$1-6\alpha+3\alpha^2\equiv 1+6+3\equiv 3 \mod 7$$

and 3 is not a cube $\mod 7$. Hence, $1-6\alpha+3\alpha^2$ is a generator for $\mathbb{Z}[\alpha]^\times/\mathbb{Z}[\alpha]^{\times 3}$, so all the units modulo cubes have the form $(1-6\alpha+3\alpha^2)^k$ for $k=0,1$ or 2, as desired. □

Now, by Claim 3.3 and Claim 3.4, we can write $(X+Y\alpha)$ as $(X+Y\alpha)=(\alpha-1)(\alpha-2)(\beta)^3$. Now, as all of these are principal ideals, from this ideal equation we can recover the following equation of elements, where $u\in\mathbb{Z}[\alpha]^\times$:

$$X+Y\alpha=(\alpha-1)(\alpha-2)\beta^3u \tag{3.5}$$

Furthermore, as $1-6\alpha+3\alpha^2=\frac{(2-\alpha)^3}{2}$, by Claim 3.5, we can rewrite this as

$$X+Y\alpha=(\alpha-1)(\alpha-2)\beta^3\left(\frac{(2-\alpha)^3}{2}\right)^k v^3=(\alpha-1)(\alpha-2)\frac{(\beta v(2-\alpha)^k)^3}{2^k} \tag{3.6}$$

for some $v\in\mathbb{Z}[\alpha]^\times$. Now, by making $\gamma=\beta v(2-\alpha)^k$ and multiplying both sides of (3.6) by 2^k, we get

$$2^kX+2^kY\alpha=(\alpha-1)(\alpha-2)\gamma^3 \tag{3.7}$$

As $\gamma\in\mathbb{Z}[\alpha]$, we can write it as $\gamma=A+B\alpha+C\alpha^2$ for some $A,B,C\in\mathbb{Z}$. Plugging this into (3.7) and comparing the coefficients of α^2, we get that

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

Now, note that all the terms in the right hand side, except possibly A^3, are multiples of 3. Thus, we must have that $3\mid A^3$, that is, $3|A$. Now, if we plug $A=3A'$, we now get that all the terms, except possibly $6B^3$, are multiples of 9. This implies that $3\mid B$. Similarly, if we plug $B=3B'$, we see that all the terms, except possibly $36C^3$, are multiples of 27, so we must have that $3\mid C$. Thus, we have gotten that $3\mid A,B,C$, so dividing everything by 27, we get the same equation as (3.8), but with A',B',C' instead of A,B,C. Repeating this argument, we get that $3^N\mid A,B,C$ for all N, so $A=B=C=0$. However, plugging this in (3.7), we get that $X+Y\alpha=0$, which is possible if and only if $X=Y=0$. Hence, we get that the only solution for (3.2) is $(0,0,0)$, which implies that Selmer's example does not have any nontrivial solution in $\mathbb{Q}$, as desired.

Remark 3.6. For Claim 3.5, $1-6\alpha+3\alpha^2$ is actually a generator of the whole $\mathbb{Z}[\alpha]^\times$. However, proving this requires more effort, and Claim 3.5 was enough for our goal.

Remark 3.7. Finding exceptions to the local-global principle is not an easy task. In general, if there is a simple way to show that an equation does not have rational solutions, it is usually via an argument $\mod p$. However, failure $\mod p$ will precisely imply that there is no solution in $\mathbb{Q}_p$, so this is not an exception to the Hasse principle. Take, for example, the cubic equation $x^3+2y^3+4z^3=0$. In [5], it was shown through a simple argument that there were no solutions in $\mathbb{Q}$ because of failure $\mod 2$, but this also implies there is no solution in $\mathbb{Q}_2$.

Remark 3.8. With similar arguments, we can also prove that the curves $x^3+5y^3+12z^3$, $x^3+4y^3+15z^3$, $x^3+3y^3+20z^3$, and $x^3+3y^3+22z^3$ are exceptions to the local-global principle.

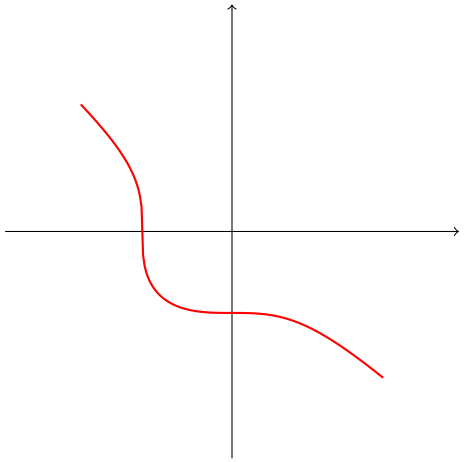

FIGURE 1. $4y^3 = -3x^3 - 5$

4. A family of curves that do not satisfy the local-global principle

As we saw in the previous sections, the curve $3x^3 + 4y^3 + 5z^3 = 0$ is an exception to the Hasse principle. However, we now sketch the construction of an explicit family of curves that do not satisfy the local-global principle. Namely, we will show that the family of curves

$$5x^3 + 9y^3 + 10z^3 + 12\left(\frac{t^2+82}{t^2+22}\right)^3 (x+y+z)^3 = 0 \tag{4.1}$$

does not satisfy the local-global principle. As before, showing that this has a solution in $\mathbb{R}$ is not hard. Indeed, if we fix y and z, the curve is a cubic polynomial in x, so it has a real solution. By perturbing y, z if necessary, we can ensure this solution is not $(0,0,0)$. Now, we proceed to prove that it has solutions in $\mathbb{Q}_p$ for all $p < \infty$. In order to do this, we will invoke two lemmata and a claim. The proofs of these results can be found in [2].

Lemma 4.1. *Let V be a smooth cubic surface in $\mathbb{P}^3$ over an algebraically closed field k. Let L be a line in $\mathbb{P}^3$ intersecting V in exactly 3 points. Let W be the blowup of V at these points. Let $W \to \mathbb{P}^1$ be the fibration of W by plane cubics induced by the projection $\mathbb{P}^3 \backslash L \to \mathbb{P}^1$ from L. Assume that some fiber of $\pi : W \to \mathbb{P}^1$ is smooth. Then at most 12 fibers are singular, and if there are exactly 12, each of them is a nodal plane cubic.*

Sketch. This result can be proven using the Euler characteristic

$$\chi(V) = \sum_{i=1}^{2\dim V} (-1)^i \dim_{\mathbb{F}_l} H^i_{\text{ét}}(V, \mathbb{F}_l)$$

where l is a prime distinct from the characteristic of k.

Lemma 4.2. *If $F(x,y,z) \in \mathbb{F}_p[x,y,z]$ is a nonzero homogeneous cubic polynomial such that F does not factor completely into linear factors over $\mathbb{F}_p$, then the subscheme X of $\mathbb{P}^2$ defined by $F = 0$ has a smooth $\mathbb{F}_p$-point.*

Proof. First, note that the polynomial has to be squarefree, as otherwise it would factor completely. From this, we get that X is reduced. If X is a smooth cubic curve, as in [5], we can show that it has genus 1. Thus, by the Hasse bound, there is at least one $\mathbb{F}_p$-point. Now, if X is not smooth, by enumerating the possibilities as in [2], we get X must be a nodal or cuspidal cubic or a union of a line and a conic. It follows that the Galois action on components is trivial because when there is more than one component,

these have different degrees. Thus, there is an open set of X isomorphic to $\mathbb{P}^1$ with at most two geometric points deleted. However, $\#\mathbb{P}^1(\mathbb{F}_p) \geq 3$, so there is still at least one $\mathbb{F}_p$-point on X, as desired. $\square$

Let us show that our family of curves does not satisfy the local-global principle. Consider the cubic surface

$$V : 5x^3 + 9y^3 + 10z^3 + 12w^3 = 0 \tag{4.2}$$

in $\mathbb{P}^1$. It is a result of Cassels and Guy [4] that V does not satisfy that local-global prinicple. That is, it has no solutions in $\mathbb{Q}$, but it has a solution in $\mathbb{Q}_p$ for all $p < \infty$. Now, consider the line

$$L : x + y + z = w = 0 \tag{4.3}$$

Their intersection $V \cap L$ (as a subscheme of $L \cong \mathbb{P}^1$) is defined by

$$5x^3 + 9y^3 - 10(x + y)^3 = 0 \tag{4.4}$$

As the discriminant of this curve is $242325 = 3^3 \cdot 5^2 \cdot 359 \neq 0$, we have that V and L have exactly 3 geometric points of intersection. Note that this remains true in characteristic p for $p \neq 3, 5, 359$. Now, consider the blowup W of V at these intersection points. Explicitly, $W \subseteq \mathbb{P}^3 \times \mathbb{P}^1$ is given by the points $((x, y, z, w), (u_0, u_1))$ such that

$$W : 5x^3 + 9y^3 + 10z^3 + 12w^3 = 0 \tag{4.5}$$

$$u_0 w = u_1(x + y + z) \tag{4.6}$$

Here, the induced fibration $W \to \mathbb{P}^1$ is given by the projection to the second factor, namely $((x, y, z, w), (u_0, u_1)) \mapsto (u_0, u_1)$. If we define $u = \frac{w}{x+y+z}$, from the equations (4.5) and (4.6), we get that the fiber W_u above u can be written as

$$W_u : 5x^3 + 9y^3 + 10z^3 + 12u^3(x + y + z)^3 = 0 \tag{4.7}$$

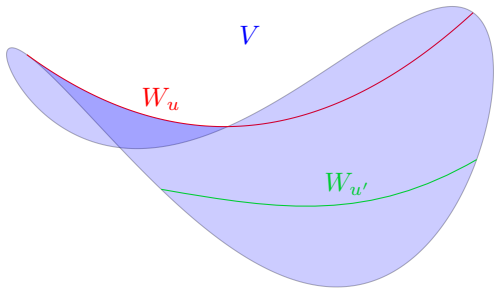

FIGURE 2. The fibers W_u can be thought of as curves in V. (Picture adapted from [6])

Note that u runs over all of $\mathbb{P}^1$. However, we will prove that for a particular family of choices of u, the curves W_u are an exception to the local-global principle. Let us proceed to show this. First, we verify that the W_u are smooth. By dehomogenizing (4.7), we get

$$f(x, y) = 5x^3 + 9y^3 + 10 + 12u^3(x + y + 1)^3 = 0 \tag{4.8}$$

For f to have a singularity, we must have that

$$f = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0 \tag{4.9}$$

Now, (4.9) is a system of three equations with three variables x, y, u, so we can solve for u by eliminating x and y. After doing this, from the calculation done in [2], we get

$$2062096u^{12} + 6065760u^9 + 4282200u^6 + 999000u^3 + 50625 = 0 \tag{4.10}$$

That is, W_u has a singular point if and only if u satisfies (4.10). In particular, W_0 is a smooth fiber. Thus, by Lemma 4.1 for $k = \mathbb{C}$, we get that the 12 singular fibers implied by the 12 solutions of (4.10) are the only singular fibers. Moreover, these singular fibers must be nodal plane cubics. Now, by [2], the polynomial in (4.10) is irreducible over $\mathbb{Q}$, so it follows that none of this 12 singular points is in $\mathbb{Q}$. That is, W_u is always smooth for $u \in \mathbb{P}^1(\mathbb{Q})$. Furthermore, we can show that for any prime p that does not divide the discriminant Δ of the polynomial (4.10), we have that W_u has a $\mathbb{Q}_p$-point. First, by [2], $\Delta = 2^{146} \cdot 3^{92} \cdot 5^{50} \cdot 359^4$. Now, let us fix a prime $p \neq 2, 3, 5, 359$ and a place $\overline{Q} \dashrightarrow \overline{\mathbb{F}_p}$. Note that the 12 singular u-values of $\mathbb{P}^1(\overline{\mathbb{Q}})$ reduce to 12 distinct singular u-values in $\mathbb{P}^1(\overline{\mathbb{F}_p})$ for the family $\overline{W} \to \mathbb{P}^1$ defined by the equations (4.5) and (4.6) over $\mathbb{F}_p$. However, recall that we noted that the fiber W_0 is still smooth in characteristic p, so it follows that, by Lemma 4.1, the fibers $\overline{W} \to \mathbb{P}^1$ are all smooth plane cubics or nodal plane cubics. Hence, by Lemma 4.2 and Hensel's lemma, we get that W_u has a $\mathbb{Q}_p$-point for all $u \in \mathbb{P}^1(\mathbb{Q}_p)$. Finally, it remains to show that this is also the case for $p = 2, 3, 5, 359$.

Claim 4.3. *If $u \in \mathbb{Q}$ satisfies $u \equiv 1 \bmod p\mathbb{Z}_p$ for $p = 2, 3,$ and 5, and $u \in \mathbb{Z}_{359}$, then the fiber W_u has a point in $\mathbb{Q}_p$ for all $\mathbb{Q}_p$, $p < \infty$.*

Sketch. We use Lemma 4.2 and Hensel's lemma to prove the existence of $\mathbb{Q}_p$-points.

Now, for u, we need a function $\mathbb{P}^1 \to \mathbb{P}^1$ that maps $\mathbb{P}^1(\mathbb{Q}_p)$ into $1 + p\mathbb{Z}_p$ for $p = 2, 3,$ and 5 and into $\mathbb{Z}_{359}$ for $p = 359$ so that we can apply Claim 4.3. As $\left(\frac{-22}{p}\right) = -1$ for $p = 2, 3, 359$, the function

$$u = 1 + \frac{60}{t^2 + 22} = \frac{t^2 + 82}{t^2 + 22} \tag{4.11}$$

works. Indeed, the denominator will not be 0 for these values and $2, 3 \mid 60$. Now, plugging this into (4.7), we get

$$X_t : 5x^3 + 9y^3 + 10z^3 + 12\left(\frac{t^2 + 82}{t^2 + 22}\right)^3 (x + y + z)^3 = 0 \tag{4.12}$$

which is precisely the family of curves we claimed were an exception for the local-global principle, as desired.

References

[1] K. Conrad. *Selmer's example.*

[2] B. Poonen. *An explicit algebraic family of genus-one curves violating the Hasse principle.*

[3] L. Modes. *18.782 Introduction to Arithmetic Geometry: Pset 4.*

[4] J.W.S Cassels and M.J.T Guy. *On the Hasse principle for cubic surfaces.*

[5] L. Modes. *18.782 Introduction to Arithmetic Geometry: Pset 10.*

[6] user121799. https://tex.stackexchange.com/questions/429935/how-to-draw-pictures-of-surfaces-in-latex.

Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139