RECENT THOUGHTS ON ABELIAN POINTS

1. Introduction

While at MSRI in early 2006, I got asked a very interesting question by Dimitar Jetchev, a Berkeley grad student. It motivated me to study abelian points on algebraic curves (and, to a lesser extent, higher-dimensional algebraic varieties), and MSRI's special program on Rational and Integral Points was a convenient setting for this.

It did not take me long to find families of curves without abelian points; I wrote these up in a paper which will appear[1] in Math. Research Letters.

Since then I have continued to try to put these examples into a larger context. Indeed, I have tried several different larger contexts on for size. When, just a couple of weeks ago, I was completing revisions on the paper, the context of "Kodaira dimension" seemed most worth promoting. Now, after ruminating about my upcoming talk for several days it seems that "Field arithmetic" should also be part of the picture. Needless to say, the final and optimal context (whatever that might mean!) has not yet been found.

So, after having mentally rewritten the beginning of my talk many times, it strikes me that the revisionist approach may not be best: rather, I will for the most part present things in their actual chronological order.

2. Dimitar's Question

It was:

Question 1. *Let $C_{/\mathbb{Q}}$ be Selmer's cubic curve:*

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

Is there an abelian cubic field L such that $C(L) \neq \emptyset$? Or an abelian number field of any degree?

Some basic comments: a finite degree field extension L/K is **abelian** if it is Galois with abelian Galois group, i.e., if $\mathrm{Aut}(L/K)$ is an abelian group of order $[L : K]$. The easy examples of abelian extensions are quadratic extensions (in characteristic different from 2!); for every degree $d \geq 3$, most degree d field extensions $L/\mathbb{Q}$ are not even Galois, let alone abelian (if M is the Galois closure of $L/\mathbb{Q}$ – i.e., the splitting field of a defining polynomial for L – then usually $\mathrm{Gal}(M/\mathbb{Q}) = S_d$). Dimitar had tried searching for points over abelian cubic fields computationally, without success.

What is so special about this curve? It has no rational points over $\mathbb{Q}$, despite the fact that it has points in every completion of $\mathbb{Q}$: i.e., it is a counterexample to the Hasse principle – indeed the most famous and one of the oldest (1951), although

[1] At least, that was what the referee recommended, which to my mind is the *de facto* moment of acceptance of a paper. Your money back if the editorial board of MRL overturns the referee's decision.

there are even older hyperelliptic quartic counterexamples due to Lind (1940) and Reichardt (1942). This means that it will be locally trivial over every extension field L and hence hard to rule out the possibility that it may have L-rational points. Indeed, there is no known algorithm which is guaranteed to determine whether $C(L) = \emptyset$ for any given (say) cubic field L, although there are some computational procedures which seem to work well in practice (Dimitar is much better versed in these procedures than I); still less do we have any clue how to handle infinitely many fields at once! It is a very hard question.

3. My answer

I had, and still have, no idea how to answer it.[2]

4. But

It got me to thinking. Putting aside the specifically cubic part, his question is in fact asking whether Selmer's curve has points over the maximum abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$. This means the (infinite) compositum of all finite degree abelian extensions $K/\mathbb{Q}$. The Galois group of any algebraic extension of fields is naturally the inverse limit of the Galois groups of the finite subextensions (so is a profinite group). Note also that for any property P of groups such that if G_1 and G_2 have property P so do all subgroups of $G_1 \times G_2$, the compositum of any two P-Galois extensions of $\mathbb{Q}$ is again a P-Galois extension of $\mathbb{Q}$, so there is indeed a unique maximal such extension, say $\mathbb{Q}^P$. Interesting examples of such properties include: being abelian, being nilpotent, being solvable, and being a p-group.

We do know, by the way, quite explicitly what the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ is (we do not know the other aforementioned examples): it is the field $\mathbb{Q}(\mu_\infty)$ obtained by adjoining to $\mathbb{Q}$ all roots of unity, and the Galois group is $\hat{\mathbb{Z}}^\times$. This turns out to be of relatively little importance: in generalizations to other fields (especially, other number fields) K I will always be interested in K^{ab}, and not just $K(\mu_\infty)$, and this will cause no additional trouble.

I got to thinking that Dimitar asked me whether a particular cubic curve – so, a very particular genus one curve – $C_{/\mathbb{Q}}$ has points over $\mathbb{Q}^{\mathrm{ab}}$. Can I find *some* genus one curve (or better yet, some cubic curve) which does not have points over $\mathbb{Q}^{\mathrm{ab}}$?

In fact it was known, and even known to me, that there is some algebraic curve $C_{/\mathbb{Q}}$ without points over $\mathbb{Q}^{\mathrm{ab}}$: this is an old (1973) theorem of Gerhard Frey. Frey's work is described in the important tome **Field Arithmetic** by Fried and Jarden.[3] To say more than this on Field Arithmetic right now would be "revisionist" – all I remembered at the time was that the book does not contain an *explicit* example of a curve $C_{/\mathbb{Q}}$ without abelian points. Rather, Frey's construction gives a torsor over a higher-dimensional abelian variety without abelian points. Applying Bertini's

[2] It's not going to be an "and then I proved (dramatic pause) this; and *then* I proved (longer dramatic pause) THAT" kind of talk.

[3] In fact the entire subject of Field Arithmetic was named after, and vastly grew and matured around, this book, which has recently appeared in a second and much larger edition. I am not aware of any other field of mathematics that is so closely associated to a single text.

theorem, such a torsor must contain some curve, but it's far from clear what these curves might be.

Remark: I had better make clear that part of our definition of curve – and later, of variety – is *geometric irreducibility.* This hypothesis is necessary to make the question interesting. Otherwise, let $L/\mathbb{Q}$ be your favorite non-abelian Galois extension, and let $V = \mathrm{Gal}(L/\mathbb{Q}) \times \mathbb{P}^1$. Geometrically this variety is just the direct sum of $[L : \mathbb{Q}]$ copies of the projective line, but it has an obvious fixed-point free action of $\mathrm{Gal}(L/\mathbb{Q})$ which needs to be trivialized in order to get a rational point. In other words, the set of all fields $K/\mathbb{Q}$ for which V has a K-rational point has a unique minimal element, namely L. Clearly then V does not have any abelian points. In order to ensure that all finite-type K-schemes have K-rational points, we would need – of course! – to ensure that K is algebraically closed.

I was soon able to construct cubic curves $C_{/\mathbb{Q}}$ with $C(\mathbb{Q}^{\mathrm{ab}}) = \emptyset$. My first construction was "abstract", in that I used the characterization of cubic curves without rational points as curves of genus one and index 3, and made a Galois cohomological argument. I want to softpedal such arguments during this talk, although they are the "meat" of the proofs of most of the coming results. Anyway, by cohomological considerations I was eventually led to the following:

Theorem 1. *Let $p \equiv -1 \pmod 3$ and a, b, c be positive integers prime to p. Then the curve*

$$C_p : apX^3 + bp^2Y^3 + cZ^3 = 0$$

has no $\mathbb{Q}^{\mathrm{ab}}$-rational points.

The proof is quite easy and I will give it momentarily, but first a few remarks.

Remark(ably): The day after I found this example Colliot-Thélène gave a colloquium talk at Berkeley on Diophantine equations. His *first* example of an equation without rational solutions was the curve above: apparently it is quite a famous one. After the talk, I caught him and mentioned my recent realization that (when $p \equiv -1 \pmod 3$) this curve has no abelian points, asking him whether this too had been previously known: apparently not.[4]

Remark: In particular we may take $p = 2$, $a = b = 1$, $c = 5$, getting that $2X^3 + 4Y^3 + 5Z^3 = 0$ has no abelian points. If only we could correct the 2 to a 3 (experimental error?!?) we would get Selmer's curve. So in some (quite silly) sense, I came as close as possible to answering Dimitar's question.

Remark: You will not, I think, find a simpler example of a curve without abelian points. In addition to being simple in some naive sense, the above curves have genus 1 and index 3. A curve of genus zero is a plane conic $aX^2 + bY^2 + cZ^2 = 0$, which has quadratic points. A curve of genus 1 and index 1 is an elliptic curve (it has a rational point!), and a curve of genus 1 and index 2 is a hyperelliptic quartic (with affine model given by) $y^2 = P_4(x)$: these – and indeed, all hyperelliptic curves – also have quadratic points.

[4] Although it is not entirely fair to equate "known to Colliot-Thélène" with "known to anyone," if you have met him you will understand the temptation to make such an equation.

Proof: We observe first that C has no $\mathbb{Q}_p$-rational points. For, if not, we would have a solution $(x, y, z) \in \mathbb{Z}_p^3$ with $\min(\operatorname{ord}_p(x),\ \operatorname{ord}_p(y),\ \operatorname{ord}_p(z)) = 0$, and this is visibly impossible: looking at the equation we see that p must divide first z, then x, then finally y. Moreover, if $K/\mathbb{Q}_p$ is any finite extension with uniformizer π and ramification index $e(K/\mathbb{Q}_p)$ prime to 3, then running through the above argument with ord_π in place of ord_p shows that C has no K-rational points.

But now suppose that there exists a solution in the ring of integers of $\mathbb{Q}_p(\mu_N)$ for some positive integer N. Write $N = M \cdot p^i$ with $(M, p) = 1$. We have $e(\mathbb{Q}_p(\mu_N)/\mathbb{Q}_p) = \varphi(p^i) = p^{i-1}(p-1)$, which is, by our assumption on p, prime to 3. The proof is completed by recalling that the maximal abelian extension of $\mathbb{Q}_p$ is obtained by adjoining all roots of unity (the local Kronecker-Weber theorem).[5]

5. Further examples

It now seems natural to search for examples over other number fields and for curves of other genera. If you look back at the previous example, a short Cebotarev-density theorem argument shows that for any number field K whose Galois closure does not contain $\mathbb{Q}(\mu_3)$, there are infinitely many p's for which the curve $(C_p)_{/\mathbb{Q}}$ fails to have rational points over the maximal abelian extension of K. Surely this strange hypothesis on K can be omitted with more work? Indeed, yes:

Theorem 2. *For every number field K, there is a genus one curve $C_{/\mathbb{Q}}$ with $C(K^{\mathrm{ab}}) = \emptyset$.*

I should say in passing that the proof I found of the general case is almost ridiculously high-powered: I used (i) the Deuring-Waterhouse classification of orders of elliptic curves over $\mathbb{F}_p$; (ii) the Poitou-Tate global duality theorem; (iii) Mazur's theorem on rational torsion; (iv) a theorem of Ono-Skinner on prime quadratic twists of analytic rank zero; (v) the elliptic modularity theorem; and (vi) the Gross-Zagier-Kolyvagin theorem! Nevertheless, the proof itself takes less than a page.

More interesting is the case of higher genus. Again, every curve of genus zero or two is hyperelliptic over the ground field, so has quadratic points. We constructed some examples in genus one; what about higher genera? I was able to prove the following two theorems.

Theorem 3. *For all odd $d > 1$, there exists a degree d plane curve $C_{/\mathbb{Q}}$ with $C(\mathbb{Q}^{\mathrm{ab}}) = \emptyset$.*

Theorem 4. *For all $g \geq 4$, there exists a curve $C_{/\mathbb{Q}}$ with $C(\mathbb{Q}^{\mathrm{ab}}) = \emptyset$.*

Please note that the case of genus 3 curves (aka plane quartics) is conspicuously missing.

6. Some hints on the proofs

So as to (I hope) save some time for after the fact philosophizing, I will not present the proofs in any detail, but rather drop a series of hints. First we recall the two oldest and best tricks for showing that a variety $V_{/K}$ fails to have rational

[5] Actually this is overkill; the more elementary dévissage of an extension $K/\mathbb{Q}_p$ into an unramified extension followed by a tamely ramified extension followed by a p-extension would suffice.

points over some extension field L.

1: Geometric functoriality: Suppose that there is a K-morphism $V \to W$ and $W(L) = \emptyset$. Then necessarily $V(L) = \emptyset$.

To apply this trick, we would like to start with a sizable supply of varieties W over $\mathbb{Q}$ with $W(\mathbb{Q}^{\mathrm{ab}}) = \emptyset$ and then "pull-back" to lots of V's. But how will we show that $W(\mathbb{Q}^{\mathrm{ab}}) = \emptyset$?

2: Arithmetic functoriality: Of course, if M is a field extension of L and $V(M) = \emptyset$ then $V(L) = \emptyset$. Earlier we applied this idea with $L = \mathbb{Q}^{\mathrm{ab}}$ and $M = \mathbb{Q}_p^{\mathrm{ab}}$: i.e., we found varieties which do not even have abelian points locally at some place.

3: Nonabelian Ramification Indices: How did we do that? We found varieties over $\mathbb{Q}_p$ which could only have points over a finite extension if that finite extension had ramification index divisible by 3, but if $p \equiv -1 \pmod 3$ there is no such abelian extension. We can try this trick with other degrees $d > 2$.

There are two (apparently) different ways to generalize our basic example: we can go further up or further in. The second in simpler, so (with apologies to C.S. Lewis) we will describe it first.

6.1. **Further in.**

Theorem 5. *Let p be a prime and $d > 1$ an integer which is prime to $p(p-1)$. Then*

$$\sum_{i=0}^{d-1} p^i X_i^d$$

has no points over $\mathbb{Q}^{\mathrm{ab}}$.

The proof is exactly the same. Now by an application of Dirichlet's theorem, for every odd $d > 1$, there exists such a prime p, hence we get a smooth degree d hypersurface in d variables without points over $\mathbb{Q}_p^{\mathrm{ab}}$. Applying Bertini's theorem, we can intersect with a general 2-plane to get degree d plane curves: thus we have given a (complete!) proof of Theorem 3.

Remark: Problem 11.2.10 of the new edition of *Field Arithmetic* asks for a proof or disproof of the claim that if a field K admits any geometrically irreducible variety without K-rational points, it admits a *plane* curve without K-rational points. We have just verified that this holds (even with a nonsingular plane curve) for $\mathbb{Q}_p^{\mathrm{ab}}$ for all p and hence also for $\mathbb{Q}^{\mathrm{ab}}$. As far as I know this was open up until now.

6.2. **Further up.** On the other hand, one can recognize a different form of the nonabelian ramification indices argument in the following classic result:

Theorem 6. *(Lang-Tate) Let K be a p-adic field, $A_{/K}$ an abelian variety with good reduction, V a principal homogeneous space for A of order n prime to p. Then, for any finite extension L/K, $V(L) \neq \emptyset \iff n \mid e(L/K)$.*

Remark: The curves of Theorem 1 are a (globalized, explicit) instance of this theorem with $n = 3$: the Jacobian elliptic curve $X^3 + Y^3 + abcZ^3 = 0$ (visibly!) has good reduction modulo p.

I am very fond of the local analysis that is used to apply this result, but in the interests of time I will only record the following consequence.

Theorem 7. *For every p-adic field K, there exists a genus one curve $C_{/K}$ with $C(K^{\mathrm{ab}})$.*

Remark: Intriguingly, it follows from Tate's non-Archimedean organization that any genus one curve over a p-adic field whose Jacobian has split multiplicative reduction *does* have an abelian splitting field. The case of good reduction and order divisible by p deserves closer investigation.

Theorem 8. *Let ℓ be either 4 or an odd prime. Then there exists a genus one curve $C^{\ell}_{/\mathbb{Q}}$ which has period and index both equal to ℓ and which does not have any abelian points.*

We only remark here that the period of C is its order in the Weil-Chatelet group of its Jacobian elliptic curve and its index is the least positive degree of a rational divisor, and that I had previously written several papers on this sort of problem.

Finally, let $g \geq 4$, and write $g = k\ell + 1$ with $k \in \mathbb{Z}$ and ℓ either 4 or an odd prime. The curve C^{ℓ} has two effective divisors D and D' each of degree $k\ell$ and with disjoint support. Then $D - D' = div(f)$, where f is a rational function on C^{ℓ}; taking the square root of f we get a degree 2 cover $Y \to C^{\ell}$ with precisely $2k\ell$ simple branch points; by Riemann-Hurwitz Y has genus $k\ell + 1 = g$.

7. Some geometric thoughts

No algebraic geometer could fail to notice that our two basic examples – from which all others were obtained by going "further up or further in" – were all in Kodaira dimension zero. Of course from a curve of genus 1 and a curve of genus, say, 4, one can by taking products get varieties of all possible dimensions and non-negative Kodaira dimensions. Vexingly, we did not get every example of non-negative Kodaira dimension we wanted – conspicuously missing were K3 surfaces, which in the form of quartic surfaces would lead by Bertini ("further in") to genus 3 curves. But certainly nothing in the above strategy will help us get any examples of negative Kodaira dimensional varieties $V_{/\mathbb{Q}}$ without abelian points. Are there any?

This is a very interesting question. If we restrict just to (possibly singular) Fano hypersurfaces we are asking an old question in modern language: is $\mathbb{Q}^{\mathrm{ab}}$ a C_1 field? (Actually to say that $\mathbb{Q}^{\mathrm{ab}}$ is C_1 is slightly stronger: it means that every Fano hypersurface defined over every abelian number field has a point in the maximal abelian extension of $\mathbb{Q}$.) This was conjectured by Emil Artin.

In one of several early papers that ought to be more widely read today, Lang proved Artin's conjecture with $\mathbb{Q}$ replaced by $\mathbb{Q}_p$: in fact he proved the stronger result that a local field with separably closed residue field is C_1. Lang's result does not really come close to proving Artin's conjecture, but it suggests that a disproof would be very deep: for instance if we want to find a cubic surface $S_{/\mathbb{Q}}$ without abelian points, we certainly cannot use our quaint local methods. But there's more:

a theorem of Kanevsky says that if, for every $K/\mathbb{Q}$, the Brauer-Manin obstruction is the only one to the existence of K-rational points on S, then $S(\mathbb{Q}^{\mathrm{ab}}) \neq \emptyset$. Moreover classical analytic number theory (especially, theorems of Brauer and Birch; see Davenport's beautiful book on Diophantine equations) says that a "sufficiently Fano" hypersurface over $\mathbb{Q}$ (i.e., for every fixed degree and sufficiently many variables) has points even over $\mathbb{Q}(\sqrt{-1})$. So Artin's conjecture is quite plausible, but whether it should extend to all Fano, or rationally connected, or negative Kodaira dimension varieties is much less clear. Notable here is a recent example of Colliot-Thélène and Madore of a del Pezzo surface over a C_1 field without rational points.

It is also natural to ask what happens when we replace $\mathbb{Q}$ with an arbitrary field (say of characteristic zero): for instance, curves of genus zero and two still have abelian points. Interestingly, it turns out to be possible to produce quite a lot more examples of varieties without abelian points defined over the Laurent series field $\mathbb{Q}((t))$: in an appendix to my paper I find (i) a twisted form of $(\mathbb{P}^1)^4$, (ii) a geometrically rational surface, and (iii) a genus 3 curve without abelian points. Note that the completed maximal abelian extension of $\mathbb{Q}((t))$ is $\mathbb{Q}^{\mathrm{ab}}((\sqrt{t}))$, so that we are essentially "adding a dimension" to our field for free. In retrospect, these results are thus closely related to the proof that for any non-separably closed field K, $K((t))$ is not C_1.

8. Field arithmetic

Note that I never really justified my interest in $\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}$ as opposed to some other interesting infinite algebraic extension: the problem was given to me, and I liked it, but perhaps we should look at other fields as well.

First a preliminary remark: in Frey's original paper he shows that the maximal *nilpotent* extensions of $\mathbb{Q}$ and $\mathbb{Q}_p$ are not PAC. I am pretty sure that all my examples indeed lack nilpotent points, but I will admit to not being especially interested in this case (I have to keep reminding myself of the definition of a nilpotent group.)

In contrast, it is very interesting to look at solvable points on algebraic varieties: a very deep open problem is that the maximal solvable extension, $\mathbb{Q}^{\mathrm{solv}}$ of $\mathbb{Q}$ is PAC: that is, every geometrically irreducible variety over a solvable number field has a point over a solvable field extension. This is a beautiful problem and at first very surprising, since it is exactly the opposite of what happens in the zero-dimensional case: most finite $\mathbb{Q}$-schemes do not have solvable points!

It is almost certainly a very difficult question. For instance, around 2000 Richard Taylor realized that it would imply the Fontaine-Mazur conjecture. Surely he then had a try at proving the PAC-ness of $\mathbb{Q}^{\mathrm{solv}}$, and that he did not succeed is sobering for all of us. Indeed, in 2005 Mirela Ciperiani wrote a sensational thesis on a very special case: she proved that a genus one curve $C_{/\mathbb{Q}}$, locally trivial and with semistable Jacobian, has points over a solvable extension. The 73 page paper (which she gave to me just a few days ago) is joint with her thesis advisor, one A. Wiles of Princeton, NJ.

But I am willing to go one up on this conjecture. While I was a grad student at Harvard, Barry Mazur suggested to me that every genus one curve over $\mathbb{Q}$ should have not only solvable points but *metabelian* points, i.e., points over $(\mathbb{Q}^{\mathrm{ab}})^{\mathrm{ab}}$, and that perhaps a Heegner point argument might work.[6] So, on a wing and a prayer I essay the following

Conjecture 9. *The field* $(\mathbb{Q}^{\mathrm{ab}})^{\mathrm{ab}}$ *is pseudoalgebraically closed.*

Let me end with some tantalizing comments:

All of our basic (Kodaira dimension zero) local examples have points over cyclic extensions of the maximal cyclotomic extension of $\mathbb{Q}_p$. However, as far as I can tell, even for genus one curves over $\mathbb{Q}_p$ the question remains open and is not especially easy (it comes down an issue of wild ramification).

This conjecture implies that PAC-ness of $\mathbb{Q}^{\mathrm{solv}}$: indeed, algebraic extensions of PAC fields are PAC.

However, it is much more interesting for the following reason: PAC is one of the two basic properties of fields studied in *Field Arithmetic.* The other is Hilbertianity: the property that each G-Galois covering of the projective line over that field K has an irreducible fiber (i.e., specializes to give a Galois extension L/K with the same Galois group). Hilbertian fields have enormous absolute Galois groups: indeed, it is conjectured that every finite group is a Galois group over every Hilbertian field. However, it is as yet impossible to prove this conjecture for the Hilbertian fields (e.g. $\mathbb{Q}$) that are most familiar to us.

But the triumph of Field Arithmetic is the discovery that there are fields which are both PAC and Hilbertian. Since there are geometrically connected fine moduli spaces of Galois coverings (Hurwitz spaces), the inverse Galois problem has an affirmative solution for fields which are PAC and Hilbertian. Unfortunately $\mathbb{Q}^{\mathrm{solv}}$ is not Hilbertian: indeed, by construction it does not have any proper solvable extensions. However, a theorem of Kuyk asserts that any abelian extension of any Hilbertian field is Hilbertian. Applying it twice, we get that $(\mathbb{Q}^{\mathrm{ab}})^{\mathrm{ab}}$ is Hilbertian. So:

Proposition 10. *If* $(\mathbb{Q}^{\mathrm{ab}})^{\mathrm{ab}}$ *is PAC, then the inverse Galois problem has an affirmative solution over it.*

By way of comparison, we have thus far only been able to show that approximately zero percent of the finite groups are Galois groups over $\mathbb{Q}$; over $\mathbb{Q}^{\mathrm{ab}}$ one can do much better, getting most "classical" finite simple groups, but putting the Jordan-Holder factors together remains intractable. Maybe one more "ab" will do the trick! (In fact, if $(\mathbb{Q}^{\mathrm{ab}})^{\mathrm{ab}}$ turns out not to be PAC, we can always tack on any finite number of "ab"'s and ask the same question...)

For further details, please see

`http://math.uga.edu/~pete/plclarkarxiv8v2.pdf`

The paper has not yet gone through proofs, so any suggestions, comments or improvements may still make it into the final published version.

[6] This is sufficiently reminiscent of the Ciperiani-Wiles paper that one can postulate a prior Mazur-Wiles converation on this subject.