Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 92 (2017)
Heft: 1

Artikel: On a modular Fermat equation
Autor: Pila, Jonathan
DOI: https://doi.org/10.5169/seals-685880

Comment. Math. Helv. 92 (2017), 85–103
DOI 10.4171/CMH/407

Commentarii Mathematici Helvetici

On a modular Fermat equation

Jonathan Pila

Abstract. We study some diophantine problems suggested by the analogy between multiplicative groups and powers of the modular curve in problems of "unlikely intersections". We prove a special case of the Zilber–Pink conjecture for curves.

Mathematics Subject Classification (2010). 11G18, 11D41, 03C64.

Keywords. Zilber–Pink conjecture, Fermat equation, o-minimality.

1. Introduction

To motivate the title problem, we recall some classical diophantine statements. We identify (algebraic) varieties with their sets of complex points. Thus, in particular, $\mathbb{G}_{\mathrm{m}} = \mathbb{G}_{\mathrm{m}}(\mathbb{C}) = \mathbb{C}^{\times}$ is the multiplicative group of non-zero complex numbers, and $Y(1) = Y(1)(\mathbb{C}) = \mathbb{C}$ is the moduli space parameterising elliptic curves defined over $\mathbb{C}$, up to isomorphism over $\mathbb{C}$, by their j-invariant.

The Multiplicative Manin–Mumford conjecture (MMM; a theorem Laurent [21], see also [9,24,43]) concerns the distribution of *torsion points* in a subvariety $V \subset \mathbb{G}_{\mathrm{m}}^k$. These are the torsion points in the group, namely the points of the form $(\zeta_1, \ldots, \zeta_k)$ where $\zeta_i \in \mathbb{C}^{\times}$ are roots of unity. MMM states that the torsion points contained in V are contained in a finite number of *torsion cosets* contained in V. Torsion cosets are the cosets of subtori by torsion points; otherwise expressed, they are the irreducible components of subvarieties defined by systems of multiplicative relations, that is relations of the form $x_1^{a_1} \ldots x_k^{a_k} = 1$. Thus a torsion point is precisely a torsion coset of dimension zero. The "original" Manin–Mumford conjecture (MM) is the same statement for a subvariety of an abelian variety, in which torsion cosets are cosets of abelian subvarieties by torsion points. MM is a theorem of Raynaud [39,40].

The André–Oort conjecture [2,28] was partly motivated by an informal analogy with MM. It concerns the distribution of *special points* in a subvariety V of a *Shimura variety* X, and is now "almost" fully proved [17,45,46]. For cartesian powers of the modular curve it is a theorem ("Modular André–Oort"; MAO) proved in [3,30]. MAO states that, for $V \subset Y(1)^k$, the *special points* of $Y(1)^k$ contained in V are contained in finitely many *special subvarieties* of $Y(1)^k$ contained in V. The

special subvarieties of $Y(1)^k$ are the irreducible components of subvarieties defined by systems of modular relations, that is relations of the form $\Phi_{N_{ij}}(x_i, x_j) = 0$, where Φ_N are the classical modular polynomials. A special point is precisely a special subvariety of dimension zero. See §2 for a more careful definition of special points and subvarieties in $Y(1)^2$, and §6 for $Y(1)^k$.

The two statements are unified within Pink's version [37] of what is now known as the Zilber–Pink conjecture (ZP). See also [32, 49, 50] for the general formulation of this far-reaching conjecture, which is very much open, and §7 for the statement in $Y(1)^k$. ZP governs the interaction between a subvariety V of a mixed Shimura variety X, and the collection of *special subvarieties* of X (see [37]). In $\mathbb{G}_{\mathrm{m}}^k$, the special subvarieties are the aforementioned torsion cosets. Thus, within ZP, MMM and MAO are analogues in a strict sense, and modular relations are analogues of multiplicative ones.

In the multiplicative setting, the Multiplicative Mordell–Lang conjecture (MML; a theorem of Laurent [21]) generalises MMM. Let us state it in the special case of the variety $V \subset \mathbb{G}_{\mathrm{m}}^2$ defined by $u + v = 1$ (the *unit equation*): there are only finitely many solutions to $u + v = 1$ when u, v are restricted to the division group of a finitely generated subgroup of $\mathbb{C}^\times$. Important special cases, for finitely generated subgroups of algebraic, or even rational, numbers were established in fundamental work of Siegel, Mahler, Lang, and Liardet; see [6, 19, 23, 44].

The modular analogue of this statement ("Modular Mordell–Lang") is proved, in general form, in [14, 31]. In the special case it asserts that there are only finitely many solutions to $u + v = 1$ when u, v are restricted to finitely many *Hecke orbits* (or are special points). The Hecke orbit of $x \in \mathbb{C}$ is $\{y \in \mathbb{C} : \exists N\ \Phi_N(x, y) = 0\}$. It is the set of j-invariants of elliptic curves which are *isogenous* to the one with j-invariant x.

Now we observe that Fermat's Last Theorem (FLT; theorem of Wiles [47]) may also be expressed in these terms: it asserts that $u + v = 1$ has no solutions for $u, v \in \mathbb{Q}^{\times n}$ when $n \geq 3$. It seems not to have been observed that the condition on u, v fits naturally into the multiplicative group setting: they are required to be in the subgroup consisting of nth powers of rational numbers. The modular analogue of $u = x^n$ is $\Phi_n(x, u) = 0$. Generalising a little, we are led to investigate the rational solutions x, y of the system

$$\Phi_N(x, u) = 0, \quad \Phi_M(y, v) = 0, \quad u + v = 1, \quad N, M \geq 1. \tag{$*$}$$

This is the "modular Fermat equation" of the title. If x is not special, then neither is u, and N is unique. If x (and hence u) is special then N is not unique and to avoid trivialities we will frame our results in terms of *minimal* solutions, namely those for which N is minimal with $\Phi_N(x, u) = 0$, and likewise for M.

Given N, M one may eliminate u, v in $(*)$ to find that (x, y) lies on a (possibly reducible) algebraic curve $V_{N,M}$. The strict analogue of FLT would take $N = M$, but

this plays no role for us. We prove the following partial analogue of "asymptotic" FLT. It asserts that there are no rational points on any of the curves $V_{N,M}$ with large prime $\max\{N, M\}$. We say nothing about possible solutions for small N, M.

1.1. Theorem. *There exists L such that $(*)$ has no minimal solutions with $x, y \in \mathbb{Q}$ for which $\max\{N, M\} \geq L$ and $\max\{N, M\}$ is a prime number.*

Our proof of this theorem uses a variant of the o-minimality and point-counting strategy which has been used over recent years to prove various cases of the André–Oort (and Zilber–Pink) conjecture, using the Counting Theorem of Pila–Wilkie [35]. The strategy was originally proposed by Zannier in the context of the Manin–Mumford conjecture (see [36]), where it relies on torsion points having high degree (relative to their order).

For André–Oort, the strategy depends on special points having high degree over $\mathbb{Q}$ in a suitable sense (see [33,45]). Our results here likewise depend on $\mathbb{Q}(u, v)$ having large degree over $\mathbb{Q}$ (relative to $\max\{N, M\}$, in a sense made precise below). The applicability of the Counting Theorem in these settings relies ultimately on the result of Wilkie [48] that the real exponential function gives rise to an *o-minimal structure*. The constant L in 1.1 is presently ineffective. Before going further into the specifics, let us observe that this method has no purchase for FLT or Mordell–Lang type problems, simply because when u, v are in a group generated by rational numbers, or a finitely generated group, $[\mathbb{Q}(u, v) : \mathbb{Q}]$ is bounded.

We can remove the primality condition on $\max\{N, M\}$ conditionally on a special case of a statement ("GO1", see §8) formulated in Habegger–Pila [15]. Consider $x, y \in \overline{\mathbb{Q}}$ such that the elliptic curves E_x, E_y, whose j-invariants are x, y, are related by a cyclic isogeny of degree N. So $\Phi_N(x, y) = 0$ for the modular polynomial Φ_N. If x, y are not special then, as mentioned above, N is unique.

1.2. Strong Galois-Orbit Hypothesis (SGH). There exist $c, \delta > 0$ such that if $(x, y) \in \overline{\mathbb{Q}}^2$ are not special and $\Phi_N(x, y) = 0$, then

$$[\mathbb{Q}(x, y) : \mathbb{Q}] \geq cN^{\delta}.$$

The plausibility of this conjecture is discussed briefly in §3. Essentially, it is on a par with expectations for the best dependence in the Strong Uniform Boundedness Conjecture (Merel's theorem [26]). In §8 we show that SGH is the essential case of the statement GO1 alluded to above, and that, in view of [15,34], it implies the full Zilber–Pink conjecture for $Y(1)^k$ (see §7 for the statement). We need just the special case of 1.2 for $x \in \mathbb{Q}$ to prove an unrestricted version of 1.1.

1.3. Theorem. *Assume SGH for $x \in \mathbb{Q}$. Then there exists L such that $(*)$ has no minimal solutions with $x, y \in \mathbb{Q}$ for $\max\{N, M\} \geq L$.*

The reason we are able to prove Theorem 1.1 is that SGH for $x \in \mathbb{Q}$ and N a prime number follows from recent results of Najman [27]. His results are more

precise, but imply in particular that if $\Phi_N(x, y) = 0$ with $x \in \mathbb{Q}$ non-special and $N \geq 41$ a prime then

$$[\mathbb{Q}(y) : \mathbb{Q}] \geq N/3.$$

Though very much in the spirit of "unlikely intersections", the conclusion of 1.3 is seemingly not a consequence of the Zilber–Pink conjecture, because rational points in $Y(1)^2$ are neither special nor contained in finitely many Hecke orbits. Likewise, FLT is not a consequence of MML because $\mathbb{Q}^{\times n}$ is not finitely generated.

In §§4–6 we consider generalisations. We can prove analogues of 1.1 and 1.3 for more general curves and higher-dimensional varieties in $Y(1)^k$. These suggest the formulation of analogous conjectures in the multiplicative setting which generalise (asymptotic) FLT. Our methods cannot address them, but we prove (Theorem 6.4) the analogue of one of our main conjectures (5.4), for the *inverse* Fermat equation. This would seem to add credence to the conjectures since $u^n = x$ is also an analogue of $\Phi_n(x, u) = 0$. All our conjectures for curves in §4 are implied by the *abc* conjecture.

In §7 and §8 we study the relationship between SGH and statements formulated in [15]. We observe that, if x, y are non-algebraic points with $\Phi_N(x, y) = 0$, then the large gonality of modular curves [1, 51] implies that we get a high extension degree even over finitely generated fields. Note that gonality growth of some positive power of N is necessary if SGH is to be true. This enables us to prove a special case of the Zilber–Pink conjecture for curves, a counterpart to the result of [14].

1.4. Theorem. *Let $V \subset Y(1)^3$ be a curve which is not defined over $\overline{\mathbb{Q}}$. Then the Zilber–Pink conjecture holds for V.*

Note that if V as in 1.4 is not contained in any proper subvariety of $Y(1)^3$ defined over $\overline{\mathbb{Q}}$ then the conclusion follows from the main result of Chatzidakis–Ghioca–Masser–Maurin [7]. We will use this in extending the above result to curves in $Y(1)^k$ provided that no image under a coordinate projection to $Y(1)^3$ is defined over $\overline{\mathbb{Q}}$.

In our proofs, the Galois and gonality results mentioned (which show that the points in question have "many" conjugates), are opposed to upper bounds for rational points on suitable sets definable in an o-minimal structure. This basic strategy has been used in many problems along these lines. A new feature here is that the proofs use a family of definable sets, and rely on uniformity in the Counting Theorem.

2. Proof of Theorems 1.1 and 1.3

A *special point* in $\mathbb{C}$, also known as a *singular modulus*, is the j-invariant of a CM elliptic curve. Equivalently, it is a number $\sigma = j(\tau)$ where $\tau \in \mathbb{H}$ is a quadratic point ($[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$). Here $\mathbb{H}$ is the complex upper half-plane and $j : \mathbb{H} \to \mathbb{C}$ is the elliptic modular function.

2.1. Definition. A *special subvariety* of $\mathbb{C}^2$ is defined to be one of the following: $\mathbb{C}^2$ itself; a modular curve T_N defined by $\Phi_N(x, y) = 0$; a line $x = \sigma$ or $y = \sigma$ where σ is a singular modulus; or a point (σ, σ') where σ, σ' are singular moduli (a *special point* of $\mathbb{C}^2$). By definition, *weakly special subvarieties* include the above, all horizontal and vertical lines, and all points.

2.2. Proof of Theorem 1.1. Let $F \subset \mathbb{H}$ be the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ by Mobius transformations. The restriction $j : F \to \mathbb{C}$ of the elliptic modular function is definable in the o-minimal structure $\mathbb{R}_{\text{an exp}}$.

Define the following family of sets in $\mathrm{GL}_2^+(\mathbb{R})^2$, parameterised by $Q = (z, w) \in \mathbb{H}^2$,

$$Z_Q = \{(g, h) \in \mathrm{GL}_2^+(\mathbb{R})^2 : gz, hw \in F \text{ and } j(gz) + j(hw) = 1\}.$$

This family is definable in the o-minimal structure $\mathbb{R}_{\text{an exp}}$; see e.g. [30].

Suppose that we have a solution (x, y) to $(*)$ with large prime $L = \max\{N, M\}$. Then we have (u, v) with $\Phi_N(x, u) = 0, \Phi_M(y, v) = 0$. Let us assume for now neither x nor y is special. So $\Phi_N(x, u) = 0$, $\Phi_M(y, v) = 0$, and by the results of Najman [27] we have

$$[\mathbb{Q}(u, v) : \mathbb{Q}] \geq cL^{\delta}.$$

Take $z, w \in F$ with $j(z) = x, j(w) = y$ and put $Q = (z, w)$. Thus we have at least that many conjugate points (u', v') over $\mathbb{Q}$, and each of these gives a solution of the system $(*)$ with the same (x, y). Each such (u', v') gives rise to a rational point on Z_Q, and (by [14, Lemma 5.2]) of height bounded by $c'L^{10}$

By the Counting Theorem [35], which is uniform over the family, if L is sufficiently large then Z_Q contains some positive dimensional real algebraic curve. The corresponding points $(gz, hw) \in \mathbb{H}^2$ must be non-constant, as the algebraic curves in Z_Q must account for "many" distinct (u', v'). So we get a real algebraic curve contained in

$$\{(z, w) \in \mathbb{H}^2 : j(z) + j(w) = 1\}.$$

But then we must have a complex algebraic curve contained in it, which then must coincide with it. This gives an algebraic curve in $\mathbb{H}^2$ whose image under j in $\mathbb{C}^2$ is algebraic. Then by the "Ax–Lindemann" theorem [30, Theorem 1.6], the image curve $u + v = 1$ must be a modular curve. But it isn't. Thus L is bounded.

Suppose x (or y) is special. There are only finitely many rational special points, so one is in a finite union of Hecke orbits, and for these one has a suitable Galois lower bound $[\mathbb{Q}(u) : \mathbb{Q}] \geq cN^{\delta}$, for the minimal N, for suitable absolute positive δ (by isogeny estimates of Masser–Wüstholz [25], subsequently improved by others (especially [13, 29]). So one again gets $[\mathbb{Q}(u, v) : \mathbb{Q}] \geq cL^{\delta}$. (In fact x, y cannot both be special, as $u+v = 1$ contains no special points, as shown by Kühne [18].) □

2.3. Proof of Theorem 1.3. This is exactly the same as above, except we appeal to SGH for $x \in \mathbb{Q}$ instead of the results of [27] for the Galois lower bounds. □

3. How plausible is SGH?

SGH is related to uniform bounds for torsion in elliptic curves over number fields (Mazur, Kamienny, Merel [26],...) and Serre's Uniformity Conjecture (Bilu–Parent [5],...) and seems in line with expectations. A point $(x, y) \in T_N$ parameterises an elliptic curve with a cyclic subgroup of order N defined over $\mathbb{Q}(x, y)$. According to the Strong Uniform Boundedness Theorem of Merel (see [26, 41]), the size of the torsion subgroup of K-rational points of an elliptic curve defined over a numberfield K with $[K : \mathbb{Q}] = d$ is bounded by some $B(d)$. The known bounds for $B(d)$ are exponential in d but it is conjectured that $B(d)$ can be taken polynomial in d (see [41, Remark 2]). The corresponding conjectures for cyclic subgroups of size N, i.e. for cyclic isogenies, would imply SGH. The results of Najman [27] support these expectations.

That the gonality (defined in the proof of 7.3 below) of modular curves grows at least as a positive power of N is certainly necessary for SGH to hold. Conversely, Frey [12] has shown (using Faltings's Big Theorem, i.e. his proof of Mordell–Lang [11]) that if a curve has infinitely many points defined over fields of degree d over a field of definition K, then the gonality of C/K is at most $2d$. Thus, the modular curve $\Phi_N(x, y) = 0$ has only finitely many points defined over fields of degree at most cN over $\mathbb{Q}$ for some positive c.

4. Generalisation to curves

There is nothing special about the curve $u + v = 1$ in Theorems 1.1 and 1.3, except that it is not weakly special. Both theorems hold for the system $(*)_V$ in which a non-weakly-special curve $V \subset \mathbb{C}^2$ replaces the curve $u + v = 1$ in $(*)$ and indeed 1.3 for V is unconditional if V is not defined over $\overline{\mathbb{Q}}$. We do not formulate the results as still more general formulations are in §6.

If V is special, say defined by $\Phi_K(u, v) = 0$, then one can have rational solutions to $(*)_V$ with $x = y$ and arbitrarily large $\max\{N, M\}$. For if $\Phi_N(x, u) = 0$, $\Phi_M(x, v) = 0$ then u, v are Hecke equivalent, and one need only choose N, M such that this Hecke equivalence is given by Φ_K. Further, any weakly special curve whose fixed coordinate is in the Hecke orbit of a rational number will admit rational solutions with arbitrarily large $\max\{N, M\}$ coming from the non-fixed coordinate. But if we require $\min\{N, M\} \geq L$ then only special subvarieties admit such points for arbitrarily large L (under SGH for $x \in \mathbb{Q}$ or unconditionally with $\max\{N, M\}$ prime).

This suggests the following "Fermat–Mordell" statement, in which a *weakly special subvariety* of $\mathbb{G}_{\mathrm{m}}^k$ is a coset of an algebraic subtorus. It is a consequence of the *abc* Conjecture (see e.g. [6, Ch. 12] and below).

4.1. Conjecture. *Let $V \subset \mathbb{G}_{\mathrm{m}}^2$ be a curve that is not a weakly special subvariety. There is $n(V)$ such that there are no rational points $(x^n, y^m) \in V$, $x, y \in \mathbb{Q}$, $x, y \neq 0, \pm 1$ with $n, m \geq n(V)$.*

Note that 4.1 is formulated in a slightly weaker form than the analogy with 1.3 would suggest (which would be $\max\{n, m\} \geq n(V)$), in order to avoid counterexamples if one exponent is small. For example, $u + v = 1$ contains (lots of) points of the form $u = x^n, v = y$, with $x, y \in \mathbb{Q}$ and arbitrarily large n. This form is also adopted in subsequent conjectures.

One could formulate still more general conjectures addressing solutions in the image of $(\mathbb{Q}^\times)^2$ under morphisms $(\mathbb{C}^\times)^2 \to (\mathbb{C}^\times)^2$ of large degree, or even correspondences, but this appears to require some care and we defer this for now. We do not discuss here precisely which multiplicative weakly special varieties contain infinitely many such points.

This conjecture clearly follows from Faltings's Theorem [10] if the genus $g(V) \geq 2$ (with $n(V) = 1$). If $g(V) \leq 1$ the relation on (x^n, y^m) could still be of genus one or less for some small n, m. These conjectures might be approachable for V an elliptic curve.

One can go further and state the following "Fermat–Mordell–Lang" formulation. Though apparently quite strong, it is nevertheless a consequence of the *abc* Conjecture.

4.2. Conjecture. *Let Γ be a finitely generated subgroup of $\mathbb{Q}^\times$. There are only finitely many points $(u, v) = (sx^n, ty^m)$ on $u + v = 1$ with $x, y \in \mathbb{Q}$, $s, t \in \Gamma$, and $n, m \geq 4$.*

4.3. Proposition. *The abc Conjecture implies Conjecture 4.2.*

Proof. Let Γ be a finitely generated subgroup of $\mathbb{Q}^\times$. Enlarging if necessary, we may assume that Γ is generated by -1 and some finite set $p_1, \ldots, p_k$ of prime numbers, and we set $P = p_1 \ldots p_k$. Now suppose we have a solution (u, v) to the equation in 4.2 with $n \geq m \geq 4$. Let us write $x = A/B$, $y = C/D$ where $A, B, C, D \in \mathbb{Z}$ are non-zero, with $(A, B) = (C, D) = 1$. By incorporating any p_i that occur as factors into s or t, we may assume that A, B, C, D are relatively prime to P (and positive). Multiplying through by a common denominator for s, t and B^n we have

$$SA^n + TC^m \frac{B^n}{D^m} = UB^n$$

where S, T, U are integers in Γ. We may assume they are relatively prime. Since $(D, CT) = 1$ we have $D^m | B^n$. Multiplying through by D^m however we conclude that $B^n | D^m$, hence they are equal. So we have

$$SA^n + TC^m = UB^n.$$

The largest term in absolute value is either TC^m or one of the terms involving an nth power. Changing signs if needed, let us assume first that our equation is as above,

with all terms positive. By the *abc* Conjecture (see e.g. [6, Ch. 12]) with $\epsilon = 1/4$ and $K = K_\epsilon$ we have

$$UB^n < K\mathrm{rad}\big(SA^nTC^mUB^n\big)^{1+\epsilon} \leq K\bigg(P\Big(\frac{U}{S}\Big)^{1/n}\Big(\frac{U}{T}\Big)^{1/n}B^3\bigg)^{5/4}.$$

Since $n \geq 4$ we find

$$U^{3/8}B^{1/4} \leq KP^{5/4}.$$

Then U, B are bounded, whence S, T, A, C are also bounded. The other case, when TC^m is largest, is similar. □

Of course one can also formulate a generalisation of 4.2 for with a general (non-weakly-special) curve in place of $u + v = 1$. Note that the modular analogues of these do hold under SGH for $x \in \mathbb{Q}$ (or unconditionally for tuples of isogenies where the largest degree is prime). That is because the notion of "generation" in the modular setting is rather weak: the analogous statement is to seek points $(u, v) : u + v = 1$ where each of u, v is either in the union of finitely many Hecke orbits or is in the Hecke orbit of a rational number under a modular correspondence of large (prime) degree.

5. Generalisation to higher-dimensional varieties

The proof of Theorems 1.1 and 1.3 generalise without difficulty to higher dimensions, under the assumption of SGH for $x \in \mathbb{Q}$ in generalising 1.3.

5.1. Definition. A *special subvariety* of $Y(1)^k$ is an irreducible component of the intersection of (any number of) subvarieties of the following form: $x_i = c$ where c is constant and special; $\Phi(x_k, x_\ell) = 0$ where Φ is a modular polynomial. For a *weakly special subvariety*, the constant coordinates need not be special. See e.g. [14, 15, 30].

5.2. Theorem. *Let $V \subset Y(1)^k$. Then there exists $L(V)$ with the following property. Suppose $u = (u_1, \ldots, u_k) \in V$ with $\Phi_{N_i}(x_i, u_i) = 0$ (where N_i is minimal with this property if x_i is special), $x_i \in \mathbb{Q}$, $i = 1, \ldots, k$. Let $N = \max\{N_i\}$. Assume $N \geq L(V)$ and further that*

(a) *N is a prime number, or*

(b) *SGH holds for $x \in \mathbb{Q}$*

then u lies in a positive dimensional weakly special variety contained in V.

Proof of 5.2. Let $K \subset \mathbb{C}$ be finitely generated field of definition of V. We take a definable family of sets

$$Z_Q = \{(g_1, \ldots, g_k) \in \mathrm{GL}_2^+(\mathbb{R})^k : \\ g_i z_i \in F, i = 1, \ldots, k, (j(g_1 z_1), \ldots, j(g_k z_k) \in V\}$$

parameterised by points $Q = (z_1, \ldots, z_k) \in \mathbb{H}^k$. Then a point $u = (u_1, \ldots, u_k)$ with $\Phi_{N_i}(x_i, u_i), i = 1, \ldots, k$ and large $L = \max\{N_i\}$ has (by the results of [27] in case (a) and by SGH for $x \in \mathbb{Q}$ in case (b)) "many" conjugates over K, and gives rise to a Q for which Z_Q has "many" rational points. By the Counting Theorem, we get a real algebraic arc in Z_Q containing "many" of these points, and from it a real algebraic arc in $\{(z_1, \ldots, z_k) : (j(z_1), \ldots, j(z_k)) \in V\}$, hence a complex algebraic curve contained there which, by the Ax–Lindemann theorem for the modular function [30], is contained in a positive dimensional weakly special subvariety contained there, and it must be defined over $\overline{K}$, as all coordinates of u and its conjugates are. The conjugates of this weakly special subvariety (over K) contain all the conjugates of u. □

If one looks for points with large $\min\{N_i\}$, then (by an inductive argument) only strongly special subvarieties survive: under the same hypotheses and assumptions, there is $L'(V)$ such that every point in V of this form with $\min\{N_i\} \geq L'$ (and all N_i are prime for the unconditional version) lies in a special subvariety contained in V.

By analogy, one can formulate a conjectural generalisation of FLT in the setting of subvarieties of multiplicative groups. As observed above, some weakly special subvarieties of $\mathbb{G}_{\mathrm{m}}^k$ do have rational points which are arbitrarily large powers.

5.3. Conjecture. *Let $V \subset \mathbb{G}_{\mathrm{m}}^k$. There is a positive integer $n(V)$ such that if $P = (x_1^{n_1}, \ldots, x_k^{n_k}) \in V(\mathbb{Q})$, with all $x_i \in \mathbb{Q}^\times, x_i \neq \pm 1$ and $n_i \geq n(V)$, then P lies in a positive dimensional weakly special subvariety of $\mathbb{G}_{\mathrm{m}}^k$ contained in V.*

The General Lang Conjecture [6, 14.3.7] implies that all but finitely many such points lie in the *special set* of V. In the next section we will see that we can prove the analogue of 5.3, for the *inverse* Fermat equation.

Let SGH_d denote the special case of SGH in which $[\mathbb{Q}(x) : \mathbb{Q}] \leq d$. Under the assumption of SGH_d, the proofs of 1.3 and 5.2(b) go through if x, y are restricted to be of degree at most d over $\mathbb{Q}$. One could then formulate all the conjectures above in this stronger form, with the hypothesis on the exponents now depending on V, Γ, d. The following conjecture is the most ambitious statement taking up all these variants.

5.4. Conjecture. *Let $V \subset \mathbb{G}_{\mathrm{m}}^k$ be a subvariety defined over $\mathbb{C}$, let Γ be a finite rank subgroup of $\mathbb{C}^\times$, and let $d \geq 1$. There exists a constant $n(V, \Gamma, d)$ with the following property. Suppose $P = (u_1, \ldots, u_k) \in V$ is a point such that, for $i = 1, \ldots, k$, we have $u_i = s_i x_i^{n_i}$ with $s_i \in \Gamma$, x_i not a root of unity, $[\mathbb{Q}(x_i) : \mathbb{Q}] \leq d$ and $n_i \geq n(V, \Gamma, d)$ then P lies in a positive-dimensional weakly special variety contained in V.*

It seems interesting to investigate whether Vojta's conjectures (see e.g. [6, Ch. 14]), which do imply Mordell–Lang, imply the above.

Let us conclude this section with a somewhat different generalisation of 1.3, and a further conjecture in the multiplicative setting. We enunciate a different weakening of SGH.

5.5. Weak Galois-Orbit Hypothesis (WGH). Let F be a number field. There exists constants $c = c(F), \delta = \delta(F)$ such that if $(x, y) \in F \times \overline{\mathbb{Q}}$ are not special and $\Phi_N(x, y) = 0$ then $[F(y) : F] \geq cN^{\delta}$.

5.6. Theorem. *Assume WGH holds. Let K be a finitely generated subfield of $\mathbb{C}$, and let $V \subset Y(1)^k$. Then there exists an integer $L = L(K, V)$ with the following property. If $u = (u_1, \ldots, u_k) \in V$ with $\Phi_{N_i}(x_i, u_i) = 0$, $x_i \in K$ and N_i minimal having $\Phi_{N_i}(x_i, u_i) = 0$, $i = 1, \ldots, k$, and $\max\{N_i\} \geq L$ then u lies in a positive dimensional weakly special subvariety contained in V.*

Proof. We may assume that V is defined over K. Let $F = K \cap \overline{\mathbb{Q}}$. Then F is finitely generated (see [8, §12.4] or [16, Th. 24.9]), and hence is a number field. Suppose $N_i = \max\{N_j, j = 1, \ldots, k\}$. For $x_i \in F$ and large N_i the conclusion follows using WGH and the proof of 5.2(b). For non-algebraic x_i (and then also u_i) we apply Lemma 7.3 below to conclude that $[K(y) : K] \geq cN_i^{\delta}$ for suitable c, δ depending on K, and then follow the proof of 5.2(b). □

It is then natural to conjecture the analogous statement in the multiplicative setting.

5.7. Conjecture. *Let K be a finitely generated subfield of $\mathbb{C}$. Let $V \subset \mathbb{G}_{\mathrm{m}}^k$. There exists an integer $n = n(K, V)$ such that if $P = (x_1^{n_1}, \ldots, x_k^{n_k}) \in V$, with $x_i \in K^{\times}$ but not a root of unity, and $n_i \geq n(V)$, for all $i = 1, \ldots, k$, then P lies in a positive dimensional weakly special subvariety of $\mathbb{G}_{\mathrm{m}}^k$ contained in V.*

I do not know whether this statement in the case of plane curves follows from the *abc* conjecture. In the special case of $V \subset \mathbb{G}_{\mathrm{m}}^2$ defined by $u + v = 1$, it asserts the impossibility of solving this equation in $K^{\times n}$, where K is a finitely generated field over $\mathbb{Q}$, for large n (depending on K).

6. Other settings and inverse Fermat

It is natural to consider analogues in the setting of abelian varieties. The most natural analogue of 1.3 for an elliptic curve E in place of $\mathbb{G}_{\mathrm{m}}$ is the following statement, which is a consequence of Mordell–Lang (ML; Faltings's Big Theorem [11]) for $E \times E$. A *weakly special subvariety* of an abelian variety is a translate of an abelian subvariety.

6.1. A consequence of ML. Let E be an elliptic curve (defined over $\mathbb{C}$), and let $C \subset E \times E$ be a curve which is not weakly special. There exists $L = L(E, C)$ with the following property. If $X, Y, U, V \in E$ are points such that: $U = [n]X$, $V = [m]Y$, $(U, V) \in C$, $X, Y \in E(\mathbb{Q})$ then $n, m \leq L$.

Since $E(\mathbb{Q})$ is finitely generated, U, V are in a finitely generated subgroup of $E \times E$. The statement then follows from ML for $E \times E$.

One can consider a variant formulation. Let E be an elliptic curve in the form $y^2 = x^3 + ax + b$. Multiplication by n on E induces an operation on $\mathbb{C}$ as follows: $[n]x = z$ if $[n](x, y) = (z, w)$ on E. There is a corresponding notion of "weakly special" variety in $\mathbb{C}^2$, comprising vertical and horizontal lines and the curves where $[n]x = [m]y$ identically for some n, m.

6.2. Conjecture. *Let E as above and $V \subset \mathbb{C}^2$ not "weakly special". There exists $L = L(E, V)$ with the following property. If $x, y \in \mathbb{Q}$ and $([n]x, [m]y) \in V$ then $\max\{n, m\} \leq L$.*

This statement is presumably not a consequence of ZP (as the points with rational x are not finitely generated).

We now consider the analogue of Conjecture 5.3 for the inverse Fermat equation: after all, $\Phi_n(x, u) = 0$ is likewise the analogue of $x = u^n$. On the inverse Fermat equation itself see e.g. Lenstra [22].

Recall that, if K is a field, $c \in K$, the polynomial $x^n - c$ is reducible over K iff $c \in K^p$ for some prime number $p|n$, or $c \in -4K^4$ and $4|n$ (see e.g. Lang [20, VI, 9.1]). The first condition is a natural minimality for u with $u^n = c \in K$: it guarantees that n is the *order* of u over K in that no smaller power of u lies in K. The second condition reflects the example $x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$. Under the first condition only, one can get a lower bound on $[K(u) : K]$, when $K = \mathbb{Q}$, from results of Risman [42].

6.3. Lemma. *Let θ have order n over $\mathbb{Q}$. Then $[\mathbb{Q}(\theta) : \mathbb{Q}] \gg_\epsilon n^{1/2-\epsilon}$ for any $\epsilon > 0$.*

Proof. Write $h = [\mathbb{Q}(\theta) : \mathbb{Q}]$. By [42, Cor. 2], we have $n = t\ell$ where ℓ divides h and $\phi(t)$ divides h (and t is square-free). Either t or ℓ must exceed $\sqrt{n}$. □

6.4. Theorem. *Let $V \subset \mathbb{G}_{\mathrm{m}}^k$. There is a positive integer $n(V)$ with the following property. Suppose $P = (u_1, \ldots, u_k) \in V$ and, for each $i = 1, \ldots, k$, $u_i^{n_i} = x_i$ where $x_i \in \mathbb{Q}^\times$, and n_i is the order of u_i over $\mathbb{Q}$. Suppose $\max\{n_1, \ldots, n_k\} \geq n$. Then P lies in a positive-dimensional weakly special variety contained in V.*

Proof. Under our assumptions, by Lemma 6.3, the point $(u_1, \ldots, u_k)$ has degree at least $c \max\{n_1, \ldots, n_k\}^\delta$ over $\mathbb{Q}$ for some absolute c, δ, and hence will have large degree over some fixed finitely generated field of definition of V. Let $F = \mathbb{R} \times [0, 2\pi]i$, a fundamental domain for the action of $2\pi i\mathbb{Z}$ on $\mathbb{C}$ by translation. The restriction $\exp : F \to \mathbb{C}^\times$ of the exponential function is definable in $\mathbb{R}_{\text{an exp}}$. We take the definable family of sets

$$Z_Q = \{(r_1, \ldots, r_k) \in \mathbb{R}^k : z_j = 2\pi i r_j \in F, j = 1, \ldots, k, \\ \text{and } (\exp(z_1 + 2\pi i r_1), \ldots, \exp(z_k + 2\pi i r_k)) \in V\}.$$

parameterised by points $Q = (z_1, \ldots, z_k) \in \mathbb{C}^n$. The rest of the proof is the same as the proof of 5.2, using the Ax–Lindemann theorem for exp (a special case of Ax–Schanuel [4]). □

7. Proof of Theorem 1.4

In this section we prove Theorem 1.4. The key point is that modular curves have large gonality, and this implies that transcendental points $(x, y) : \Phi_N(x, y) = 0$ give rise to extensions of large degree over an arbitrary (but fixed) finitely generated extension of $\mathbb{Q}$. We first give a statement of the Zilber–Pink conjecture (ZP) for subvarieties of $Y(1)^k$. See [15] for various alternative formulations.

7.1. Definition. Let $V \subset Y(1)^k$. A subvariety $A \subset V$ is called *atypical* (for V in $Y(1)^k$) if there is a special subvariety $T \subset Y(1)^k$ such that $A \subset V \cap T$ and

$$\dim A > \dim V + \dim T - k.$$

7.2. Zilber–Pink Conjecture for $Y(1)^k$. Let $V \subset Y(1)^k$. Then V has only finitely many maximal atypical subvarieties.

7.3. Lemma. *Let K be a finitely generated subfield of $\mathbb{C}$. There exist positive constants c, δ (depending on K) with the following property. Let $P = (x, y) \in \mathbb{C}^2$ be a point with non-algebraic coordinates such that $\Phi_N(x, y) = 0$. Then*

$$[K(x, y) : K] \geq cN^{\delta}.$$

Proof. Let us write $K = L(\kappa)$ where L is a pure transcendental extension of $\mathbb{Q}$ and $[K : L]$ is a finite algebraic extension. Do this minimising $[K : L]$ say. Write $L = \mathbb{Q}(t_1, \ldots, t_n)$ with the t_i independent transcendental elements.

For a curve C over a field F with function-field $F(C)$ we write $d_F(C)$ for its *gonality*: the minimum extension degree $[F(C) : F(t)]$ over $t \in F(C)$.

Let P be such a point. We may assume that x, y are algebraic over K. Let us choose $t_1, \ldots, t_m$ such that x (and hence y) are algebraic over $t_1, \ldots, t_m$ but not over $t_1, \ldots, t_{m-1}$. Let $M = \mathbb{Q}(t_1, \ldots, t_{m-1})$ and write $t = t_m$. The extension of fields $M(t, x, y)/M(x, y)$ corresponds to a dominant morphism of curves over M. Thus

$$d_M(M(t, x, y)) \geq d_M(M(x, y))$$

(see e.g. Poonen [38], where this fact is proved but described as well known). Let $d_{\mathbb{C}}(\Phi_N(x, y) = 0)$ denote the $\mathbb{C}$-gonality of the modular curve. Then we have

$$d_M(M(x, y)) \geq d_{\mathbb{C}}(\Phi_N(x, y) = 0).$$

Now $d_{\mathbb{C}}(\Phi_N(x, y) = 0) \geq c_0 N$ for some positive constant c_0 (see [51] and also [1] where an explicit such bound is given). Therefore

$$[L(x, y) : L] = [M(t, x, y) : M(t)] \geq c_0 N,$$

and so $[K(x, y) : K] \geq c_1 N$ with $c_1 = c_0/[K : L]$. This proves the lemma. □

7.4. Proof of Theorem 1.4. For $A \subset Y(1)^k$, write $\langle A \rangle$ for the smallest special subvariety of $Y(1)^k$ containing A. If $\langle V \rangle \neq Y(1)^3$ then V is atypical, and is then the unique maximal atypical subvariety. Conversely, if V is atypical then it must be contained in a proper special subvariety. So we may assume that V is not contained in any proper special subvariety, and that atypical subvarieties of V are points which are contained in some special subvariety of codimension 2.

Suppose two coordinates, say x, y, are constant on V. They must be non-special and not in the same Hecke orbit. So a point (x, y, z) satisfying two special relations must be either a special point z that is in the Hecke orbit of either x or y (but then x or y would be special), or a z which is in the Hecke orbit of both x and y (but then x and y would be in the same Hecke orbit). Both are impossible.

Suppose just one coordinate, say x, is constant. Then the image V_{yz} of V under projection to the y, z-plane is a non-special curve, and we seek points which are either special or in the Hecke orbit of x. Finiteness follows by "Modular Mordell–Lang" [14, 31].

So we may assume that no coordinate is constant on V. We are looking for points $P = (x, y, z)$ satisfying two special relations. Let P be such a point. It has one of the following forms: it is defined by two coordinates being special; or by one coordinate being special and a modular relation on the other two coordintates; or by modular relations between two distinct pairs of coordinates.

Now if two coordinates are special, then we get a special point on the image of V under projection to those coordinates. This image is not special (since $\langle V \rangle = Y(1)^3$), and so for each choice of pair of coordinates there are only finitely many such points.

If P is a point of the second type, we distinguish two subcases. In the first subcase, the two modular related points are algebraic. Then P is an algebraic point of V and in a finite set. In the second subclass, the two modular-related coordinates are transcendental over $\overline{\mathbb{Q}}$. Such P then has "many" conjugates over K, by a combination of Lemma 7.3 and Landau–Siegel. We conclude this case by o-minimality and point-counting, much as we deal with the following final case.

The last case concerns points P satisfying modular relations on two distinct sets of coordinates. So all three coordinates of P are in the same Hecke orbit. By Lemma 7.3, P has "many" conjugates over K, and thus V contains "many" points P' which are intersections with special subvarieties of the same complexity as the one containing P.

Let $Z \subset \mathbb{H}^3$ be the preimage of V in $\mathbb{H}^3$ intersected with F^3, where F is the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$. Then Z is definable. For $g, h \in \mathrm{GL}_2^+(\mathbb{R})$ we have the Mobius subvariety $M_{g,h} \subset \mathbb{H}^3$ defined by

$$M_{g,h} = \{(u, gu, hgu) \in \mathbb{H}^3 : u \in \mathbb{H}\}.$$

We consider the following definable subset of $\mathrm{GL}_2^+(\mathbb{R})^2$:

$$W = \{(g, h) : M_{g,h} \cap Z \neq \emptyset\}.$$

Each conjugate P' of P over K gives rise to a rational point $(g, h) \in W$ whose height is $\leq c\langle P\rangle^C$, and we get $\geq c'\langle P\rangle^{C'}$ such points. By the Counting Theorem, W contains positive-dimensional semi-algebraic sets, and the intersection points of the corresponding Mobius subvarieties with Z must move, by the same argument used in [14], in order to account for the "many" distinct pre-images of the P'.

Complexifying the real parameter of the moving family of Mobius subvarieties we get a complex surface in $\mathbb{H}^3$ which intersects Z in a set of at least one real dimension, and hence in a set of one complex dimension, and so contains the premiere of V. By Ax–Schanuel [34] (though in this case in fact just the special case "Ax-Logarithms" established in [14]), V is contained in a proper weakly special subvariety of $\mathbb{C}^3$.

But this is a contradiction, as V is not contained in a proper special subvariety (by hypothesis), and no coordinate is constant on V (as we reduced to this case).

7.5. Proposition. *Let $V \subset Y(1)^4$ be a curve which is not contained in any proper special subvariety and assume that no image of V under a coordinate projection to $Y(1)^3$ is defined over $\overline{\mathbb{Q}}$. Then there are only finitely many points $(w, x, y, z) \in V$ such that, for some N, M, $\Phi_N(w, x) = 0, \Phi_M(y, z) = 0$.*

Proof. Suppose two coordinates are constant on V. Say w is one of them. If x is also constant we cannot have $\Phi_N(w, x) = 0$, for then V would be contained in a proper special; and for other x there are no points of the required form. If, say, z is also constant then x, y are non-constant (by above) and V projects to a curve V_{xy} in the xy-plane. We are looking for points in V_{xy} whose x, y coordinates are in the Hecke orbits of w, z, respectively, and finiteness follows by Modular Mordell–Lang as above.

Suppose just one coordinate, say w is constant. So y, z are non-constant and satisfy some algebraic relation. If this relation is not defined over $\overline{\mathbb{Q}}$ then, with finitely many exceptions, the sought points have y, z non-algebraic. Let K be a finitely generated field of definition of V. Then $[K(x) : K] \geq cN^\delta$ for some $c, \delta > 0$ by isogeny estimates, and $[K(y, z) : K] > cM^\delta$ for some $c, \delta > 0$ by gonality, and an argument using o-minimality, point-counting and Modular Ax–Lindemann concludes as above.

So we can suppose that no coordinates are constant on V, and so every pair of coordinates satisfy some algebraic relation. Suppose neither of the relations $R(w, x) = 0$, $S(y, z) = 0$ are defined over $\overline{\mathbb{Q}}$. Then, with finitely many exceptions, each pair $(w, x), (y, z)$ consists of transcendental points. These have large degree over K in relation to the complexity $\max\{N, M\}$, and we conclude as above.

If on the other hand both these pairs of relations are over $\overline{\mathbb{Q}}$ then w, x, y, z are all algebraic, and there are only finitely many points when even three of the coordinates are, under our hypotheses.

We are reduced to the case that $R(w, x) = 0$, say, is defined over $\overline{\mathbb{Q}}$, but $S(y, z) = 0$ is not. Consider the curve image V_{xyz} under projection to the xyz coordinates. We are looking for points where x is algebraic, and y, z have a modular

relation. If V_{xyz} is not contained in a proper subvariety of $Y(1)^3$ defined over $\overline{\mathbb{Q}}$ then the finiteness of such (x, y, z) is a trivial consequence of the main theorem of [7].

So we may assume that V_{xyz} is contained in a proper subvariety W defined over $\overline{\mathbb{Q}}$, defined say by $P(x, y, z) = 0$. We observe that there can be only finitely many x for which the relation $P(x, y, z)$ on y, z is divisible by modular relation. For other x, if x is algebraic and $\Phi_M(y, z) = 0$ then y, z must also be algebraic, and there are only finitely many such points. □

7.6. Theorem. *Let $V \subset Y(1)^k$ be a curve such that no image of it under projection to three coordinates is defined over $\overline{\mathbb{Q}}$. Then ZP holds for V.*

Proof. As above, we may assume that V is not contained in any proper special subvariety of $Y(1)^k$. We consider atypical points, and these involve either 2 coordinates (for two points being special), or 3 coordinates, or 4 coordinates (the case of modular correspondences between disjoint pairs of coordinates). In each case, finiteness is covered by either 7.4 or 7.5. □

8. SGH and GO1

In this section we show that SGH in fact implies the statement formulated as GO1 in [15], of which it is a special case.

We define the *complexity* of a special subvariety as follows. If $x \in \mathbb{C}$ is special, we denote by $D(x)$ the discriminant of the corresponding quadratic order (i.e. the endomorphism ring of the elliptic curve E with j-invariant x). Alternatively, $D(x)$ is the discriminant $b^2 - 4ac$ where $az^2 + bz + c = 0$ is the minimal polynomial of some pre-image $z = j^{-1}(x)$ of x over $\mathbb{Z}$.

8.1. Definition. The *complexity* of a special subvariety $T \subset Y(1)^k$ is

$$\Delta(T) = \max\{D(x_i), N(x_h, x_\ell)\}$$

where $D(x_i)$ ranges over all constant coordinates, and $N(x_h, x_\ell) = N$ if x_h, x_ℓ are non-constant coordinates which are related by a modular polynomial Φ_N, and we range over all such related pairs.

8.2. Formulation GO1 [15]. Let $V \subset Y(1)^k$ be defined over a field K which is finitely generated over $\mathbb{Q}$. There are positive constants c, η with the following property. If $P \in V$ defined over a field extension of K then $[K(P) : K] \geq c\Delta(\langle P \rangle)^\eta$.

8.3. Proposition. *SGH implies GO1 for the subvarieties $Y(1)^k \subset Y(1)^k$, $k = 1, 2, \ldots$ as subvarieties defined over $\mathbb{Q}$.*

Proof. Suppose $x = (x_1, \ldots, x_k) \in Y(1)^k$. Some x_i may be special, and some pairs of coordinates may be related by modular polynomials. For the special x_i we have Landau–Siegel. Suppose $x_{i_1}, \ldots, x_{i_k}$ are all in the same Hecke orbit. The complexity

of $\langle(x_{i_1},\dots,x_{i_k})\rangle$ is then the maximum N of the N_{ab} such that $\Phi_{N_{ab}}(x_{i_a},x_{i_b})=0$, and by SGH we have $[\mathbb{Q}(x_1,\dots,x_n):\mathbb{Q}]\geq cN^{\delta}$. □

8.4. Proposition. *GO1 for $Y(1)^k\subset Y(1)^k$, $k=1,2,\dots$ implies GO1 in general.*

Proof. Assume the truth of GO1 for $Y(1)^n\subset Y(1)^n, n=1,2,\dots$ and let $V\subset Y(1)^n$ defined over a field K finitely generated over $\mathbb{Q}$. Let us write $K=L(\kappa)$ where L is purely transcendental over $\mathbb{Q}$ and $[K:L]$ is algebraic. Let $P=(x_1,\dots,x_n)\in V$. We may suppose all coordinates are algebraic over K.

Some coordinates of P may be special, and some related by modular polynomials. If x_i is special, then it is algebraic and its degree over $\mathbb{Q}$ is bounded below by $c\Delta(x)^{\delta}$ be Landau–Siegel. If $\Phi_N(x_i,x_j)$ then we distinguish two cases. If one (and hence both) x_i,x_j are algebraic, the required lower bound follows from SGH. If they are not algebraic, then $[\mathbb{Q}(x_i,x_j):\mathbb{Q}(x_i)]=\deg\Phi_N$, and the required degree bound follows via the gonality argument in the proof of 7.2. □

Note that GO1, is stronger than the conjectured "LGO" used in [15] to give a conditional proof of the Zilber–Pink conjecture for $Y(1)^k$ (a second condition in [15], a suitable "Ax–Schanuel" statement for the modular function, has subsequently been affirmed in [34]). Thus SGH implies the full Zilber–Pink conjecture for $Y(1)^k$.

Acknowledgements. I am grateful to Peter Sarnak for several helpful discussions, and I thank Jordan Ellenberg, Gareth Jones, and the referee for helpful comments, suggestions, and corrections. The work was partially supported by grants from the EPSRC (EP/J019232/1 and EP/N008359/1).

References

[1] D. Abramovich, A linear lower bound for the gonality of modular curves, *Internat. Math. Res. Notices*, **1996** (1996), no. 20, 1005–1011. Zbl 0878.14019 MR 1422373

[2] Y. André, *G-functions and geometry*, Aspects of Mathematics, E13, Vieweg, Braunschweig, 1989. Zbl 0688.10032 MR 0990016

[3] Y. André, Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire, *J. Reine Angew. Math.*, **505** (1998), 203–208. Zbl 0918.14010 MR 1662256

[4] J. Ax, On Schanuel's conjectures, *Ann. of Math. (2)*, **93** (1971), 252–268. Zbl 0232.10026 MR 0277482

[5] Y. Bilu and P. Parent, Serre's uniformity problem in the split Cartan case, *Ann. of Math. (2)*, **173** (2011), 569–584. Zbl 1278.11065 MR 2753610

[6] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Mathematical Monographs, 8, Cambridge University Press, 2006. Zbl 1115.11034 MR 2216774

[7] Z. Chatzidakis, D. Ghioca, D. Masser, and G. Maurin, Unlikely, likely and impossible intersections without algebraic groups, *Atti Acad. Naz. Lincei Rend. Lincei Mat. Appl.*, **24** (2013), 485–501. Zbl 1320.11060 MR 3129750

[8] P. Clark, *Field Theory*, web notes. Available at: `http://math.uga.edu/~pete/`

[9] L. van den Dries and A. Günaydin, The fields of real and complex numbers with a small multiplicative group, *Proc. London Math. Soc.*, **93** (2006), 43–81. Zbl 1101.03028 MR 2235481

[10] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörperen, *Invent. Math.*, **73** (1983), 349–366. Zbl 0588.14026 MR 0718935

[11] G. Faltings, Diophantine approximation on abelien varieties, *Ann. of Math. (2)*, **133** (1991), 549–576. Zbl 0734.14007 MR 1109353

[12] G. Frey, Curves with infinitely many points of fixed degree, *Israel J. Math.*, **85** (1994), 79–83. Zbl 0808.14022 MR 1264340

[13] É. Gaudron and G. Rémond, Théorème des périodes et degrés minimaux d'isogénies, *Comment. Math. Helv.*, **89** (2014), 343–403. Zbl 1297.11058 MR 3225452

[14] P. Habegger and J. Pila, Some unlikely intersections beyond André–Oort, *Compos. Math.*, **148** (2012), 1–27. Zbl 1288.11062 MR 2881307

[15] P. Habegger and J. Pila, O-minimality and certain atypical intersections, *Ann. de l'Éc. Norm. (4)*, **49** (2016), no. 4, 813–858. Zbl 06680006 MR 3552014

[16] I. M. Isaacs, *Algebra: a graduate course*, reprint of the 1994 original. Graduate Studies in Mathematics, 100, AMS, Providence, RI, 2009. Zbl 1157.00004 MR 2472787

[17] B. Klingler and A. Yafaev, The André–Oort conjecture, *Ann. of Math. (2)*, **180** (2014), 867–925. Zbl 06380809 MR 3245009

[18] L. Kühne, An effective result of André–Oort type, *Ann. of Math. (2)*, **176** (2012), 651–671. Zbl 1341.11035 MR 2925393

[19] S. Lang, Integral points on curves, *Inst. Hautes Études Sci. Publ. Math.*, **6** (1960), 319–335. Zbl 0112.13402 MR 0130219

[20] S. Lang, *Algebra*, revised third edition, Graduate Texts in Mathematics, 211, Springer, New York, 2002. Zbl 0984.00001 MR 1878556

[21] M. Laurent, Équations diophantiennes exponentielles, *Invent. Math.*, **78** (1984), 299–327. Zbl 0554.10009 MR 0767195

[22] H. W. Lenstra, On the inverse Fermat equation, *Discrete Math.*, **106/107** (1992), 329–331. Zbl 0766.11018 MR 1181928

[23] P. Liardet, Sur une conjecture de Serge Lang, *Asterisque*, **24-25** (1975), 187–210. Zbl 0315.14005 MR 0376688

[24] H. B. Mann, On linear relations between roots of unity, *Mathematika*, **12** (1965), 107–117. Zbl 0138.03102 MR 0191892

[25] D. Masser and G. Wüstholz, Isogeny estimates for abelian varieties, and finiteness theorems, *Ann. of Math. (2)*, **137** (1993), 459–472. Zbl 0804.14019 MR 1217345

[26] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.*, **124** (1996), 437–449. Zbl 0936.11037 MR 1369424

[27] F. Najman, Isogenies of non-CM elliptic curves with rational j-invariants over number fields, to appear in *Math. Proc. Camb. Phil. Soc.* arXiv:1506.03127

[28] F. Oort, Canonical lifts and dense sets of CM points, *Arithmetic Geometry (Cortona, 1994)*, F. Catanese (ed.), 228–234, Symposia. Math., XXXVII, Cambridge Univ. Press, 1997. Zbl 0911.14018 MR 1472499

[29] F. Pellarin, Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques, *Acta Arith.*, **100** (2001), 203–243. Zbl 0986.11046 MR 1865384

[30] J. Pila, O-minimality and the André–Oort conjecture for $\mathbb{C}^n$, *Ann. of Math. (2)*, **173** (2011), 1779–1840. Zbl 1243.14022 MR 2800724

[31] J. Pila, Special point problems with elliptic modular surfaces, *Mathematika*, **60** (2014), 1–31. Zbl 06347372 MR 3164515

[32] J. Pila, O-minimality and Diophantine geometry, in *Proceedings of the ICM, (Seoul, 2014)*, S. Y. Jang, Y. R. Kim, D.-W. Lee, and I. Yie, (eds.), Vol. I, 547–572, Kyang Moon SA, Seoul, 2014. Zbl 1314.00103

[33] J. Pila and J. Tsimerman, Ax–Lindemann for $\mathcal{A}_g$, *Ann. of Math. (2)*, **179** (2014), 659–681. Zbl 1305.14020 MR 3152943

[34] J. Pila and J. Tsimerman, Ax–Schanuel for the j-function, *Duke Math. J.*, **165** (2016), no. 13, 2587–2605. Zbl 06650079 MR 3546969

[35] J. Pila and A. J. Wilkie, The rational points of a definable set, *Duke Math. J.*, **133** (2006), 591–616. Zbl 1217.11066 MR 2228464

[36] J. Pila and U. Zannier, Rational points in periodic analytic sets and the Manin–Mumford conjecture, *Rend. Lincei Mat. Appl.*, **19** (2008), 149–162. Zbl 1164.11029 MR 2411018

[37] R. Pink, A common generalization of the conjectures of André–Oort, Manin–Mumford, and Mordell–Lang, 17 April, 2005. Available from: `http://www.math.ethz.ch/~pink/`

[38] B. Poonen, Gonality of modular curves in characteristic p, *Math. Res. Lett.*, **14** (2007), 691–701. Zbl 1138.14016 MR 2335995

[39] M. Raynaud, Courbes sur une variété abélienne et points de torsion, *Invent. Math.*, **71** (1983), no. 1, 207–233. Zbl 0564.14020 MR 0688265

[40] M. Raynaud, Sous-variétés d'une variété abélienne et points de torsion, in *Arithmetic and Geometry, Volume I*, 327–352, Progr. Math., 35, Birkhäuser, Boston, MA, 1983. Zbl 0581.14031 MR 0717600

[41] M. Rebolledo, Merel's theorem on the boundedness of the torsion of elliptic curves, in *Arithmetic geometry*, 71–82, Clay Math. Proc., 8, Amer. Math. Soc., Providence, RI, 2009. Zbl 1250.11059 MR 2498054

[42] L. J. Risman, On the order and degree of solutions of pure equations, *Proc. Amer. Math. Soc.*, **55** (1976), 261–266. Zbl 0327.12102 MR 0396508

[43] P. Sarnak and S. Adams, Betti numbers of congruence subgroups (with an appendix by Z. Rudnick), *Israel J. Math.*, **88** (1994), 31–72. Zbl 0843.11027 MR 1303490

[44] C.-L. Siegel, Über einige Anwendungen diophantischer Approximationen, reprint of *Abh. Preuss. Akad. Wissen. Phys. Math. Kl. (1929)*, 41–69 (German). English translation by C. Fuchs in *On Some Applications of Diophantine Approximations*, 81–138, Quad./Monogr., 2, Ed. Norm., Pisa, 2014. Zbl 1311.11006 MR 3330350

[45] J. Tsimerman, A proof of the André–Oort conjecture for $\mathcal{A}_g$, 2015. arXiv:1506.01466

[46] E. Ullmo and A. Yafaev, Galois orbits and equidistribtuion of special subvarieties: towards the André–Oort conjecture, *Ann. of Math. (2)*, **180** (2014), 823–865. Zbl 1328.11070 MR 3245008

[47] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math. (2)*, **141** (1995), 443–551. Zbl 0823.11029 MR 1333035

[48] A. J. Wilkie, Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function, *J. Amer. M. Soc.*, **9** (1996), 1051–1094. Zbl 0892.03013 MR 1398816

[49] U. Zannier, Some Problems of Unlikely Intersections, in *Arithmetic and Geometry*, with appendices by D. Masser, Annals of Mathematics Studies, 181, Princeton University Press, 2012. Zbl 1246.14003 MR 2918151

[50] B. Zilber, Exponential sums equations and the Schanuel conjecture, *J. London Math. Soc. (2)*, **65** (2002), 27–44. Zbl 1030.11073 MR 1875133

[51] P. G. Zograf, Small eigenvalues of automorphic Laplacians in spaces of parabolic forms, *Zap. Nauchn. Sem. Leningrad Otdel. Mat. Inst. Steklov (LOMI)*, **134** (1984), 157–168 (Russian); English translation in *J. Soviet Math.*, **36** (1987), 106–114. Zbl 0609.10016 MR 0741858

Received March 03, 2016

J. Pila, Mathematical Institute, University of Oxford, Oxford OX2 6GG, UK
E-mail: jonathan.pila@maths.ox.ac.uk