Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

Polynomial and Fermat–Pell families that attain the Davenport–Mason bound

par Noam D. ELKIES et Mark WATKINS

Résumé. &c.

Abstract. etc.

1. Introduction and Motivation

The Masser-Oesterlé ABC conjecture [26, 28] famously links the additive and multiplicative structure of the ring of integers by asserting that if (A, B, C) are coprime integers with $A + B + C = 0$ then

$$¿ \qquad \max\bigl(|A|, |B|, |C|\bigr) \ll_\epsilon \Biggl(\prod_{p|ABC} p\Biggr)^{1+\epsilon} \qquad ?$$

for each $\epsilon > 0$. Oesterlé shows [28] that we cannot take $\epsilon = 0$ in this conjecture. Hall's conjecture is the important special case that arises when A and B are respectively a perfect cube and a perfect square, say $-x^3$ and y^2. This conjecture addresses nonzero values of small magnitude of $x^3 - y^2$ for integers x, y, and asserts that

$$¿ \qquad |x^3 - y^2| \gg_\epsilon x^{1/2-\epsilon} \quad \text{when } x > 0 \text{ and } x^3 \neq y^2. \qquad ?$$

Hall originally conjectured [18] that either $x^3 = y^2$ or $|x^3 - y^2| \gg \sqrt{|x|}$; it is now believed (though not proved) that that was too optimistic even in this special case of the ABC conjecture. Danilov [9] showed that at any rate the conjecture cannot hold with $\sqrt{|x|}$ replaced by $|x|^c$ for some $c > 1/2$.

The function field analogue of the ABC conjecture is known to be true, being the special case $g = 0$ of Mason's theorem (the "fundamental inequality" [25, p.14, Lemma 2]). Letting $N(P)$ be the conductor[1] of the polynomial P, Mason's theorem states that if (A, B, C) are relatively prime polynomials over a field of characteristic zero, and $A(t) + B(t) + C(t) = 0$, then

$$\max\bigl(\deg(A), \deg(B), \deg(C)\bigr) \leq \deg\bigl(N(ABC)\bigr) - 1.$$

[1] In analogy with the usual ABC conjecture, this is defined as the product of the irreducible monic factors of P.

We can then consider how small the degree of

$$X(t)^3 - Y(t)^2 = K(t) \tag{1}$$

can be (when $K \neq 0$) for polynomials X, Y. It is already a result of Davenport [10] (answering a question of Birch [4]) that if we take (X, Y) to be of degrees $(2m, 3m)$ respectively, then the degree of K is at least $m+1$. Later work of Stothers [35] is a precursor to the work of Mason, and gives a criterion concerning the case where $\deg(K) = m + 1$.

The Fermat–Pell version of this question is to ask for

$$X(t)^3 - Q(t)Y(t)^2 = L(t) \tag{2}$$

of small degree, where Q is quadratic. Integer solutions of the Fermat–Pell equation $Q(t) = u^2$ over the field generated by the coefficients of X, Y, Q then yield small values of $x^3 - y^2$ in the same field. Here X, Y are of degrees $2m, 3m - 1$, and $\deg(L)$ must attain the lower bound m of Mason's theorem.

Hall and Fermat–Pell polynomials also arise naturally in several Diophantine contexts beyond the Hall conjecture. Such polynomials yield examples of Belyĭ maps on $\mathbf{P}^1$, which for the first few values of m can be interpreted as natural maps between elliptic or Shimura modular curves. The small nonzero values of $|x^3 - y^2|$ that are the topic of Hall's conjecture correspond to small discriminants $12^3(x^3 - y^2)$ of elliptic curves $\eta^2 = \xi^3 - 3x\xi + 2y$; when $X(t)$ and $Y(t)$ are Hall polynomials, the same formula $\eta^2 = \xi^3 - 3X(t)\xi + 2Y(t)$ gives an elliptic surface over the t-line with a high-order multiplicative fiber at $t = \infty$. Hall and Fermat–Pell polynomials also yield sections of elliptic surfaces of the special form $\eta^2 = \xi^3 + A(t)$. Shioda [32] has exploited these connections with elliptic surfaces to explain some of the arithmetic behavior of these polynomials beyond what the known general theory of Belyĭ functions could predict.

1.1. Our goal. We wish to give explicit examples of Hall and Fermat–Pell polynomials (up to coordinate transformation) that minimise the degrees of K and L in (1) and (2) relative to X and Y. We first use the theory of Belyĭ maps to reduce the counting of the number of such solutions to an enumeration problem in group theory. The Hall cases were handled in [35, Theorem 4.6], though we only found this out after we had written a computer programme for enumeration. We have not considered a generalisation of the work of Stothers to the Fermat–Pell case, but instead just rely on our enumerations. We are able to give an exact enumeration in some of the smaller Fermat–Pell cases, and give a probabilistic method for use with the larger ones. Then we use a variety of techniques to exhibit solutions in both the Hall and Fermat–Pell cases. The most powerful of these methods is the generic idea of multi-dimensional p-adic Newton iteration (finding local solutions and lifting them), though there are interesting alternative constructions in some of the smaller cases. Even when we do resort to the generic NEWTON method we often must first transform our systems in ways specific to this problem in order to make the computations feasible. In several cases we use connections with modular curves or elliptic surfaces to account for DIOPHANTINE properties of the resulting polynomials or BELYĬ functions.

2. BELYĬ functions

A BELYĬ function [2] is a holomorphic function f from a RIEMANN surface to the projective complex line that is ramified above only three points, commonly taken to be $0, 1, \infty$.[2] In our case, f is a rational function from $\mathbf{P}^1(\mathbf{C})$ to itself. By the RIEMANN–HURWITZ formula [30, §7] [19, V, §2] [20, II, §5], the ramification multiplicity is $2 \cdot \deg(f) - 2$. In the HALL case, $f(t) = X(t)^3/Y(t)^2$ is a BELYĬ function of degree $6m$, having $2m$ triple points (roots of X), $3m$ double points (roots of Y), and, since we have $f(t) - 1 = K(t)/Y(t)^2$, we also have a preimage of 1 with multiplicity $6m - (m+1) = 5m - 1$ at infinity.[3] Similarly, in the FERMAT–PELL case, $f(t) = X(t)^3/Q(t)Y(t)^2$ is a BELYĬ function of degree $6m$, having $2m$ triple points, $3m - 1$ double points, and a preimage of 1 with multiplicity $5m$ at infinity.

In both cases we find that the ramification multiplicity $12m - 2$ of f is completely accounted by the three cases $f(t) = 0, 1, \infty$, the sum being

$$(3-1)(2m) + (2-1)(3m) + (5m-1-1)(1) = 12m - 2$$

in the HALL case, while in the FERMAT–PELL case it is

$$(3-1)(2m) + (2-1)(3m-1) + (5m-1)(1) = 12m - 2.$$

Conversely a function for which the preimages of $0, 1, \infty$ have these multiplicities arises from an identity (1) or (2) with the desired degrees, determined uniquely up to the obvious scalings $(X, Y, K) \mapsto (\lambda^2 X, \lambda^3 Y, \lambda^6 K)$, $(X, Q, Y, K) \mapsto (\lambda^2 X, \mu^{-2} Q, \lambda^3 \mu Y, \lambda^6 K)$.

For any $a \in \mathbf{C}^*$ and $b \in \mathbf{C}$, the function $f(at+b)$ satisfies our ramification conditions if and only if f does; we say that $f(t)$ and $f(at+b)$ are equivalent.

The following standard argument ([27]? FIX THIS) uses the existence theorem for RIEMANN surfaces to reduce the enumeration of solutions modulo equivalence to a group theory problem. Let Σ be the complement of $\{0, 1, \infty\}$ in $\mathbf{P}^1(\mathbf{C})$, and fix a base point $z_0 \in \Sigma$. Then $\pi_1(\Sigma)$ is a free group on two generators s_0, s_∞, represented by closed paths through z_0 that wind once around 0 and ∞ respectively, with $(s_0 s_\infty)^{-1}$ winding once around 1. Arbitrarily label the preimages of z_0 under f by distinct integers

---

[2] Since the automorphism group $\mathrm{PSL}(2, \mathbf{C})$ of $\mathbf{P}^1(\mathbf{C})$ acts triply transitively, all choices of three branch points are equivalent.

[3] That is, $f(t) - 1$ has a root of multiplicity $5m - 1$ at $t = \infty$.

in $[6m] := \{1, 2, 3, \ldots, 6m\}$. Then lifting closed paths through z_0 from Σ to the t-line gives a group homomorphism from $\pi_1(\Sigma)$ to the symmetric group S_{6m}. Moreover, s_0 and s_∞ lift to permutations g, h whose cycle structures are given by the multiplicities of $f^{-1}(\{0\})$ and $f^{-1}(\{\infty\})$ respectively, and whose product's cycle structure is given by the multiplicities of $f^{-1}(\{1\})$. Equivalent functions $f(t)$ yield the same g and h, while changing the labeling of $f^{-1}(\{z_0\})$ by a permutation of $[6m]$ effects a conjugation of g, h, gh by the same permutation. Thus an equivalence class of solutions f yields g, h in S_{6m} up to conjugation by the same element of S_{6m}, with the cycle structures of g, h, gh matching the multiplicities of $f^{-1}(\{0\})$, $f^{-1}(\{\infty\})$, $f^{-1}(\{1\})$ respectively. Conversely, starting with such g, h we obtain by the Riemann existence theorem a branched cover of $\mathbf{P}^1(\mathbf{C})$ that has the structure of a Riemann surface of genus 0; by the uniformization theorem we find a rational coordinate t on this surface that identifies it with $\mathbf{P}^1(\mathbf{C})$ and has its pole at the multiple preimage of 1. This recovers f up to equivalence.

2.1. A group theory problem. We have thus reduced the counting of solutions to Hall's equation to a group theory problem; how many S_{6m} conjugacy classes of (g, h) pairs are there for which the cycle structures of (g, h, gh) are equal to $\bigl((3)^{2m}, (2)^{3m}, (5m-1)^1\bigr)$ respectively? Similarly, in the Fermat–Pell case we want the cycle structures of (g, h, gh) to be $\bigl((3)^{2m}, (2)^{3m-1}, (5m)^1\bigr)$. Note that we can assume that g is fixed, while we can also specify the fixed points of gh and similarly their images under h.

We originally wrote a computer programme to enumerate such conjugacy classes, but then realised that [35, Theorem 4.6] already gave the answer for the Hall case (see also [41] and [22, Chapter ?]). However we have not attempted to adapt the method to the Fermat–Pell case, and so simply give our experimental data in Table 2. For small m we can get provable results, while for larger m we can assert a result with high confidence using randomised techniques.[4]

We wrote a Magma [5] programme for the $m = 3$ Fermat–Pell case which, after fixing m points of the product gh and their images under h, tried each of the $\frac{1}{(2m-1)!}\prod_{i=2}^{2m}\binom{2i}{2} = 62370$ products of $2m-1$ transpositions in S_{4m}. The `IsConjugate` command of Magma allowed us to determine conjugacy classes and so find the expected 10 solutions, but this took about 40 seconds, in large part due to the 600000 tests for simultaneous conjugacy. We then realised that simultaneous conjugacy can be tested more easily (see below) in our special case, and wrote a `C` programme[5] to do the

[4] That is, we conjugate h by random group elements and then give further consideration to those for which gh has the proper cycle structure. This works well because we have a reasonable probability of obtaining (in the Hall case) a $5m$-cycle as an arbitrary element of S_{5m}.

[5] This is to be available from some web address.

same calculation. This reduced the running time by a factor of about 500, though testing for simultaneous conjugacy is still quite time-consuming.[6] We then exported the obtained (g,h) pairs into MAGMA, using its implementation of the SCHREIER-SIMS algorithm [24] to obtain the subgroup G of S_{6m} generated by g and h. Associated to such a group G is a degree of imprimitivity, which is 1 when G is primitive as a permutation group, and in general is the number of blocks which G permutes.

TABLE 1. Data for HALL case

m	$\#C$	d	G
1	1	2	$2^2 \cdot S_3 \cong S_4$
2	1	3	$3^3 \cdot A_4$
3	1	2	$2^9 \cdot \mathrm{PSL}_2(\mathbf{F}_8)$
4	1	1	A_{24}
5	1	1	S_{30}
5	2	2	$2^{14} \cdot S_{15}$
5	1	3	$3^{10} \cdot \mathrm{PGL}_2(\mathbf{F}_9)$
6	6	1	A_{36}
7	14	1	S_{42}
7	5	2	$2^{21} \cdot A_{21}$
8	47	1	A_{48}
8	2	3	$3^{16} \cdot A_{16}$
9	136	1	S_{54}
9	14	2	$2^{26} \cdot S_{27}$
10	442	1	A_{60}
11	1377	1	S_{66}
11	42	2	$2^{33} \cdot A_{33}$
11	5	3	$3^{22} \cdot S_{22}$
12	4522	1	A_{72}
13	14792	1	S_{78}
13	132	2	$2^{38} \cdot S_{39}$
14	49522	1	A_{84}
14	14	3	$3^{28} \cdot A_{28}$
15	429	2	$2^{45} \cdot A_{45}$
17	1430	2	$2^{50} \cdot S_{51}$
17	42	3	$3^{34} \cdot S_{34}$

TABLE 2. Data for FERMAT–PELL case

m	$\#C$	k	G
1	1	1	$\mathrm{PSL}_2(\mathbf{F}_5) \cong A_5$
2	2	1	$\mathrm{PGL}_2(\mathbf{F}_{11})$
2	2	2	$2^6 \cdot \mathrm{PSL}_2(\mathbf{F}_5)$
3	9	1	A_{18}
3	1	3	$3^6 \cdot \mathrm{PSL}_2(\mathbf{F}_5)$
4	32	1	S_{24}
4	4	2	$2^{11} \cdot \mathrm{PGL}_2(\mathbf{F}_{11})$
4	2	4	$4^6 \cdot \mathrm{PSL}_2(\mathbf{F}_5)$
5	125	1	A_{30}
5	1	5	$5^3 \cdot \mathrm{PSL}_2(\mathbf{F}_5)$
6	450	1	S_{36}
6	18	2	$2^{18} \cdot A_{18}$
6	2	3	$3^{12} \cdot \big(2^{11} \cdot \mathrm{PGL}_2(\mathbf{F}_{11})\big)$
6	2	6	$6^6 \cdot \mathrm{PSL}_2(\mathbf{F}_5)$
7	1715	1	A_{42}
7	1	7	$7^6 \cdot \mathrm{PSL}_2(\mathbf{F}_5)$
8	6400	1	S_{48}
8	64	2	$2^{23} \cdot S_{24}$
8	4	4	$2^{23} \cdot \big(2^{11} \cdot \mathrm{PGL}_2(\mathbf{F}_{11})\big)$
8	2	8	$8^6 \cdot \mathrm{PSL}_2(\mathbf{F}_5)$
9	24300	1	A_{54}
9	9	3	$3^{18} \cdot \big(2^{17} \cdot A_{18}\big)$
9	1	9	$9^6 \cdot \mathrm{PSL}_2(\mathbf{F}_5)$
10	92250	1	S_{60}
10	250	2	$2^{30} \cdot A_{30}$
10	2	5	$5^{12} \cdot \big(2^{11} \cdot \mathrm{PGL}_2(\mathbf{F}_{11})\big)$
10	2	10	$2^6 5^3 \cdot \mathrm{PSL}_2(\mathbf{F}_5)$

[6] For example, with the FERMAT–PELL $m = 8$ case, we checked 129400 random h with the proper cycle structures, amounting to over 400 million conjugacy tests, which took 10 minutes.

Our results are listed in Tables 1 and 2. In the tables, d or k is the degree of imprimitivity, G is the group, and $\#C$ is the number of conjugacy classes (and thus also the number of solutions to (1) or (2)). The notation $a^b \cdot H$ denotes an extension of $(\mathbf{Z}/a\mathbf{Z})^b$ by H, so that $(\mathbf{Z}/a\mathbf{Z})^b$ is a normal subgroup with quotient H. For various $m \geq 15$ in the HALL case, we counted only imprimitive solutions, which expedites the calculation by reducing the number of conjugacy tests.[7] We expect that usually[8] each line of the table corresponds to a single GALOIS orbit of solutions, so that, for instance, there should be an essentially unique solution in a sextic field to $X(t)^3 - Y(t)^2 = K(t)$ with (X, Y, K) of degrees $(12, 18, 7)$.

We note that the imprimitive subgroups in the HALL case correspond to solutions (of smaller degree) of equations similar to HALL's equation. Suppose that we have $t\tilde{X}(t)^3 - \tilde{Y}(t)^2 = \tilde{K}(t)$ with $(\tilde{X}, \tilde{Y}, \tilde{K})$ of respective degrees $(2l-1, 3l-1, l)$. Then $\bigl(t\tilde{X}(t^3), \tilde{Y}(t^3), \tilde{K}(t^3)\bigr)$ is a solution to HALL's equation with degrees $(6l-2, 9l-3, 3l)$. These correspond to $m = 3l - 1$ and $d = 3$. Likewise, suppose that we have $\tilde{X}(t)^3 - t\tilde{Y}(t)^2 = \tilde{K}(t)$ with $(\tilde{X}, \tilde{Y}, \tilde{K})$ having degrees $(2l-1, 3l-2, l)$. Then $\bigl(\tilde{X}(t^2), t\tilde{Y}(t^2), \tilde{K}(t^2)\bigr)$ is a solution to HALL's equation with degrees $(4l-2, 6l-3, 2l)$. These correspond to $m = 2l - 1$ and $d = 2$. In these imprimitive cases we have $f(t) = \tilde{f}(t^d)$ where $\tilde{f}(t) = t\tilde{X}^3/\tilde{Y}^2$ (for $d = 3$) or $\tilde{f}(t) = \tilde{X}^3/t\tilde{Y}^2$ (for $d = 2$) is also a BELYĬ function.

For the FERMAT–PELL case, the imprimitive subgroups are not as interesting. Given a solution (X_k, Y_k, Q_k) with $k|m$ they correspond to taking t to be a nonlinear degree k polynomial in s with $Q_k\bigl(t(s)\bigr)/Q_k(s)$ square. When k is even, this is generically defined over a quadratic extension, in which case the degree of the field of a solution might be doubled. Indeed, we are essentially solving $u^2 = Q(t)$ in $\mathbf{Q}(t, u)$ and taking the kth power of the unit solution.

For the primitive FERMAT–PELL counts, the SLOANE database [33] gives us the sequence A045630, the number of $2m$-bead black-white complementable strings with m black beads and fundamental period $2m$. The total FERMAT–PELL counts are A032123, which are identified as the number of $2m$-bead black-white reversible strings with m black beads. Alternatively, if we only half-count the solutions with even primitivity, then we obtain the binomial coefficient $\binom{2m-1}{m}$.

The imprimitive HALL counts appear to be related to the CATALAN numbers, while the total HALL counts are given by A001683, idenitifed therein

[7] We do not know whether the (g, h) that give imprimitive G can be determined directly.
[8] This will be seen to be wrong for the HALL $(m, d) = (11, 3)$ case.

as the number of one-sided triangulations of the disk, and via oligomorphic[9] techniques in [7, Table 3] as the U-sequence for plane boron (trivalent) trees.

2.1.1. *More details of simultaneous conjugacy testing.* Given a symmetric group, we are interested in the number of conjugacy classes of pairs (g,h) that have a given cycle structure for each of (g,h,gh). We can always conjugate g to some fixed element of its structure. In both of our main applications we have S_{6m} with g a product of $2m$ disjoint 3-cycles. We now restrict our description to the HALL case, where h is a product of $3m$ disjoint transpositions. We take

$$g=\prod_{i=1}^{m+1}(i,i+m+1,i+2m+2)\prod_{j=m+2}^{2m}(3j-2,3j-1,3j),\ \ h=\sigma\prod_{i=1}^{m+1}(i,i+m+1)$$

where σ is a random product of $(2m-1)$ disjoint transpositions on the integers in $[2m+3,6m]$. This ensures that hg fixes the first $(m+1)$ integers. We then randomly generate such h and check whether gh is a $(5m-1)$ cycle. If it is, we then check whether (g,h) is conjugate to a previously generated $(g,\tilde{h})$. We note that (g,h) and $(g,\tilde{h})$ are conjugate precisely when (g,hg) and $(g,\tilde{h}g)$ are. For each $\tilde{h}$, we write $\alpha=hg$ and $\beta=\tilde{h}g$ and want to determine if there is some τ with $g^\tau=g$ and $\alpha^\tau=\beta$. For this, we let b run over the integers in $[m+2,6m]$; for each b we have some i such that $\beta^i(b)=g(b)$, and we check whether $\alpha^i(b)=g(b)$. If this checks out for all b, then such a τ exists.[10] This suffices to check simultaneous conjugacy.

We continue to generate random conjugates of h until the number of h with the desired cycle structure for gh exceeds the number of obtained (g,h) classes by a sufficiently large factor — we took this to be 20 in most[11] of the calculations. Since each (g,h) class is expected (up to primitivity considerations) to be equally likely to appear, this implies that the chance of missing a class is quite small; thus we are fairly confident that the numbers listed in the Tables are correct.

We could go further and try to prove these numbers are correct, using the following character-theoretic formula for the number of solutions in a finite

---

[9] See [7] for more details. A permutation group on an infinite set is oligomorphic if the number of orbits on ordered n-tuples is finite for all positive integers n.

[10] We can be more explicit. With loss of generality we can assume that τ fixes $m+2$. We can compute τ from $\tau:\beta^i(m+2)\to\alpha^i(m+2)$ by stepping through i, with the values of τ on the integers b in $[1,m+1]$ being then computable from $\tau(b)=g^{-1}\tau g(b)$.

[11] The stopping criterion in the HALL cases where we only looked for imprimitive (g,h) used a smaller factor, as generating random h was time-dominant.[12]

[12] We used the following method as a fast filter to detect whether $G=\langle g,h\rangle$ might be d-imprimitive for $d=2,3$. We note that gh and hg are both cycles of length L, and so both $(gh)^{L/d}$ and $(hg)^{L/d}$ are products of d-cycles. If G is d-imprimitive, then the elements in these d-cycles must correspond to the permuted blocks. In particular, the product $(gh)^{L/d}(hg)^{L/d}$ must also decompose into d-cycles, and we used this as our filter.

group G of the equation $g_1g_2g_3 = 1$ with g_1, g_2, g_3 in prescribed conjugacy classes C_1, C_2, C_3, in terms of the values of the irreducible characters χ of G at C_1, C_2, C_3:

$$\frac{\#C_1\#C_2\#C_3}{\#G}\sum_{\chi}\frac{\chi(C_1)\chi(C_2)\chi(C_3)}{\chi(1)},$$

where the $\chi = 1$ term yields the naive guess $\#C_1\#C_2\#C_3/\#G$, and the others, with denominators $\chi(1) = \dim(\chi)$, can be regarded as correction terms which often are small and mostly zero (this is the $k = 3$ case of [31, Theorem 7.2.1]). However, the number of conjugacy classes (and thus irreducible characters) grows so rapidly that we are unable[13] to compute this beyond the first few cases.

3. Exhibiting solutions

There are various methods we can use to exhibit solutions to these equations. The small cases are nearly trivial, and some larger examples (especially when $\#C = 1$ so the solution is rational) are known. We quote from [14, §4.1] the following Hall examples defined over $\mathbf{Q}$. For $m = 1$ and $m = 2$, the scalar $a \neq 0$ is arbitrary; changing a yields a quadratic or cubic twist, which is available because these examples have $d = 2$ and $d = 3$ respectively. The same twists can be applied to Birch's examples with $m = 3$ and $m = 5$. Once $m > 2$, we exhibit only X, which determines Y and thus K because Y is the polynomial part of the Laurent expansion of $X^{3/2}$ about $t\infty$.

$m = 1$: $X(t) = t^2 + 2a$, $\quad Y(t) = t^3 + 3at$, $\quad K(t) = 3a^2t^2 + 8a^3$
$m = 2$: $X(t) = t^4 + 4at$, $\quad Y(t) = t^6 + 6at^3 + 6a^2$, $\quad K(t) = -8a^3t^3 - 36a^4$

$$m = 3\colon\ X(t) = 36t^6 + 24t^4 + 10t^2 + 1 \quad (\text{Birch})$$

$m=4$: $X(t) = 4(t^8+6t^7+21t^6+50t^5+86t^4+114t^3+109t^2+74t+28)$ (Hall)

$m = 5, d = 1$: $X(t) = t^{10} + 2t^9 + 33t^8 + 12t^7 + 378t^6 - 336t^5 + {}$
$+2862t^4 - 2652t^3 + 14397t^2 - 9922t + 18553$ (Elkies)

$m = 5, d = 3$: $X(t) = (t/9)(t^9 + 6t^6 + 15t^3 + 12)$ (Birch)

There is also one primitive Fermat–Pell example known to be defined over $\mathbf{Q}$, namely Danilov's [9] with $m = 1$:

$$X(t) = t^2+10t+5,\ Y(t) = t^2+4t-1,\ Q(t) = t^2+22t+125,\ L(t) = 1728t.$$

This example yields the only known infinite family of integer solutions of $0 < |x^3 - y^2| < \sqrt{x}$ (indeed, it generates all known infinite families with

[13] The natural programme to use here appears to be Symmetrica [21], much of whose functionality is included in Magma.

$0 < |x^3 - y^2| \ll \sqrt{x}$), showing that the exponent in Hall's conjecture cannot be increased above 1/2.

3.1. Geometric methods and connections. Furthermore, the $(m, d) = (5, 2)$ quadratic HALL solution (that is, with coefficients in a quadratic extension of $\mathbf{Q}$) was found[14] by ELKIES using the same method (described below) as with the $(m, d) = (5, 1)$ rational HALL solution. The primitive $m = 2$ quadratic FERMAT–PELL solution was found by ELKIES using SHIMURA curves as described below.

3.1.1. *Moduli spaces.* .

- Do Hall $m = 5$ $d = 1$ and $d = 2$. [12].
- Do Hall $m = 8$ $d = 3$ here.

++++++++++++++++++++++++++++++++++

The reappearance of the EISENSTEIN field is suggestive. Indeed this too should be within the range of my MORDELL-WEIL approach: let $t = T^3$, so we have $tX^3 - Y^2 = k$ with X, Y, k of degrees 5,8,3. Then $(tX)^3 - (tY)^2 = t^2k$, a polynomial of degree 5, this time with a repeated root so the MORDELL-WEIL group is complex E_6 instead of complex E_8. Presumably points of this height fall into two conjugate orbits under the complex automorphisms.

++++++++++++++++++++++++++++++++++

- And Hall $m = 11$ $d = 3$ here? Maybe the quadratic solution.

++++++++++++++++++++++++++++++++++

Even the imprimitive solution(s) for $\deg(k) = 12$ that come from $tX^3 - Y^2 = k$ with X, Y, k of degrees $7, 11, 4$ should be accessible in this way. I don't know if you can just blast this one too with Gröbner bases or p-adic Newton. It might require combining Gröbner/Newton with the Mordell-Weil technique to make this computation feasible.

++++++++++++++++++++++++++++++++++

3.1.2. *Elliptic and SHIMURA modular curves.* Several of the BELYĬ functions f or $\tilde{f}$ associated to HALL or FERMAT–PELL solutions with small m can be interpreted as natural maps between modular curves. For the DANILOV polynomials, it was already noted in [13, p.49] that the BELYĬ function coincides with the cover $X_0(5) \to X(1)$; this was used there to explain the coefficient 1728 (since $f(t)$ is the j-function lifted to $X_0(5)$). The other examples may also be recognized from their groups G in Tables 1 and 2, which involve $\mathrm{PSL}_2(\mathbf{F}_q)$ or $\mathrm{PGL}_2(\mathbf{F}_q)$ for some prime power q. We next list the modular curves arising in each case.

For the HALL polynomials, we find that there are three cases, all imprimitive: $(m, d) = (1, 2)$, $(2, 3)$, and $(5, 3)$. For $m = 1$, the degree-3 function $\tilde{f}$

---

[14] The work of UCHIYAMA and YORINAGA [37] already had handled $(m, d) = (7, 2)$, but, for a reason we cannot detect, they seem only able to find solutions that possess a real embedding.

gives the cover $X_0(2) \to X(1)$ of elliptic modular curves; in this case f is itself a modular cover, namely $X_0(4) \to X(1)$, even though G is imprimitve. For $m = 2$, the degree-4 function $\tilde{f}$ can likewise be identified with the modular cover $X_0(3) \to X(1)$. For $m = 5$ we have a function $\tilde{f}$ of degree 10 with $G \cong \mathrm{PGL}_2(\mathbf{F}_9)$. This is a covering of SHIMURA modular curves associated to the quaternion algebra over $\mathbf{Q}(\sqrt{2})$ ramified only at the prime $(\sqrt{2})$ and one of the two infinite places. The arithmetic subgroups of $\mathrm{PSL}_2(\mathbf{R})$ arising from this quaternion algebra include nine triangle groups, comprising class III in TAKEUCHI's list [39]. One of these is the maximal group with indices $(2, 3, 8)$; another is its index-10 subgroup with indices $(3, 8, 8)$, consisting of upper-triangular matrices mod (3) (under some identification of the quaternion algebra mod (3) with a matrix algebra). Our function $\tilde{f}$ is the natural map between those two modular curves. This explains why $\tilde{f}$ has good reduction modulo the prime factor 5 of $\#G$.

For FERMAT–PELL polynomials there are two primitive modular covers. One is DANILOV's example for $m = 1$, giving $X_0(5) \to X(1)$ as noted already; its imprimitive descendant with $(m, k) = (5, 5)$ also yields a modular cover, namely $X_0(25) \to X(1)$.[15] The other is $m = 2$. This is our first example of a HALL or FERMAT–PELL solution that cannot be defined over $\mathbf{Q}$. The count of two solutions in S_{12} in Table 2 leads us to expect a solution defined over a quadratic number field, but cannot identify the field. By identifying f with a cover of SHIMURA modular curves we can predict that the field must be $\mathbf{Q}(\sqrt{5})$, and moreover each of the two covers has good reduction except above $(\sqrt{5})$ and one of the primes $(4 \pm \sqrt{5})$ lying over the rational prime (11). The bottom curve in the cover corresponds to the $(2, 3, 10)$ triangle group, which is in TAKEUCHI's class VIII: the quaternion algebra over $\mathbf{Q}(\sqrt{5})$ ramified only at the prime $(\sqrt{5})$ and one of the two infinite places. The top curve does not come from a triangle group (there are four elliptic points); it corresponds to an index-12 subgroup consisting of upper-triangular matrices modulo either of the two primes over (11).

3.2. Multi-dimensional p-adic NEWTON iteration. All of the above methods can [CHECK THIS, after the methods have been described] be seen as equating coefficients and then solving a system of polynomial equations. For many of them, after making linear substitutions we have a system of no more than 4 equations and unknowns, with small degrees for the polynomials, and these can easily be solved via GRÖBNER bases [6] or resultants [3, 36]. For instance, the FERMAT–PELL $m = 2$ case takes less than a second using MAGMA, as does the imprimitive HALL $(m, d) = (8, 3)$

---

15 We noted in [14, p.56] that all the elliptic curves with small discriminant obtained from the DANILOV identity have a rational 5-isogeny due to the connection with $X_0(5)$. The connection with $X_0(25)$ likewise explains why some of these curves, including notably the first one $X_1(11)$, even have a rational 25-isogeny.

case. However, resultants and GRÖBNER bases quickly become unwieldy as the number of variables grows, and so we must look for another method.[16]

A more generic method to try to find solutions of a polynomial system of equations is multi-dimensional p-adic NEWTON iteration, which appears in [15, §2.2] and [40].[17] It works by finding local solutions modulo a small prime p and then trying to lift them (this requires the JACOBIAN to be invertible) to p-adic high precision before using the LLL algorithm [23] to attempt to recognise these p-adic approximations as algebraic numbers. Usually the very small primes have bad reduction and are thus not so useful — also, when searching for algebraic solutions we need that p has a degree 1 factor in the (unknown) field of definition. We stress that is only a heuristic search method, and it appears difficult to prove in general that it finds all the solutions for a given polynomial system. The main bottleneck in the searching for solutions is finding all the local solutions, which usually is done simply by looping over all possibilities mod p for each of the v variables, thus taking p^v time. In practise, it is often better to first eliminate one or more variables with (say) resultants — although this will likely make the defining polynomials significantly more complicated, the gain from lessening the number of variables will likely be more important.

For the HALL cases, after linear substitutions and two resultant steps (this is usually the limit of their efficacy, though below we describe how to pre-condition the system to go further) we are left with a system of $2m-4$, $m-3$, and $(2m-10)/3$ equations, respectively for $d = 1, 2, 3$. In the (primitive) FERMAT–PELL case, we can similarly reduce to $2m-2$ equations/unknowns. In our applications here, the general rule is that a reduced system of 8 equations can examined for local solutions for $p = 5, 7$ and maybe $p = 11$, so we consider the 8-variable systems for the $(m, d) = (6, 1), (11, 2), (17, 3)$ HALL cases[18] and the $m = 5$ FERMAT–PELL case to be on the edge of computational feasibility; indeed, even the 6-variable systems can be cantankerous.

3.3. The primitive HALL case. With the primitive HALL $m = 6$ case, linear substitutions and two resultant steps gave a reduced system of 8 variables and unknowns, and we were lucky to find the expected solution over the sextic number field defined by

$$z^6 - z^5 - 60z^4 - 267z^3 - 514z^2 - 480z - 180,$$

[16] Even for the primitive HALL $m = 4$ case, after linear substitutions we were left with a 6-variable system that did not submit to GRÖBNER basis techniques.

[17] The reader might ask why we do not consider complex approximations, as (say) COUVEIGNES did [8, Chapter 3]. The multi-dimensional NEWTON approach is well-known to need a good first approximation in order to converge, and we were not sufficiently well-versed in (say) the homotopy continuation methods [38, 17, 34] to determine whether they would be of use here.

[18] We found a solution for the primitive HALL $m = 6$ case in this manner, but this was lucky.

which has discriminant $2^2 \cdot 5 \cdot 13 \cdot 29^5$. For reasons of space we do not reproduce the solution, but instead list $X(t)$ mod 17 as[19]

$$t^{12} + 14t^{10} + 14t^9 + 9t^8 + 6t^7 + 4t^6 + 7t^5 + 6t^4 + 15t^3 + 7t^2 + 3t + 10.$$

To recover $X(t)$ from this, we lift this solution of the 10-variable system in which: $X(t)$ is monic; its t^{11} coefficient is zero; and its t^9 and t^{10} coefficients are equal to each other; and then recognise the coefficients as algebraic numbers.

3.3.1. *Preconditioning.* We can handle the $m = 7$ case by pre-conditioning our system. Indeed, HALL [18] already indicates that when $X^3 - Y^2$ has degree $(m + 1)$ with $\deg(X, Y) = (2m, 3m)$, we can write $X = A^2 + B$ and $Y = A^3 + 3AB/2 + C$ with $\deg(A, B, C) = (m, m-1, m-2)$ and compute[20]

$$(A^2 + B)^3 - (A^3 + 3AB/2 + C)^2 = \frac{A^2}{4}(3B^2 - 8AC) + B^3 - C^2 - 3ABC.$$

We thus get that $3B^2 - 8AC$ must have degree at most $(m - 3)$, much smaller than the optical guess of $(2m - 2)$. We can thus adapt the reduction theory [16, Sectio 5, §§157ff] of GAUSS to (A, B, C), and get polynomials of smaller degree. For instance, in the $m = 7$ case we start with $\deg(A, B, C) = (7, 6, 5)$ and then take $D \equiv C \pmod B$ with E such that that $3B^2 - 8AC = 3D^2 - 8CE$. This gives $\deg(C, D, E) = (5, 4, 3)$, and since $\deg(3B^2 - 8AC) \le m - 3 = 4$, we can repeat this with $F \equiv E \pmod D$ to get $\deg(E, F, G) = (3, 2, 1)$ with $3F^2 - 8EG = 3B^2 - 8AC$. To invert the process, we simply have linear polynomials L and M with $B = LC + D$ and $D = ME + F$ with $8C = 3M^2E + 6MF + 8G$ and $8A = 3L^2C + 6LD + 8E$. Thus we start with the five arbitrary polynomials (E, F, G, L, M) of degrees $(3, 2, 1, 1, 1)$, and want $X^3 - Y^2$ to have degree 8. We can scale X, Y and apply an affine linear transformation $t \leftarrow at + b$ to eliminate 3 of our unknowns, and we used

$$E(t) = e_3t^3 + e_1t + e_0, \quad F(t) = f_1t^2 + f_1t + f_0,$$
$$G(t) = g_1t + g_0,\ \ M(t) = t + m_0,\ \text{ and }\ L(t) = l_1t + l_0$$

to obtain a system of 10 equations and 10 unknowns from setting the t^{18} through t^9 coefficients of $X^3 - Y^2$ equal to zero.[21]

The gain of this method is that many of the variables now appear linearly; indeed, we eliminated four variables (g_1, g_0, f_0, e_0) almost instantly, and then took a minute to eliminate e_1 which appeared quadratically. Having

[19] We originally worked mod 5, but the above is a more convenient description.

[20] We can note that UCHIYAMA and YORNIAGA [37] largely used the alternative formulation that $3X'Y - 2XY'$ is constant, though we have not considered the usefulness of this in our guise.

[21] It can be noted that computing "$X^3 - Y^2$" symbolically in this form need not be non-trivial, but takes only about a minute in this case.

reduced ourselves to 5 variables, we then searched for points modulo small primes, and with $p = 13$ found a liftable solution. We give our solution as

$$(m_0, g_1, g_0, f_1, f_0, e_3, e_1, e_0, l_1, l_0) \equiv (4, 8, 9, 12, 5, 8, 2, 10, 12, 4) \pmod{13},$$

and if we want to rewrite $X(t)$ in a nice form we can rescale and put

$$X(t) \equiv t^{14}+4t^{12}+4t^{11}+t^{10}+4t^9+10t^8+11t^7+11t^6+6t^5+6t^4+6t^3+t+11$$

which lifts as above (with $x_{14} = 1, x_{13} = 0, x_{12} = x_{11}$). Via lifting, we find a solution in the field of discriminant $-2^{12}3^3 5^2 7^7 13^2 17^{11} 31^3$ given by

$$\begin{aligned} &z^{14} - 7z^{13} + 70z^{12} - 99z^{11} - 841z^{10} + 11754z^9 - 138695z^8 + \\ &\quad + 634545z^7 - 1552229z^6 + 2048494z^5 + 133909z^4 + \\ &\quad\quad + 1879821z^3 - 17409230z^2 + 63955265z - 50955645. \end{aligned}$$

3.3.2. *Another pre-conditioning method.* For the $m = 8$ case, we analogously have $\deg(E, F, G) = (4, 3, 2)$ and then by applying reduction again we get $\deg(G, H, I) = (2, 1, 3)$ with $\deg(3H^2 - 8GI) = \deg(3B^2 - 8AC) = 5$. However, we found the above method too unwieldy,[22] and thus followed an idea in [14, p.58]. This allows us to parametrise the $m = 8$ case with 6 variables rather directly, at a small cost when considering the lifting (which is not time-dominant). We write $X = A^2 + B$ as above, and expand B/A in a Laurent expansion at infinity, and truncate it to m terms, calling the result R. (This R corresponds to the parameter called b in [14, p.58].) That is, we write

$$A(t) = \sum_{i=0}^{m} a_i t^i, \qquad R(t) = \sum_{j=1}^{m} r_j / t^j$$

and have $B + B_0 = AR$ with $B_0 = \sum_{j=1}^{8} b_j^0 / t^j$ and $C + C_0 = \frac{3}{8}(AR^2 - 2RB_0)$ with $C_0 = \sum_{j=1}^{16} c_j^0 / t^j$. Of course, we can also apply a preliminary scaling of X, Y and an affine linear transformation to t so that we can assume $a_7 = 0$, $r_1 = r_2$, and $r_8 = 1$. It is important here that the c_j^0 depend only linearly on the a's. Substituting for B and C in $X^3 - Y^2$ gives us

$$X^3 - Y^2 = \frac{A^3}{8}(16C_0 - R^3) + \frac{A^2}{64}(48B_0^2 + 192C_0 R + 24B_0 R^2 - 9R^4) + \cdots +,$$

so that we must have $16C_0 = R^3 + O(1/t^9)$, and this gives us 8 linear equations[23] for the a's in terms of the r's. It takes only 2 seconds to solve

[22] We were eventually able to reduce to 6 equations and unknowns, but only after spending about 3 days computing resultants with MAGMA. Furthermore, the obtained polynomials were sufficiently large that looping over $\mathbf{F}_{13}^6$ would take more than a week.

[23] It seems to me that we actually have $16C_0 = R^3 + O(1/t^{10})$, but that this doesn't give us any advantage.

this system symbolically.[24] We also symbolically consider

$$(A^2+B)^3-(A^3+3AB/2+C)^2=-2A^3C+3A^2B^2/4-3ABC+B^3-C^2$$

in terms of the a's and r's, and setting the t^{10} through t^{15} coefficients to zero gives us 6 equations for our six r-variables. We can try to find local solutions modulo p by looping over $\mathbf{F}_p^6$, and for each such r-vector, substituting it into the expressions for the a's, and then plugging both of these into our 6 equations. After a few days of searching, we found the mod 29 solution $(r_1,r_3,r_4,r_5,r_6,r_7)=(16,26,7,25,26,14)$, and we can convert this to

$$\begin{aligned}X(t)\equiv t^{16}+8t^{14}+8t^{13}+13t^{12}+21t^{10}+15t^9+5t^8+&\\ +23t^7+7t^6+28t^5+19t^4+16t^3+11t^2+21 &\pmod{29},\end{aligned}$$

which lifts with $x_{16}=1, x_{15}=0, x_{14}=x_{13}$. The lifting takes about 15 minutes to reach precision $29^{2^{14}}$, which was sufficient for LLL (applied to the rows of a 95-by-48 matrix) to identify (in about 30 minutes) at least one of the r's in a field of degree 47. We then used the `polredabs` command of GP/PARI [29], and in about 2 days obtained a model[25] for the field of

$$\begin{aligned}
&z^{47}+16z^{46}+86z^{45}-2412z^{44}-60409z^{43}-564293z^{42}-2387907z^{41}-9191224z^{40}-\\
&-678031657z^{39}-11353387175z^{38}-124870372198z^{37}-549211743912z^{36}-\\
&-5626462158525z^{35}-68025534438824z^{34}-1061556807021441z^{33}-9140044629505239z^{32}-\\
&-67000413335358093z^{31}-520272554511857994z^{30}-4176931330587803370z^{29}-\\
&-31227058218225197196z^{28}-209545999636517259765z^{27}-1293690372387790236609z^{26}-\\
&-7271756437125244437165z^{25}-36771591164540932942593z^{24}-\\
&-160042039052004633511923z^{23}-644322399530601414340341z^{22}-\\
&-2445395776847558603238276z^{21}-7417872425101301095910789z^{20}-\\
&-17196621498117063471125114z^{19}-32386397157887635560792769z^{18}-\\
&-40844825535173264778821847z^{17}+36650827246150576476281372z^{16}+\\
&+563773475588956867734758236z^{15}+1302641634619063062628734930z^{14}-\\
&-4267836510430588442116510096z^{13}-22544110365416143302883735573z^{12}-\\
&-19990300886177927076447942227z^{11}+28372587574955737751127155471z^{10}-\\
&-44318658029888659591887229 14z^{9}-85132687530267248495927307954z^{8}+\\
&+142170141250640512324664135524z^{7}+96860531569968846584757420456z^{6}-\\
&-720773204261926864088348092752z^{5}-302159088765700160021658596760z^{4}+\\
&+1064817393248685420448278043248z^{3}-1437891724256368310262273640 68z^{2}-\\
&-1604385707079219904755213878 16z-1806599424346853419651374650 4
\end{aligned}$$

---

[24] Our first try with MAGMA used an 8-variable polynomial ring on top of a 6-variable function field, and took 3 minutes — a simple 14-variable polynomial ring and field of fractions proved much faster in the end.

[25] The model given does not the minimise the T_2 norm for the roots, but has significantly smaller coefficients than that which does.

of discriminant $-2^{40}3^{38}5^{6}7^{16}13^{45}19^{3}31^{8}37^{5}41^{7}$. The fact that only small primes divide the discriminant is no accident, as a theorem of BECKMANN [1] implies that the field discriminant should not be divisible by primes greater than BOUND.

3.4. Imprimitive HALL cases.

3.4.1. *The d=2 imprimitive case.* We can go a bit further (even without the above pre-conditioning) in the imprimitive cases. The $m = 7$ HALL case with $d = 2$ (already solved in [37]) leads us to solve a reduced 4-variable system and get a solution $\tilde{X}(t) \equiv t^7+t^6+3t^5+3t^4+9t^3+7t^2+8t+8 \pmod{11}$, and then by taking the t^7 and t^6 coefficients to be 1, this lifts 11-adically to a solution in the quintic number field given by $z^5 + z^4 - 9z^3 - z^2 + 24z + 18$, which has discriminant $2^4 \cdot 3 \cdot 13 \cdot 17^3$.

Passing on to the case with $d = 9$ and $m = 2$, we have the quaint mod 5 solution $\tilde{X}(t) \equiv t^9 + t^8 + t^7 + t^6 + t^5 - t^4 - t^3 - t^2 - t - 1 \equiv (t-1)^9 \pmod 5$ and this lifts 5-adically as above[26] to a solution in the degree 14 number field given by

$$z^{14} - 6z^{13}+23z^{12} - 52z^{11} + 165z^{10} - 418z^9 + 847z^8 - 484z^7 + \\ + 55z^6 + 1034z^5 - 1375z^4 + 6504z^3 + 3315z^2 - 2098z + 2473.$$

of discriminant $-2^8 3^3 11^{13} 13^2 19^3 23^4$.

3.4.2. *Using pre-conditioning.* For the $(m, d) = (11, 2)$ case, we can imitate the above pre-conditioning method by writing $tX = A^2 + B$ and $t^2Y = A^3 + 3AB/2 + C$ so that $t^3K = (tX)^3 - (t^2Y)^2$, where upon we accrue three extra conditions from $t|tX$ and $t^2|t^2Y$. This allows the $(m, d) = (11, 2)$ case to be reduced from 9 to 5 variables, and we find

$$\tilde{X}(t) \equiv t^{11}+t^{10}-8t^9-7t^8+4t^7-4t^6-7t^5+3t^4-8t^3+4t^2-4t-5 \pmod{19},$$

which lifts to a solution in the field of discriminant $2^{42}3^{78}5^{6}7^{17}13^{7}19^{8}23^{10}29^{5}$ defined by

[26] It might be more expedient to augment the above solution with the additional mod 37 solution $\tilde{X}(t) \equiv t^9 + t^8 + 21t^7 + 19t^6 + 5t^5 + 33t^4 + 4t^3 + 11t^2 + 10t + 15$ mod 37) and use the Chinese Remainder Theorem in concert with the lifting.

$$
\begin{aligned}
&z^{42} + 3z^{41} - 51z^{40} - 823z^{39} + 111z^{38} + 57093z^{37} + 248707z^{36} - 2339859z^{35} - 26222235z^{34} - \\
&- 31251359z^{33} + 903792423z^{32} + 4040148663z^{31} - 24947585794z^{30} - 296796010368z^{29} - \\
&- 747168309174z^{28} + 4083658738306z^{27} + 23149936305291z^{26} - 114975922152621z^{25} - \\
&- 1507706068757736z^{24} - 5447194278960312z^{23} + 1427761982920926z^{22} + \\
&+ 54567517791997596z^{21} - 183472320841748904z^{20} - 3383827892019926802z^{19} - \\
&- 16219184627123312403z^{18} - 24847930381482614049z^{17} + 132250846168628716875z^{16} + \\
&+ 1082184816140391003791z^{15} + 4275306800230408765179z^{14} + \\
&+ 12523877363494806405939z^{13} + 34151493826687416196336z^{12} + \\
&+ 94910396766763402575318z^{11} + 276584063382549595305993z^{10} + \\
&+ 656124395389369676999645z^{9} + 1438348544726835957645039z^{8} + \\
&+ 2196419379272729564383101z^{7} + 5348985419038887561354308z^{6} + \\
&+ 8968331465330410885426980z^{5} + 27704410464576678407794965z^{4} + \\
&+ 29342904135494912055561685z^{3} + 27529540941494277523699155z^{2} + \\
&+ 7629374383438730782242400 5z + 7000990140400625753528858 0.
\end{aligned}
$$

We have not considered whether we can solve the $(m, d) = (13, 2)$ case. It seems likely that pre-conditioning in some manner would allow us to find a liftable local solution after suitable searching, but the identification of the (predicted) field of degree 132 could prove infeasible.

3.4.3. *The $d = 3$ imprimitive* Hall *case.* [First is the m=8 d=3 quadratic solution done above?! easy with Gröbner]

We can similarly solve the imprimitive cases with $d = 3$; here with $m = 11$ our counting indicates that we should have 5 solutions; we do indeed get this, but we do not get a quintic solution, but a quadratic solution (in the Eisenstein field again) and a cubic one.[27] With the field $\rho^2 - \rho + 1 = 0$ and primes $p_3 = \rho + 1$ and $p_7 = \rho + 2$ the quadratic solution is given by

$$
\begin{aligned}
\tilde{X}(t) =& p_3^2 p_7^2 t^7 - 2\rho p_3^2 p_7 (3\rho + 2)^2 t^6 - p_3^4 (101\rho + 123) t^5 + 4\rho^2 p_3^3 (233\rho + 36) t^4 \\
&+ p_3^3 \rho (1593\rho + 214) t^3 - 2 p_3^5 \rho^2 (2\rho + 3)^2 (5\rho + 12) t^2 \\
&+ 7 p_3 (2\rho + 3)(99\rho + 8) t + 2^6 p_3 p_7 (2\rho + 3),
\end{aligned}
$$

while to get the cubic solution we take $\theta^3 - 3\theta + 4 = 0$ and the note the primes of small norm $p_2 = \theta - 1$, $p_3 = \theta^2 + \theta - 3$, and $p_7 = 2\theta + 2\theta - 5$, and the fundamental unit $\eta = \theta^2 - \theta - 7$ to write

$$
\begin{aligned}
\tilde{X}(t) =& p_2^2 p_7^2 t^7 + 2 p_2 p_3 p_7 (\theta^2 + 5\theta + 3) t^6 - p_3 \eta (46\theta^2 - 108\theta + 21) t^5 \\
&+ 4 p_2^3 \eta^2 (6\theta^2 - 4\theta + 43) t^4 + p_2^4 p_3 \eta^2 (36\theta^2 + 90\theta + 169) t^3 \\
&+ 2 p_2^3 p_3 \eta^2 (10\theta^2 + 46\theta - 91) t^2 + 7 p_2^2 p_3^2 (9\theta^2 - 19\theta + 19) t + 4 p_2 p_3^2 p_7 \eta^{-1} (\theta + 2)^4.
\end{aligned}
$$

[27] Again this was already found by Uchiyama and Yorinaga [37], though their requirement of a real embedding precluded them from finding the imaginary quadratic solution.

For the $m = 14$ and $d = 3$ case we compute the mod 13 solution[28] $\tilde{X}(t) \equiv t^9 + t^8 + 3t^7 + 11t^6 + 5t^5 + 8t^4 \pmod{13}$ which lifts to a degree 14 solution in the number field of discriminant $-2^{14}3^{13}7^2 19^2 23^{12}$ given by

$$z^{14} - 5z^{13} + 39z^{12} - 112z^{11} + 749z^{10} - 3381z^9 + 19657z^8 - 70472z^7$$
$$+207090z^6 - 377076z^5 + 548100z^4 - 516006z^3 + 671328z^2 - 628236z + 281988.$$

3.4.4. *Using pre-conditioning.* We can once again imitate the above preconditioning with $tX = A^2 + B$ and $tY = A^3 + 3AB/2 + C$, and this allows the $(d, m) = (17, 3)$ case to be reduced from 9 down to 5 variables quite easily. We then found the liftable solution (with $x_{11} = x_{10} = 1$)

$$\tilde{X}(t) \equiv t^{11} + t^{10} + 17t^9 + 7t^8 + 10t^7 + 7t^6 + 7t^4 + 2t^3 + 11t^2 + 5t + 10 \pmod{19},$$

and find a solution in the field given by

$$\begin{aligned}
&z^{42} - 21z^{41} + 357z^{40} - 3157z^{39} + 21399z^{38} - 92841z^{37} + 379001z^{36} - 1615194z^{35} + \\
&+ 12409824z^{34} - 79785566z^{33} + 425518842z^{32} - 1709972796z^{31} + 6737329690z^{30} - \\
&- 29496757374z^{29} + 142047107304z^{28} - 586672008300z^{27} + 1792337908620z^{26} - \\
&- 3667426051968z^{25} + 4131652833000z^{24} + 1672231182804z^{23} - 13451208812244z^{22} + \\
&+ 27469481376672z^{21} - 17071547686704z^{20} + 31568352216912z^{19} + 10267238531088z^{18} + \\
&+ 114245883023328z^{17} + 113030562558816z^{16} + 70681071970152z^{15} + 328581962104752z^{14} + \\
&+ 125848946528928z^{13} + 362262606854400z^{12} + 104213861403120z^{11} + 90945948420432z^{10} + \\
&+ 113809072219920z^{9} + 53070158253168z^{8} + 15321865127616z^{7} + 33982002762624z^{6} + \\
&+ 23833202901984z^{5} + 2935823831136z^{4} - 2676003075648z^{3} - 784859362560z^{2} + \\
&+ 143865408960z + 70336019520,
\end{aligned}$$

which has discriminant $2^{40}3^{40}5^8 7^{42} 13^6 19^4 29^{15}$.

As above, it might be possible to find a local solution for the next case, but the expected field degree is prohibitive.

3.5. Fermat–Pell case. For the $m = 3$ case, linear substitutions reduce to 6 variables and then two additional resultant steps reduce this to 4; as expected we obtain a nonic solution in the field

$$z^9 - 3z^8 + 9z^7 - 12z^6 + 21z^5 + 27z^4 + 9z^3 + 78z^2 - 144z - 248,$$

which has discriminant $2^{11}3^{10}5^8 \cdot 11 \cdot 13$. We can list the solution as

$$X(t) \equiv t^6 + t^5 + 16t^4 + 13t^3 + 8t^2 + 13t + 15, \quad Q(t) \equiv t^2 + 3t \pmod{17},$$

which lifts with $x_6 = x_5 = y_8 = q_2 = 1$ and $q_1 = 3$.

The $m = 4$ case reduces to a 6-variable system. We were able to obtain the solution $X(t) \equiv t^8 + t^7 + 9t^6 + 17t^5 + 8t^4 + 2t^3 + 11t^2 + 11t + 6 \pmod{19}$ and $Q(t) \equiv t^2 + 3t + 16 \pmod{19}$, and by lifting this (as above) we find a degree 32 solution in the field given by

[28] The observant reader will note that we have $\tilde{X}(t) \equiv t^4(t-5)^5$ and $\tilde{Y}(t) = (t-5)(t-9)^{13}$ with $\tilde{K}(t) \equiv (t-5)^2$. IS THE SMALL DEGREE BAD? CHECK THIS

$$
\begin{aligned}
&z^{32} - 8z^{31} + 26z^{30} + 60z^{29} - 1150z^{28} + 5290z^{27} - 3190z^{26} - 39450z^{25} + 377005z^{24} -\\
&- 621930z^{23} - 2074509z^{22} + 4878072z^{21} - 16800419z^{20} + 7625850z^{19} + 130110540z^{18} +\\
&+ 5954508z^{17} - 22337394z^{16} 140686928z^{15} - 1241944340z^{14} - 2658763840z^{13} -\\
&- 667095612z^{12} + 1005753056z^{11} - 4675425152z^{10} - 5837680000z^{9} + 7173532840z^{8} +\\
&+ 22630238400z^{7} + 15817057920z^{6} - 12929490560z^{5} - 23581070400z^{4} - 12536322560z^{3} +\\
&+ 6534012672z^{2} + 8307615744z + 1803831552,
\end{aligned}
$$

whose discriminant is $-2^{48}3^{17}5^{29}7^{14}11^{6}13^{6}17^{3}19^{3}$.

For the $m = 5$ case, we would probably not be able to use resultants to reduce the system to 8 variables, and in any case, finding a solution in a field of degree 125 is unlikely to be practical. We have not considering whether pre-conditioning could be useful here.

4. Concluding comments

4.1. Acknowledgements. The second author was partially supported by Engineering and Physical Sciences Research Council (EPSRC) grant GR/T00658/01.

The communication between the authors was expedited by a workshop held at the Clay Mathematical Institute. We first became aware of the possibility of homotopy continuation methods during a talk at a conference sponsored by the Heilbronn Institute.

We thank M. Schütt for the reference [32], and A. K. Steel for advising us on the use of resultants in Magma.

References

[1] S. Beckmann, *Ramified primes in the field of moduli of branched coverings of curves.* J. Algebra **125** (1989), no. 1, 236–255, possibly available from `sciencedirect.com` through `dx.doi.org/10.1016/0021-8693(89)90303-7`

[2] G. V. Belyĭ (Г. В. Белый), О расширениях Галуа максимального кругового поля. (Russian) [On Galois extensions of a maximal cyclotomic field]. Изв. РАН. Сер. матем. [Izv. Akad. Nauk SSSR Ser. Mat.] **43** (1979), no. 2, 267–276, 479, possibly available online from `mi.mathnet.ru/izv1682`
English translation in Trans. Math. USSR Izvestia **14** (1980), no. 2, 247–256, possibly available from `turpion.org` through `dx.doi.org/10.1070/IM1980v014n02ABEH001096`

[3] É. Bézout, *Recherches sur le degré des équations résultantes de l'évanouissement des inconnues, Et sur les moyens qu'il convient d'employer pour trouver ces Équations.* (French) [Investigations concerning the degree of equations resulting from the elimination of unknowns, and suitable methods that can be employed to find these equations.] Hist. Acad. Roy. Sci (Paris) [avec Mém. Math. et Phys.] (1764), 288–338. Available online from `gallica.bnf.fr/ark:/12148/bpt6k35622`

[4] B. J. Birch, S. Chowla, M. Hall Jr., A. Schinzel, *On the difference $x^3 - y^2$.* Norske Vid. Selsk. Forh. (Trondheim) **38** (1965), 65–69.

[5] Information about the Magma system is available online from `magma.maths.usyd.edu.au`
W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language.* In *Computational algebra and number theory* Proceedings of the 1st MAGMA Conference held at Queen Mary and Westfield College, London, August 23–27, 1993. Edited

by J. Cannon and D. Holt, Elsevier Science B.V., Amsterdam (1997), 235–265. Cross-referenced as J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Possibly available from `sciencedirect.com` through `dx.doi.org/10.1006/jsco.1996.0125`

[6] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* (German) [An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal]. Doktorarbeit, Institut für Mathematik, Universität Innsbruck, Republik Österreich, 1965. English translation in Journal of Symbolic Computation, Special Issue on Logic, Mathematics, and Computer Science: Interactions, in honor of Bruno Buchberger (60th birthday), **41** (2006), no. 3-4, 475–511. Possibly available online from `sciencedirect.com` through `linkinghub.elsevier.com/retrieve/pii/S0747717105001483`

[7] P. J. Cameron, *Sequences Realized by Oligomorphic Permutation Groups.* Journal of Integer Sequences (electronic) **3** (2000), Article 00.1.5, available (only) online from `www.cs.uwaterloo.ca/journals/JIS/VOL3/groups.html` with Tables at `groupdata.html`

[8] J.-M. Couveignes, *Calcul et rationalité de fonctions de Belyi en genre 0.* (French) [Computation and rationality of Belyi functions (systems?) in genus 0]. Ann. Inst. Fourier (Grenoble) **44** (1994), no. 1, 1–38. Online at `www.numdam.org/item?id=AIF_1994__44_1_1_0`

[9] L. V. Danilov, *The Diophantine equation $x^3 - y^2 = k$ and a conjecture of M. Hall*, Math. Notes Acad. Sci. USSR, **32** (1983), no. 3–4, 617–618, and correction (letter to the editor) in *ibid.* **36** (1984), no. 3–4, 726. Possibly available from `springerlink.com` via `dx.doi.org/10.1007/BF01140190` and `dx.doi.org/10.1007/BF01141949` with the Russian originals appearing as Mat. Zametki **32** (1982), no. 3, 273–275 and *ibid.* **36** (1984), no. 3, 457–458.

[10] H. Davenport, *On $f^3(t) - g^2(t)$.* Norske Vid. Selsk. Forh. (Trondheim) **38** (1965), 86–87.

[11] N. D. Elkies, *Shimura curve computations.* In *Algorithmic number theory*, ANTS-III (Portland, OR 1998), edited by J. Buhler, Springer Lecture Notes in Computer Science **1423** (1998), 1–47. Preprint available online from `arxiv.org/math/0005160` and possibly the paper from `springerlink.com` via `dx.doi.org/10.1007/BFb0054850`

[12] N. D. Elkies, *The identification of three moduli spaces.* Preprint (1999), available online from `arxiv.org/math/9905195`

[13] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues.* In *Computational perspectives on number theory*, Proceedings of the conference in Honor of A. O. L. Atkin (Chicago, IL 1995), edited by D. A. Buell and J. T. Teitelbaum, AMS/IP Studies in Advanced Mathematics, **7**, American Mathematical Society, Providence, RI; International Press, Cambridge, MA (1998), 21–76.

[14] N. D. Elkies, *Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction.* In *Algorithmic number theory*, ANTS-IV (Leiden 2000), edited by W. Bosma, Springer Lecture Notes in Computer Science **1838** (2000), 33–63. Preprint available online at `arxiv.org/math/0005139` and possibly the paper from `springerlink.com` via `dx.doi.org/10.1007/10722028_2`

[15] N. D. Elkies, *Shimura curves for level-3 subgroups of the (2,3,7) triangle group, and some other examples.* In *Algorithmic number theory*, ANTS-VII (Berlin 2006), edited by F. Hess, S. Pauli, and M. Pohst, Springer Lecture Notes in Computer Science **4076** (2006), 302–316. Preprint available online at `arxiv.org/math/0409020` and possibly the paper from `springerlink.com` via `dx.doi.org/10.1007/11792086_22`

[16] C. F. Gauss, *Disquisitiones Arithmeticae.* (Latin) [Arithmetical investigations] (1801). Online from his complete works (1863): `resolver.sub.uni-goettingen.de/purl?PPN235993352` English translation: A. A. Clarke, *Disquisitiones Aritmeticae*, Yale Univ. Press (1965).

[17] T. Gunji, S. Kim, M. Kojima, A. Takeda, K. Fujisawa, T. Mizutani, *PHoM – a Polyhedral Homotopy Continuation Method for Polynomial Systems.* Research Report B-386, Dept. of Mathematical and Computing Sciences, Tokyo Institute of Technology, Meguro, Tokyo 152-8552, Japan, December 2002, revised January 2003. Available online at `www.is.titech.ac.jp/~kojima/PHoM/index.html`

[18] M. Hall Jr., *The Diophantine equation $x^3 - y^2 = k$.* In *Computers in number theory*, Proceedings of the Science Research Council Atlas Symposium No. 2 held at Oxford, from

18–23 August 1969. Edited by A. O. L. Atkin and B. J. Birch. Academic Press, London-New York (1971), 173–198.

[19] A. Hurwitz, *Ueber Riemann'sche Flächen mit gegebenen Verzweigungspunkten.* (German) [On Riemann surfaces with prescribed branch points]. Math. Ann. **39** (1891), 1–61, online at dz-srv1.sub.uni-goettingen.de/sub/digbib/loader?did=D27669 or possibly from springerlink.com via dx.doi.org/10.1007/BF01199469

[20] A. Hurwitz, *Ueber algebraische Gebilde mit eindeutigen Transformationen in sich.* (German) [On algebraic objects with univalent self-transformations]. Math. Ann. **41** (1893), 403–442, online at dz-srv1.sub.uni-goettingen.de/sub/digbib/loader?did=D35962 or possibly from springerlink.com via dx.doi.org/10.1007/BF01443420

[21] A. Kerber, A. Kohnert, Symmetrica, documentation and public domain software available from www.mathe2.uni-bayreuth.de/axel/symneu_engl.html

[22] S. K. Lando, A. K. Zvonkin, *Graphs on surfaces and their applications.* With an appendix by D. B. Zagier. Encyclopaedia of Mathematical Sciences **141**. Low-Dimensional Topology, II. Springer-Verlag, Berlin, 2004. xvi+455 pp.

[23] A. K. Lenstra, H. W. Lenstra Jr., L. Lovász, *Factoring polynomials with rational coefficients.* Math. Ann. **261** (1982), no. 4, 515–534, available from the Göttingen digital library at dz-srv1.sub.uni-goettingen.de/sub/digbib/loader?did=D129327 or possibly from springerlink.com via dx.doi.org/10.1007/BF01457454

[24] J. S. Leon, *On an algorithm for finding a base and a strong generating set for a group given by generating permutations.* Math. Comp. **35** (1980), no. 151, 941–974. Possibly available from jstor.org through dx.doi.org/10.2307/2006206

[25] R. C. Mason, *Diophantine equations over function fields.* London Mathematical Society Lecture Note Series **96**. Cambridge University Press, Cambridge (1984), x+125 pp.

[26] D. W. Masser, *Note on a conjecture of Szpiro.* Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988), Astérisque **183** (1990), 19–23.

[27] B. H. Matzat, *Konstruktive Galoistheorie*, (German) [Constructive Galois theory], Lecture Notes in Mathematics, **1284**, Springer-Verlag, Berlin, 1987.

[28] J. Oesterlé, *Nouvelles approches du «théorème» de Fermat.* (French) [New approaches to Fermat's "theorem"]. Séminaire Bourbaki, Vol. 1987/88, Astérisque **161-162** (1988), Exp. **694** (1989), no. 4, 165–186.

[29] PARI/GP, CVS development version 2.4.2-1896, Université Bordeaux I, Bordeaux, France, November 2007. Online at pari.math.u-bordeaux.fr

[30] B. Riemann, *Theorie der Abel'schen Functionen.* (German) [Theory of Abel's Functions]. J. Reine Angew. Math. **54** (1857), 115–155. Available from the Göttingen digital library at dz-srv1.sub.uni-goettingen.de/sub/digbib/loader?did=D266795 or transcription available from www.maths.tcd.ie/pub/HistMath/People/Riemann/AbelFn

[31] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, v. 1, Jones and Bartlett, Boston, 1992.

[32] T. Shioda, *Elliptic surfaces and Davenport-Stothers triples,* Comment. Math. Univ. St. Pauli **54** (2005), 49–68. See www.rkmath.rikkyo.ac.jp/math/shioda/papers/esdstadd.pdf

[33] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences.* Available online at www.research.att.com/~njas/sequences

[34] A. J. Sommese, C. W. Wampler, II, *The numerical solution of systems of polynomials arising in engineering and science.* World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.

[35] W. W. Stothers, *Polynomial identities and Hauptmoduln.* Quart. J. Math. Oxford Ser. (2) **32** (1981), no. 127, 349–370, online: qjmath.oxfordjournals.org/cgi/reprint/32/3/349

[36] J. J. Sylvester *On a Theory of the Syzygetic relations of two rational integral functions, comprising an application to the Theory of Sturm's Functions, and that of the greatest Algebraical Common Measure.* Phil. Trans. Roy. Soc. London **143** (1853), 407–548. Online: links.jstor.org/sici?sici=0261-0523%281853%29143%3C407%3AOATOTS%3E2.0.CO%3B2-R

[37] S. Uchiyama, M. Yorinaga, *On the difference $f^3(x) - g^2(x)$.* Tsukuba J. Math. **6** (1982), no. 6, 215–230. Possibly available via hdl.handle.net/2241/7076

[38] J. Verschelde, *Algorithm 795: PHCpack: A General-Purpose Solver for Polynomial Systems by Homotopy Continuation.* ACM Trans. Math. Softw. **25** (1999), no. 2, 251–76. Online at `doi.acm.org/10.1145/317275.317286` with more information and documentation at `www.math.uic.edu/~jan/PHCpack/phcpack.html`

[39] K. Takeuchi, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo, **24** (1977), 201–212.

[40] M. Watkins, *A note on integral points on elliptic curves.* Including an appendix written by N. D. Elkies. J. Théor. Nombres Bordeaux, **18** (2006), no. 3, 707–19. Preprint available online at `arxiv.org/math/0604097`

[41] U. Zannier, *On Davenport's bound for the degree of $f^3 - g^2$ and Riemann's existence theorem.* Acta Arith. **71** (1995), no. 2, 107–137. Possibly available online from `matwbn.icm.edu.pl/ksiazki/aa/aa71/aa7122.pdf`
Addenda and acknowledgement of (Stothers') priority in *ibid.* **74** (1996), no. 4, 387. Possibly available online from `matwbn.icm.edu.pl/ksiazki/aa/aa74/aa7447.pdf`

Noam D. Elkies
Department of Mathematics
Harvard University
One Oxford Street
Cambridge, MA 02138
United States of America
E-mail : `elkies@math.harvard.edu`

Mark Watkins
Department of Mathematics
University Walk
University of Bristol
Bristol, BS8 1TW
England
E-mail : `watkins@maths.usyd.edu.au`