WIEFERICH PAST AND FUTURE

NICHOLAS M. KATZ

1. The early history

Fermat's Last Theorem (FLT) is the assertion that for $n \geq 3$, the equation $X^n + Y^n = Z^n$ has no solutions in integers X, Y, Z with $XYZ \neq 0$. It was proven by Fermat for $n = 4$ and by Euler for $n = 3$, cf. [Weil, page 104]. To prove it in general, then, it suffices to prove it when n is any prime $p \geq 5$. For fixed p, the "first case" of FLT is the assertion that there are no integer solutions with XYZ prime to p.

In 1909, Arthur Wieferich, then a 25 year old student at Munster, astounded the mathematical world with the following theorem.

Theorem 1.1. (Wieferich) *Let $p \geq 5$ be a prime. If the first case of FLT is false, then the following congruence holds:*

$$2^{p-1} \equiv 1 \mod p^2.$$

A prime p for which this congruence holds is called a Wieferich prime (later, a Wieferich prime to the base 2). It wasn't until 1913 that the first Wieferich prime, 1093, was found, by Meissner. The second, 3511, was found by Beeger in 1922. Computer search so far shows that the next one, if there is a next one, exceeds 6.7×10^{15}, cf. [Do-Kl].

The very next year, 1910, Mirimanoff showed that one could replace 2 by 3.

Theorem 1.2. (Mirimanoff) *Let $p \geq 5$ be a prime. If the first case of FLT is false, then the following congruence holds:*

$$3^{p-1} \equiv 1 \mod p^2.$$

A prime p for which this congruence holds is called a Wieferich prime to the base 3. The first one is 11, the next, found by Kloss in 1965, cf. [Son, 3.2], is 1006003, and the next one, if it exists, exceeds 9.7×10^{14}, cf. [Do-Kl]. At this point, the race was on.

In 1914, Vandiver showed that one could replace 2 or 3 by 5.

Theorem 1.3. (Vandiver) *Let $p \geq 7$ be a prime. If the first case of FLT is false, then the following congruence holds:*

$$5^{p-1} \equiv 1 \mod p^2.$$

There are now six known Wieferich primes to the base 5, namely

$$20771, 40487, 53471161, 1645333507, 6692367337, 188748146801.$$

The first two of these were found in 1961, the last in 2005. If there is a next one, it exceeds 9.7×10^{14}, cf. [Do-Kl].

In 1917, Pollaczek claimed one could replace 2 by any prime ≤ 31, cf. [Gr-Mo]. The current record, set is 1994 by Suzuki, is that one can replace 2 by any prime

≤ 113. [At this point, Wiles and Taylor-Wiles had proven FLT in general, so the motivation for going further disappeared.]

2. The Crandall-Dilcher-Pomerance model

For a nonzero integer a and a prime p not dividing a, we form the "Fermat quotient"

$$q_a(p) := \frac{a^{p-1}-1}{p} \bmod p.$$

For fixed p, the map

$$\{a \in \mathbb{Z} | p \nmid a\} \mapsto q_a(p)$$

defines a surjective homomorphism from $(\mathbb{Z}/p^2\mathbb{Z})^\times$ to $\mathbb{F}_p$. The Crandall-Dilcher-Pomerance model [Cr-Di-Po, &3. Statistical Considerations] proposes that if we fix an integer $a \neq 0, \pm 1$ and view the resulting sequence $\{q_a(p)\}_{p\nmid a}$ in the product $\prod_{p\nmid a}\mathbb{F}_p$, then we get a "random" element of this product, for its Haar measure of total mass one.

To see what this implies, we apply the strong law of large numbers, cf. [Ito, Thm. 4.5.1]. For each prime $p \nmid a$, we have the function f_p on $\mathbb{F}_p$ which is the characteristic function of A mod p. These functions are independent, the expectation of f_p is $E(f_p) = 1/p$, and its variance is bounded by $Var(f_p) \leq 2/p$. So for any real $\epsilon > 0$ the series $\sum_p Var(f_p)/(\log\log p)^{1+\epsilon} \leq \sum_p 2/p(\log\log p)^{1+\epsilon}$ converges. The strong law of large numbers then asserts that the sequence of functions

$$\frac{\sum_{p\leq X, p\nmid a}(f_p - 1/p)}{(\log\log X)^{\frac{1+\epsilon}{2}}}$$

converges to zero on a set of measure one. In other words, the set of elements $\{x_p\}_{p\nmid a}$ in $\prod_{p\nmid a}\mathbb{F}_p$ for which we have the asymptotic formula

$$\#\{p \leq X, p \nmid a, x_p = A \bmod p\} \cong \log\log X + o((\log\log X)^{\frac{1+\epsilon}{2}})$$

as $X \to \infty$ is a set of measure one.

If the particular sequence $\{q_a(p)\}_{p\nmid a}$ shares this measure one property, we get the prediction that as $X \to \infty$, we have $q_a(p) = A \bmod p$ for about $\log\log X$ of the primes $p \nmid a, p \leq X$.

When a is itself prime, and we take $A = 0$, we get the prediction that as $X \to \infty$, the number of Wieferich primes to the base a is asymptotic to $\log\log X$. This model then predicts both that there are infinitely many Wieferich primes to the base a, and that no computer experiment will ever convince us of it.

3. Another point of view: the Wieferich Conjecture, first version

The Crandall-Dilcher-Pomerance prediction is analogous to the Lang-Trotter conjecture [L-T] for an elliptic curve E over $\mathbb{Q}$, say with good reduction at primes $p \nmid N$; this conjecture predicts, for each integer A, an asymptotic formula for the number of primes $p \leq X, p \nmid N$, for which $p + 1 - \#E(\mathbb{F}_p) = A$, cf. [Ka-LTR].

The Sato-Tate conjecture (now a theorem), on the other hand, concerns the distribution in the closed interval $[-2, 2]$ of the sequence, indexed by primes $p \nmid N$, of normalized (Hasse bound) quantities

$$\frac{p + 1 - \#E(\mathbb{F}_p)}{\sqrt{p}}.$$

Its natural analogue is then the following conjecture, which we call the Wieferich Conjecture. To formulate it, we define, for a nonzero integer a and a prime p not dividing a, the "Wieferich quotient"

$$W_a(p) := \frac{a^{p-1}-1}{p^2} \in (1/p)\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z} \subset \mathbb{R}/\mathbb{Z}.$$

As p varies, all the Wieferich quotients $W_a(p)$ lie in the same[1] compact group, namely $\mathbb{R}/\mathbb{Z}$.

Recall that given a compact space Y together with a Borel probability measure μ on Y, a sequence of points $y_n, n \geq 1$ in Y is said to be equidistributed for the measure μ if, for any continuous $\mathbb{C}$-valued function f on Y, we have the integration formula

$$\int_Y f(y)d\mu = \lim_{M\to\infty} (1/M)\sum_{i=1}^{M} f(y_i).$$

Conjecture 3.1. (Wieferich Conjecture, first form) *For any integer $a \neq 0, \pm 1$, the sequence of its Wieferich quotients $W_a(p)$, indexed by primes $p \nmid a$, is equidistributed in $\mathbb{R}/\mathbb{Z}$ for its Haar measure of total mass one. Equivalently, the sequence of points $\exp(2\pi i W_a(p))$, indexed by primes $p \nmid a$, is equidistributed in the unit circle S^1 for its Haar measure of total mass one: for any continuous $\mathbb{C}$-valued function f on S^1, we have the integration formula*

$$(1/2\pi)\int_0^{2\pi} f(\theta)d\theta = \lim_{X\to\infty} (1/\#\{p \leq X, p \nmid a\}) \sum_{p\leq X, p\nmid a} f(W_a(p)).$$

4. the general setting for a conjecture of Wieferich type

Suppose we are given an integer $N \geq 1$ and a smooth group scheme G over $\mathbb{Z}[1/N]$ with geometrically connected fibres of dimension $d \geq 1$. We have $Lie(G)$, a free $\mathbb{Z}[1/N]$-module of rank d. We choose a free $\mathbb{Z}$-module $\mathbb{L}ie(G)$ together with an isomorphism $Lie(G) \cong \mathbb{L}ie(G) \otimes_{\mathbb{Z}} \mathbb{Z}[1/N]$. For each prime $p \nmid N$, we have a short exact sequence of finite groups

$$0 \to \mathbb{L}ie(G) \otimes_{\mathbb{Z}} (p\mathbb{Z}/p^2\mathbb{Z}) \to G(\mathbb{Z}/p^2\mathbb{Z}) \to G(\mathbb{F}_p) \to 0.$$

If we are given in addition a point $P \in G(\mathbb{Z}[1/N])$, we can play the following game. For each prime $p \nmid N$, define

$$n_p := \#G(\mathbb{F}_p),$$

and denote by P_{p^2} the image of P in $G(\mathbb{Z}/p^2\mathbb{Z})$. Then $n_p P_{p^2}$ lies in $G(\mathbb{Z}/p^2\mathbb{Z})$ and dies in $G(\mathbb{F}_p)$, so lies in $\mathbb{L}ie(G) \otimes_{\mathbb{Z}} (p\mathbb{Z}/p^2\mathbb{Z})$. Given this data

$$(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie(G)),$$

we then define, for each prime $p \nmid N$, the Wieferich quotient

$$W_P(p) := \frac{n_p P_{p^2}}{p^2} \in (1/p)\mathbb{L}ie(G)/\mathbb{L}ie(G) \subset \mathbb{L}ie(G) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \subset \mathbb{L}ie(G) \otimes_{\mathbb{Z}} (\mathbb{R}/\mathbb{Z}).$$

When we start with an integer $a \neq 0, \pm 1$ and view it as a point $P \in \mathbb{G}_m(\mathbb{Z}[1/a])$, then with $G := \mathbb{G}_m/\mathbb{Z}[1/a] = \mathrm{Spec}\,(\mathbb{Z}[1/a][t, 1/t])$, $N = a$, and with $\mathbb{L}ie(G) :=$

[1]However, one should remember that $W_a(p)$ lies in $(1/p)\mathbb{Z}/\mathbb{Z}$, so for odd p, $W_a(p) \neq 1/2$ in $\mathbb{R}/\mathbb{Z}$. Thus for p odd, $W_a(p)$ has a unique representative in the open interval $(-1/2, 1/2)$.

$Lie(\mathbb{G}_m/\mathbb{Z}) \cong \mathbb{Z}$, with basis dual to dt/t, then this "fancy" $W_P(p)$ is just the earlier Wiefeich fraction $W_a(p)$ of the previous section.

In the general case of data

$$(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie(G)),$$

when "should" we expect the sequence of Wieferich fractions $W_P(p)$, indexed by primes $p \nmid N$, to be equidistributed in the compact group $\mathbb{L}ie(G) \otimes_{\mathbb{Z}} (\mathbb{R}/\mathbb{Z}) \cong (\mathbb{R}/\mathbb{Z})^d$ for its Haar measure of total mass one?

We will answer this in a series of lemmas.

Lemma 4.1. *Suppose $(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie(G))$ is a situation for which the sequence of Wieferich fractions $W_P(p)$ is equidistributed in $\mathbb{L}ie(G) \otimes_{\mathbb{Z}} (\mathbb{R}/\mathbb{Z})$. Then for any integer $m \neq 0$, the sequence of Wieferich fractions $W_{mP}(p)$ is equidistributed in $\mathbb{L}ie(G) \otimes_{\mathbb{Z}} (\mathbb{R}/\mathbb{Z})$.*

Proof. By the Weyl criterion, equidistribution of the sequence of Wieferich fractions $W_P(p)$ holds if and only if, for every nontrivial continuous character

$$\chi : \mathbb{L}ie(G) \otimes_{\mathbb{Z}} (\mathbb{R}/\mathbb{Z}) \to S^1,$$

we have, writing $\pi(X, N)$ for $\#\{p \leq X, p \nmid N\}$,

$$\lim_{X\to\infty} (1/\pi(X, N)) \sum_{p\leq X, p\nmid N} \chi(W_P(p)) = 0.$$

For each p, we have $W_{mP}(p) = mW_P(p)$, so the Weyl criterion still holds, simply because the character group of $\mathbb{L}ie(G) \otimes_{\mathbb{Z}} (\mathbb{R}/\mathbb{Z})$ is torsion free. □

Lemma 4.2. *Suppose $(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie(G))$ is a situation for which the sequence of Wieferich fractions is equidistributed in $\mathbb{L}ie(G) \otimes_{\mathbb{Z}} (\mathbb{R}/\mathbb{Z})$. Then G is commutative, and the cyclic subgroup generated by P is Zariski dense in $G_{\mathbb{Q}}$ (or equivalently is Zariski dense in $G_{\mathbb{C}}$).*

Proof. We first prove the Zariski density statement. Denote by $H \subset G$ the Zariski closure of the cyclic subgroup generated by P. Replacing if necessary P by a nonzero multiple mP, we replace $H_{\mathbb{C}}$ by its identity component, but we keep the equidistribution, thanks to the lemma above. So we may assume that $H_{\mathbb{C}}$ is connected. Inverting finitely many more primes if necessary, we may further assume that $H/\mathbb{Z}[1/N]$ is a smooth group scheme with geometrically connected fibres of some dimension $d_0 \geq 0$. If $d_0 = d$, then $H = G$. A fortiori, the (larger) cyclic subgroup generated by the original point P is Zariski dense in G. Once G has a Zariski dense abelian subgroup, G is commutative.

If $d_0 < d$, then $Lie(H)_{\mathbb{Q}}$ is a proper subspace of $Lie(G)_{\mathbb{Q}}$. Let us define $\mathbb{L}ie(H) := \mathbb{L}ie(G) \cap Lie(H)_{\mathbb{Q}}$, intersection inside $Lie(G)_{\mathbb{Q}}$. After possibly inverting finitely many primes, $\mathbb{L}ie(H)$ is a $\mathbb{Z}$ form of $Lie(H)$. Now all the Wieferich fractions $W_P(p)$ lie in $\mathbb{L}ie(H) \otimes_{\mathbb{Z}} (\mathbb{R}/\mathbb{Z})$, which is a close set of measure zero in the larger group $\mathbb{L}ie(G) \otimes_{\mathbb{Z}} (\mathbb{R}/\mathbb{Z})$, so cannot be equidistributed in that larger group. □

Lemma 4.3. *If $G/\mathbb{Z}[1/N]$ is commutative, and we choose a lattice $\mathbb{L}ie(G)$, then for each prime $p \nmid N$, the maps*

$$G(\mathbb{Z}[1/N]) \to G(\mathbb{Z}/p^2\mathbb{Z})$$

and

$$G(\mathbb{Z}/p^2\mathbb{Z}) \to (1/p)\mathbb{L}ie(G)/\mathbb{L}ie(G) \subset \mathbb{L}ie(G) \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z}, \quad P \mapsto w_P(p),$$

are group homomorphisms.

Proof. The first map is always a homomorphism, whether or not G is commutative. For the second, it is simply the fact that when G is commutative, multiplication by an integer, here n_p, is a group homomorphism. In our case, it maps $G(\mathbb{Z}/p^2\mathbb{Z})$ to

$$\mathrm{Ker}(G(\mathbb{Z}/p^2\mathbb{Z}) \twoheadrightarrow G(\mathbb{F}_p)) \cong \mathbb{L}ie(G) \otimes (p\mathbb{Z}/p^2\mathbb{Z}) \overset{1/p^2}{\cong} (1/p)\mathbb{L}ie(G)/\mathbb{L}ie(G).$$

□

Lemma 4.4. *If $G/\mathbb{Z}[1/N]$ is $\mathbb{G}_a$, the additive group, then Wieferich equidistribution fails for any choice of $P \in G(\mathbb{Z}[1/N]) = \mathbb{Z}[1/N]$ and any choice of $\mathbb{L}ie(G)$.*

Proof. We argue by contradiction. Suppose Wieferich equidistribution holds for a choice of $P \in G(\mathbb{Z}[1/N]) = \mathbb{Z}[1/N]$ and a choice of $\mathbb{L}ie(G)$

Write P as a fraction a/b, with integers a, b, $b \geq 1$, b dividing some power of N. Denote by e_0 the $\mathbb{Z}$-basis of the "standard" choice of $\mathbb{L}ie(G)$ as $\mathbb{G}_a$ itself. Then our $\mathbb{Z}$-form $\mathbb{L}ie(G)$ has basis of the form ce_0/d, for some nonzero integers c and d which each divide a power of N. Using the basis ce_0/d and $P = a/b$ is the same as using ad/bc and the standard basis e_0. So we may assume we have Wieferich equidistribution for some P and the standard choice of $\mathbb{L}ie(G)$.

Now we apply Lemma 4.1 to clear the denominator, if any, of P, to reduce further to the case when $P = ad$ is an integer. As $n_p = p$, we have $W_P(p) = ad/p \in \mathbb{R}/\mathbb{Z}$. But this sequence $\{ad/p\}_p$ tends to 0, so averaging a continuous function f over it computes $f(0)$, not its integral over $\mathbb{R}/\mathbb{Z}$ for Haar measure. □

Proposition 4.5. *Suppose we have a situation $(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie(G))$ as in the start of this section. If G contains the additive group G_a as a normal subgroup, then Wieferich equidistribution fails.*

Proof. If G is G_a, this is the previous result. So it suffices to treat the case when G contains the additive group G_a as a normal subgroup of strictly lower dimension. At the expense of enlarging N, we may assume that we have a short exact sequence of smooth groupschemes over $\mathbb{Z}[1/N]$,

$$0 \to G_a \to G \to H \to 0$$

and a short exact sequence of their Lie algebras. We get a $\mathbb{Z}$-form $\mathbb{L}ie(H)$ of $Lie(H)$ by taking the image of $\mathbb{L}ie(G)$. For each good prime p, we have the two group orders

$$n_{p,G} := \#G(\mathbb{F}_p), \quad n_{p,H} := \#H(\mathbb{F}_p),$$

related by

$$n_{p,G} = pn_{p,H}.$$

Denote by $\phi : G \to H$ the projection onto the quotient. The Wiefrich fractions $W_P(p) \in \mathbb{L}ie(G) \otimes \mathbb{R}/\mathbb{Z}$ and $W_{\phi(P)}(p) \in \mathbb{L}ie(H) \otimes \mathbb{R}/\mathbb{Z}$ are hence related by

$$\phi(W_P(p)) = pW_{\phi(P)}(p).$$

But for each good p, $W_{\phi(P)}(p)$ is a p-torsion element of $\mathbb{L}ie(H) \otimes \mathbb{R}/\mathbb{Z}$, and hence

$$\phi(W_P(p)) = 0 \text{ in } \mathbb{L}ie(H) \otimes \mathbb{R}/\mathbb{Z}.$$

Equivalently, all the Wieferich fractions $W_P(p)$ lie in the proper subtorus

$$\mathbb{L}ie(G_a) \otimes \mathbb{R}/\mathbb{Z} \subset \mathbb{L}ie(G) \otimes \mathbb{R}/\mathbb{Z}.$$

Hence they are certainly not equidistributed in $\mathbb{L}ie(G) \otimes \mathbb{R}/\mathbb{Z}$. □

Proposition 4.6. *Suppose $(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie(G))$ is a situation in which Wieferich equidistribution holds. If G is an affine algebraic group, then $G_{\mathbb{Q}}$ is a torus.*

Proof. Say $G \subset GL(d)$. Then $G_{\mathbb{Q}}$ is the Zariski closure of the cyclic subgroup generated by some element $P \in GL(d, \mathbb{Q})$. Use Jordan decomposition to write $P = su = us$ with $s \in G(\mathbb{Q}) \subset GL(d, \mathbb{Q})$ semi simple, $u \in G(\mathbb{Q}) \subset GL(d, \mathbb{Q})$ unipotent. Denote by S and U the Zariski closures in $GL(d)_{\mathbb{Q}}$ of the cyclic groups generated by s and u respectively. Then $S \subset G_{\mathbb{Q}}$ has identity component S^0 a torus, $U \subset G_{\mathbb{Q}}$ is a unipotent group, S and T are commuting subgroups of G_Q, and $G_{\mathbb{Q}}$ is the product $S \times U$. [As $\mathbb{G}_{\mathbb{Q}}$ is geometrically connected, we see a posteriori that $S = S^0$.] Thus we have a closed normal homomorphism $U \subset G_{\mathbb{Q}}$. If U is trivial, we are done. If not, then U has a $\mathbb{G}_a$ subgroup, and hence $G_{\mathbb{Q}}$, being abelian, has $\mathbb{G}_a$ as a normal subgroup. But this is impossible, in view of Proposition 4.5 above. □

Conjecture 4.7. (Robust Wieferich Conjecture, affine case)*Let $G/\mathbb{Z}[1/N]$ be a torus, and $P \in G(\mathbb{Z}[1/N])$ a point such that the cyclic group generated by P is Zariski dense in $G_{\mathbb{Q}}$. Then for any $\mathbb{Z}$-form $\mathbb{L}ie(G))$ of $Lie(G)$, the situation $(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie(G))$ has Wieferich equidistribution.*

5. Interlude: The question of robustness

Suppose we have a situation $(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie(G))$ for which Wieferich equidistribution holds. Is it true that for any **other** choice $\mathbb{L}ie_1(G)$ of lattice in $Lie(G)$, the modified situation $(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie_1(G))$ also has Wieferich equidistribution.We do not know how to prove this. Moreover, as an "abstract" statement about equidistribution, it is false.

Here is a cautionary counterexample, due to Deligne. Suppose that we have a sequence of fractions $a_p/p, 0 \leq a_p \leq p-1$, indexed by odd primes p, which is equidistributed in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z}$ (for Haar measure). If we change the choice of lattice from $\mathbb{Z}$ to $2\mathbb{Z}$, then we are asking about the equidistribution in $\mathbb{R}/\mathbb{Z}$ of the sequence $d_p/p, 0 \leq d_p \leq p-1$, with d_p defined by the congruence $2d_p = a_p \bmod p$. Imagine that in our original sequence, each a_p is even, say $a_p = 2b_p$, with $0 \leq b_p \leq (p-1)/2$. Then for each p we have $d_p = b_p$, and visibly this sequence b_p/p is **not** equidistributed in $\mathbb{R}/\mathbb{Z}$, as each term lies in the interval $[0, 1/2]$.

How do we know there exist sequences $\{a_p/p, 0 \leq a_p \leq p-1\}_{\text{odd } p}$ which are equidistributed in $\mathbb{R}/\mathbb{Z}$ in which every a_p is even? In the product space $\prod_{\text{odd } p} \mathbb{R}/\mathbb{Z}$ with the product measure, the set of sequences $\{x_p\}_{\text{odd } p}$ which are equidistributed in $\mathbb{R}/\mathbb{Z}$ for Haar measure has measure one. So there exist such sequences. Take one, and replace, term by term, x_p by the nearest fraction of the form $2b_p/p, 0 \leq b_p \leq (p-1)/2$; break ties arbitrarily. The distance (say measured in S^1 as arc length) between x_p and $2b_p/p$ is at most $2\pi/p$, so tends to zero as p grows. Because continuous functions on a compact metric space are uniformly continuous, if the sequence x_p is equidistributed, then so is any sequence y_p for which $dist(x_p, y_p) \to 0$. In particular, our sequence $\{2b_p/p\}$ is equidistributed.

On the other hand, if we have Wieferich equidistribution for $(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie(G))$, then for any choice of larger lattice $\mathbb{L}ie(G) \subset \mathbb{L}ie_1(G)$, we will also have Wieferich equidistribution for $(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie_1(G))$. This results from the following lemma, a slight generalization of Lemma 4.1.

Lemma 5.1. *Let $V_{\mathbb{R}}$ be a finite dimensional $\mathbb{R}$ vector space, $\mathbb{L}_1 \subset V_{\mathbb{R}}$ a lattice, and $\mathbb{L} \subset \mathbb{L}_1$ a subgroup of finite index. Suppose x_n is a sequence of points in $\mathbb{L} \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} = V_{\mathbb{R}}/\mathbb{L}$ which is equidistributed for Haar measure. Then its image in the quotient group $\mathbb{L}_1 \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} = V_{\mathbb{R}}/\mathbb{L}_1$ is equidistributed for Haar measure.*

Proof. This resuits from the Weyl criterion. For some integer $m \geq 1$, we have $m\mathbb{L}_1 \subset \mathbb{L} \subset \mathbb{L}_1$. The character group of $V_{\mathbb{R}}/\mathbb{L}_1$ is torsion free, so any nontrivial character remains nontrivial when pulled back to $V_{\mathbb{R}}/m\mathbb{L}_1$, and a fortiori remains nontrivial when pulled back to $V_{\mathbb{R}}/\mathbb{L}$. □

6. The framed Wieferich conjecture

In this section, we propose a way to avoid questions of robustness. Given a smooth group scheme $G/\mathbb{Z}[1/N]$, we define a framing of $G/\mathbb{Z}[1/N]$ to be a pair (G_1, ϕ) consisting of a smooth group scheme $G_1/\mathbb{Z}$ and an injective homomorphism of smooth group schemes over $\mathbb{Z}[1/N]$, $\phi : G \subset G_1 \otimes_{\mathbb{Z}} \mathbb{Z}[1/N]$.

A framing gives rise to a $\mathbb{Z}$ form $\mathbb{L}ie(G)$ of $Lie(G)$, as follows. We have

$$Lie(G/\mathbb{Z}[1/N]) \subset Lie(G_1/\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}[1/N] \subset Lie(G_1/\mathbb{Z}),$$

and we define

$$\mathbb{L}ie(G) := Lie(G/\mathbb{Z}[1/N]) \cap Lie(G_1/\mathbb{Z}).$$

Here are two extreme examples of framings. If G is an affine algebraic group, embed it in some $GL(d)$, and take G_1 to be that $GL(d)$. If $G/\mathbb{Z}[1\mathbb{N}]$ extends to a smooth group scheme $G_1/\mathbb{Z}$, use G_1. For example, if L is a $\mathbb{Z}$-algebra which is a free, finitely generated $\mathbb{Z}$-module, then $L^\times$, the group scheme over Z whose A-valued points, for variable $\mathbb{Z}$-algebras A, are $(A \otimes_Z L)^\times$, is smooth over $\mathbb{Z}$.

Here is an intermediate example. Take for D any nonzero nonsquare integer, and take the quadratic order $R := \mathbb{Z} + \mathbb{Z}\sqrt{D}$. As in the paragraph above, the group scheme $R^\times$ over Z is smooth over $\mathbb{Z}$. The subgroup $G \subset R^\times$ defined by $Norm = 1$, whose A-valued points are the elements $x + y\sqrt{D}$, $x, y \in A$, satisfying $x^2 - Dy^2 = 1$, is smooth over $\mathbb{Z}[1/2]$, but not over $\mathbb{Z}$. So here we might take G_1 to be $R^\times$. Then $Lie(R^\times) = R$ and we get $\mathbb{L}ie(G)) = \mathbb{Z}\sqrt{D}$, the elements in R having trace zero. [On the other hand, if D is squarefree and is 1 mod 4, then the $Norm = 1$ subgroup of $\mathcal{O}^\times$ for $\mathcal{O} := \mathbb{Z} + \mathbb{Z}\delta, \delta := (1 + \sqrt{D})/2$, is itself smooth over $\mathbb{Z}$, and its Lie consists of the elements in $\mathcal{O}$ of trace zero.]

Conjecture 6.1. (Framed Wieferich Conjecture, affine case)*Let $G/\mathbb{Z}[1/N]$ be a torus, $P \in G(\mathbb{Z}[1/N])$ a point which generates a Zariski dense subgroup of $G_{\mathbb{Q}}$, (G_1, ϕ) a framing of $G/\mathbb{Z}[1/N]$ and $\mathbb{L}ie(G))$ the resulting lattice. Then the situation $(G/\mathbb{Z}[1/N], P \in G(\mathbb{Z}[1/N]), \mathbb{L}ie(G))$ has Wieferich equidistribution.*

7. The case of elliptic curves and products thereof

Let us begin with an elliptic curve $E/\mathbb{Q}$. We choose a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with all coefficients $a_i \in \mathbb{Z}$. Following Silverman [Si, IV, Thm. 5.3], we denote by $\mathcal{W} \subset \mathbb{P}^2_{\mathbb{Z}}$ the closed subscheme defined by the corresponding projective equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

One knows[Si, IV, Thm. 5.3] that the open set $\mathcal{W}^{sm} \subset \mathcal{W}$ where $\mathcal{W}$ is smooth over $\mathbb{Z}$ is a smooth group scheme. Its Lie algebra is the free $\mathbb{Z}$-module $H^1(\mathcal{W}, \mathcal{O}_{\mathcal{W}})$,

the $\mathbb{Z}$ dual of the free $\mathbb{Z}$ module spanned by the invariant differential $dx/(2y+a_1x)$. Concretely, this means that we take x/y as a uniformizing parameter along the zero section " ∞", and view the Lie algebra as the free $\mathbb{Z}$-module on x/y (viewed as a basis of I/I^2, for I the ideal sheaf defining the zero section. Over some $\mathbb{Z}[1/N]$, $\mathcal{W}$ is smooth, and is (necessarily) the Neron model over $\mathbb{Z}[1/N]$ of $E/\mathbb{Q}$. The group scheme $\mathcal{W}^{sm}/\mathbb{Z}$ sits inside the identity component of the Neron model over $\mathbb{Z}$ of $E/\mathbb{Q}$, but is equal to it if and only if the chosen Weierstrass equation is minimal.

Conjecture 7.1. (Ellliptic Wieferich Conjecture) *Given an integer Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

of an elliptic curve over $\mathbb{Q}$, with good reduction over $\mathbb{Z}[1/N]$, and a point $P \in E(\mathbb{Q}) = \mathcal{W}(\mathbb{Z}[1/N])$ which is not of finite order (i.e., P generates a Zariski dense subgroup of $E_{\mathbb{Q}}$), then $(\mathcal{W}/\mathbb{Z}[1/N], P \in \mathcal{W}(\mathbb{Z}[1/N), Lie(\mathcal{W}^{sm}/\mathbb{Z}))$ has Wieferich equidistribution.

Bombieri has written a computer program to compute the Wieferich fractions in this case. Computer experiments so far give results compatible with the conjecture.

Remark 7.2. In the elliptic case, each integer Weierstrass equation has its $\mathcal{W}^{sm}$ a subgroup scheme of the Neron model $\mathcal{N}/\mathbb{Z}$ of $E/\mathbb{Q}$. So we have an inclusion $Lie(\mathcal{W}^{sm}/\mathbb{Z}) \subset Lie(\mathcal{N}/\mathbb{Z})$. In view of Lemma 5.1, Wieferich equidistribution for $(\mathcal{W}/\mathbb{Z}[1/N], P \in \mathcal{W}(\mathbb{Z}[1/N), Lie(\mathcal{W}^{sm}/\mathbb{Z}))$ implies Wieferich equidistribution for the "terminal" situation $(\mathcal{N}/\mathbb{Z}[1/N], P \in \mathcal{N}(\mathbb{Z}[1/N), Lie(\mathcal{N}/\mathbb{Z}))$.

Suppose we are given a product of elliptic curves, say $E_1, ..., E_n$ over $\mathbb{Q}$, and in each $E_i(\mathbb{Q})$ a point P_i which is not of finite order. If we suppose that for $i \neq j$, E_i is not geometrically (i.e., over $\mathbb{C}$) isogenous to E_j, then the point $(P_1, ..., P_n)$ generates a Zariski dense subgroup of $(E_1 \times_{\mathbb{Q}} ... \times_{\mathbb{Q}} E_n)_{\mathbb{Q}}$. [To see this, use Goursat's Lemma [Rib, 5.2.1] to treat the case $n = 2$, then proceed by induction, applying Goursat to the product of E_1 with $\prod_{i\geq 2} E_i$.] Then we have the following conjecture.

Conjecture 7.3. *For any choice of integral Weierstrass models $\mathcal{W}_i$ of the E_i, using $\prod_i Lie(\mathcal{W}_i^{sm}/\mathbb{Z})$ as our model for Lie, the sequence of n-tuples of Wieferich fractions $(w_{P_1}(p), ...w_{P_n}(p))$, indexed by primes $p \nmid N$, is equidistributed in the n-fold self product of $\mathbb{R}/\mathbb{Z}$ with itself.*

Or suppose we have a single elliptic curve $E/\mathbb{Q}$, whose Mordell Weil rank (the $\mathbb{Q}$-dimension of $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$) is an integer $n \geq 2$. Let $P_1, ..., P_n \in E(\mathbb{Q})$ form a $\mathbb{Z}$-basis of $E(\mathbb{Q})/(\text{torsion})$. Suppose further that E is geometrically not CM (i.e., that $\text{End}(E_{\mathbb{C}}) = \mathbb{Z}$), then the point $(P_1, ..., P_n)$ generates a Zariski dense subgroup of $E^n_{\mathbb{Q}} := (E \times_{\mathbb{Q}} ... \times_{\mathbb{Q}} E)_{\mathbb{Q}}$. [Use Goursat's Lemma, just as in the paragraph above.] We have the following conjecture.

Conjecture 7.4. *For any choice of integer Weierstrass equation for E, using $\prod_i Lie(\mathcal{W}^{sm}/\mathbb{Z})$, as our model for Lie, the sequence of n-tuples of Wieferich fractions $(w_{P_1}(p), ...w_{P_n}(p))$, indexed by primes $p \nmid N$, is equidistributed in the n-fold self product of $\mathbb{R}/\mathbb{Z}$ with itself.*

Using the Weyl criterion, we see that this conjecture is equivalent to the truth of the elliptic Wiefericn conjecture for E, with lattice $Lie(\mathcal{W}^{sm}/\mathbb{Z})$, for **all** nontrivial

linear combinations $\sum_i n_i P_i$ of the P_i (or equivalently, for E, $Lie(\mathcal{W}^{sm}/\mathbb{Z})$, and every[2] nontorsion point in $E(\mathbb{Q})$).

8. The case of abelian varieties

We begin with an abelian variety $A/\mathbb{Q}$, and denote by $\mathcal{A}/\mathbb{Z}$ its Neron model. We suppose that over $\mathbb{Z}[1/N]$, $\mathcal{A}$ is an abelian scheme (i.e., our $A/\mathbb{Q}$ extends to an abelian scheme over $\mathbb{Z}[1/N]$).

Conjecture 8.1. (Wieferich Conjecture for Abelian varieties) *Suppose given $P \in \mathcal{A}(\mathbb{Z}[1/N]) = A(\mathbb{Q})$ which generates a Zariski dense subgroup of $A_{\mathbb{Q}}$. Then the situation $(\mathcal{A}/\mathbb{Z}[1/N], P \in \mathcal{A}(\mathbb{Z}[1/N]), Lie(\mathcal{A}/\mathbb{Z}))$ has Wieferich equidistribution.*

Unlike the case of elliptic curves, we do not in general know how to specify any explicit smooth extension of $A/\mathbb{Q}$ to a smooth group scheme over $\mathbb{Z}$ other than the Neron model, nor do we have an explicit (i.e., suitable for computer experiment) description of the Neron model. However, there are cases where we can be more explicit.

We can use Raynaud's theorem [Bo-Lu-Ra, Thm. 1 in 9.5] that if X is a regular scheme which is projective and flat over $\mathbb{Z}$ with geometrically reduced and irreducible fibres of dimension one, with $X_{\mathbb{Q}}$ a smooth curve over $\mathbb{Q}$, then $Pic^0_{X/\mathbb{Z}}$ is the Neron model $\mathcal{N}$ of the Jacobian $Jac_{X_{\mathbb{Q}}/\mathbb{Q}}$ of the generic fibre. In this case we have $Lie(Pic^0_{X/\mathbb{Z}}/\mathbb{Z}) = H^1(X, \mathcal{O}_X)$, which is certainly explicit. In the next two sections are some examples of such an $X/\mathbb{Z}$.

9. CM examples

Fix an odd prime ℓ. Define ϵ to be 1 if ℓ is 1 mod 4, and to be -1 if ℓ is -1 mod 4. In other words, ϵ is that choice of sign for which $\epsilon\ell$ is 1 mod 4. Take for X the curve whose affine equation is

$$y^2 + y = x^\ell + \frac{\epsilon\ell - 1}{4},$$

with its section ∞ tacked on. Then X is lisse over $p = 2$ (Artin-Schreier). If we invert 2, we can complete the square to write this as

$$(y + 1/2)^2 = x^\ell + \epsilon\ell/4,$$

i.e., we get the equation (in new variables $Y = (y + 1/2), x$)

$$Y^2 = x^\ell + \epsilon\ell/4.$$

This is lisse over $\mathbb{Z}[1/2\ell]$, so all in all our X is lisse over $\mathbb{Z}[1/\ell]$. The second form of the equation shows that X is regular over $\mathbb{Z}_\ell$.

Its Jacobian, even over $\mathbb{C}$, is simple. Indeed, we have the following (presumably well known) lemma.

Lemma 9.1. *For any odd prime ℓ, and any $a \in \mathbb{C}^\times$, the Jacobian of the curve $C : y^2 = x^\ell + a$ is a simple abelian variety.*

---

[2] In taking nontrivial sums of the P_i, we get every point of the form (a point of infinite order) + (a torsion point). But for primes p not dividing either N or the order of the torsion point, the Wieferich fraction attached to the torsion point vanishes, as for such a prime p, n_p kills the torsion point in $E(\mathbb{Q}) = \mathcal{W}(\mathbb{Z}[1/N])$, so a fortiori kills it in $\mathcal{W}(\mathbb{Z}/p^2\mathbb{Z})$.

Proof. The action of $\zeta \in \mu_\ell$ on C given by $(x,y) \mapsto (\zeta x, y)$ makes the Jacobian a CM abelian variety with CM by the cyclotomic ring $\mathbb{Z}[\zeta_\ell]$. The differentials of the first kind on C have basis the one-forms $x^i dx/y, i = 0$ to $(\ell-3)/2$. So the CM type is the subset $\Phi := \{1, 2, ..., (\ell-1)/2\}$ of $\mathbb{F}_\ell^\times$. The simplicity of this CM Jacobian is equivalent to the statement that in $\mathbb{F}_\ell^\times$, the only element b such that multiplication by b maps the subset Φ to itself is $b = 1$, cf. [Shim-Tan, Prop. 26, page 69] for this equivalence. Let b be such an element. Then b itself must lie in Φ, because 1 lies in Φ. If $b \neq 1$, think of b as an integer in the range $2 \leq b \leq (\ell-1)/2$, and define the integer c by $1 \leq c < b$, $p \equiv c \bmod b$. Then $(p-c)/b$ lies in Φ, but $b \times (p-c)/b = p - c > p - b \geq p - (p-1)/2 > (p-1)/2$ does not lie in Φ,. □

Let us denote by J_ℓ the Jacobian of our curve $C_\ell : y^2 = 4x^\ell + \epsilon\ell$. To test the Wieferich conjecture, we need a rational point P on J_ℓ which is of infinite order. To do this, we look for a rational point Q on the curve C_ℓ, such that the divisor class of $Q - \infty$ is not a torsion point onJ_ℓ. If we find such a Q, we take P to be the class of $Q - \infty$.

Here is one (empirical) approach. Take for ℓ a prime which can be written as

$$\ell = 4 + n^2$$

for some integer n. [Conjecturally, there are infinitely many such ℓ, cf. [Ha-Wr, Conj. F] and [Ba-Ho].] The first few are

$$5 = 4 + 1, 13 = 4 + 3^2, 29 = 4 + 5^3, 53 = 4 + 7^2.$$

Any such ℓ is 1 mod 4, and $Q := (x = -1, y = n)$ is a point on $y^2 = 4x^\ell + \ell$. For each of these first four ℓ, namely $5, 13, 29, 53$, the point $Q - \infty$ has infinite order in J_ℓ. We show this as follows. The polynomial $4x^\ell + \ell$ is $\mathbb{Q}$-irreducible (because it is Eisenstein at ℓ), so $J_\ell(\mathbb{Q})$ has no nontrivial points of order 2. The torsion subgroup $J_\ell(\mathbb{Q})_{tors}$of $J_\ell(\mathbb{Q})$ is thus of odd order. It injects into $J_\ell(\mathbb{F}_p)$ for each odd prime p of good reduction (i.e. for each odd prime $p \neq \ell$), cf. [Ka-Gal, Appendix]. So the order of the torsion subgroup divides the odd part of the gcd of the orders of the groups $J_\ell(\mathbb{F}_{p_i})$ for any finite list of odd primes $p_i \neq \ell$. Taking respectively the pairs of primes $(3, 11)$ for 5, and $(3, 5)$ for each of $13, 29, 53$, we see that in each case the odd part of the gcd is ℓ. So the group $J_\ell(\mathbb{Q})_{tors}$ is either trivial or has order ℓ, in each of these four cases. If the torsion subgroup is trivial, then our nontrivial point $P := Q - \infty$ is necessarily of infinite order. If the torsion subgroup has order ℓ, it suffices to show that the point $P := Q - \infty$ is not of order ℓ. This is a special case of the following lemma (where we go back to the $y^2 = x^\ell + \epsilon\ell/4$ form of the equation).

Lemma 9.2. *Let ℓ be an odd prime, $a \in \mathbb{C}^\times$ any number not of the form $1 + \ell B$ for any $B \in \mathbb{Z}[1/2]$. On the Jacobian of the complex curve $y^2 = x^\ell + a$, neither of the points $(x = -1, y = \pm(a-1)^{1/2}) - \infty$ has order ℓ.*

Proof. We argue by contradiction. Suppose these points have order ℓ. This means there is a function on the curve with zero of order ℓ at $Q = (x = -1, y = (a-1)^{1/2})$, a pole of order ℓ at ∞, and no other zeroes or poles. The functions holomorphic outside ∞ have unique representations as $\mathbb{C}[x] + y\mathbb{C}[x]$. Remember that x has a double pole at ∞, while y has a pole of order ℓ at ∞. So our function must be of the form $R(x) - y$ with $R(x) \in \mathbb{C}[x]$ of degree $\leq (\ell-1)/2$. If it has a zero of order ℓ at $Q = (x = -1, y = (a-1)^{1/2})$, then its image under the hyperelliptic involution,

namely $R(x)+y$, has a zero of order ℓ at $-Q = (x=-1, y=-(a-1)^{1/2})$. Hence their product $(R(x)-y)(R(x)+y) = R(x)^2 - (x^\ell + a)$ must be a scalar multiple of $(x+1)^\ell$, the function whose divisor is $\ell[Q] + \ell[-Q] - 2\ell[\infty]$.

Thus $R(x)^2 - a = \alpha(x+1)^\ell + x^\ell$ for some $\alpha \in \mathbb{C}^\times$. Because $R(x)^2$ has degree at most $\ell - 1$, we must have $\alpha = -1$. Changing $R(x)$ to $iR(x)$, we have the equation

$$(x+1)^\ell - x^\ell = R(x)^2 + a,\ \deg(R) \leq (\ell-1)/2.$$

Dividing by ℓ and replacing $R(x)$ by $R(x)/\sqrt{\ell}$, the equation becomes

$$((x+1)^\ell - x^\ell)/\ell = R(x)^2 + a/\ell,\ \deg(R) \leq (\ell-1)/2.$$

The left hand side is of the form

$$(\text{monic integer poly. without constant term, degree } \ell-1) + 1/\ell.$$

We now use Lemma 9.3 below, applied to $f(x) := ((x+1)^\ell - x^\ell)/\ell$.

With this lemma in hand, we now conclude the proof of Lemma 8.3. In view of the uniqueness, first with $A = B = \mathbb{C}$, then with $A = \mathbb{Z}[1/2]$ and $B = \mathbb{C}$, we see first that $g(x) = R(x)$, hence that $R(x)$ lies in $\mathbb{Z}[1/2][x]$, and we see that $h(x) = a/\ell$. Equating the constant terms in the equality

$$((x+1)^\ell - x^\ell)/\ell = R(x)^2 + a/\ell,$$

and remembering that $R(0) \in \mathbb{Z}[1/2]$, we get the equality

$$1/\ell = R(0)^2 + a/\ell,$$

which shows that a lies in $1 + \ell\mathbb{Z}[1/2]$. □

Lemma 9.3. (cf.[Sh, &3]) *Let $A \subset B$ be rings in which 2 is invertible. Suppose $f(x) \in B[x]$ is a monic polynomial of even degree $2n$, such that the coefficients of x^i for all $i \geq n$ lie in the subring A. Then there exist unique polynomials $g(x) \in A[x]$ and $h(x) \in B[x]$, both of degree $\leq n-1$, such that*

$$f(x) = (x^n + g(x))^2 + h(x).$$

Proof. Let us write

$$f(x) = x^{2n} + \sum_{i=1}^{n} a_i x^{2n-i} + \sum_{i=0}^{n-1} b_{2n-i} x^i.$$

Divide by x^{2n}, and set $T := 1/x$. Then we are trying to write

$$1 + \sum_{i=1}^{n} a_i T^i + \sum_{i=n+1}^{2n} b_i T^i = (1 + G(T))^2 + H(T),$$

with $G(T) \in T\mathbb{C}[T]$ of degree $\leq n$, and with $H(T) \in T^{n+1}\mathbb{C}[T]$ of degree $\leq 2n$. Looking mod T^{n+1}, we see that $1 + G(T)$ is the mod T^{n+1} truncation of the unique square root of $1 + \sum_{i=1}^{n} a_i T^i$ with constant term one. As the a_i lie in A, the square root lies in $1 + TA[[T]]$, and hence $G(T)$ lies in $TA[T]$.

The polynomial $H(T)$ is simply the error. This gives existence. For uniqueness, suppose $f(x) = (x^n + g(x))^2 + h(x) = (x^n + g_1(x))^2 + h_1(x)$. Then

$$h_1(x) - h(x) = (x^n + g(x))^2 - (x^n + g_1(x))^2 =$$

$$= ((x^n + g(x)) - (x^n + g_1(x)))((x^n + g(x)) + (x^n + g_1(x))).$$

The second product has degree $2n$, while $h_1(x) - h(x)$ has degree $\leq n-1$. So the first product must vanish, so $g = g_1$ and $h = h_1$. □

The upshot of this discussion is that in the four example curves $y^2 = 4x^\ell + \ell$, for $\ell = 5, 13, 29, 53$,we have a point $P := (-1, n)$, n such that $\ell = 4 + n^2$, such that $P - \infty$ generates a Zariski dense subgroup of the Jacobian.

10. Big monodromy examples

According to a marvelous theorem of Zarhin, if $f(x) \in \mathbb{Q}[x]$ is a polynomial of degree $n \geq 5$ whose Galois group is either A_n or S_n, the Jacobian of the hyperelliptic curve $y^2 = f(x)$, whose genus g is $(n-1)/2$ for n odd and is $(n-2)/2$ for n even, has monodromy "as big as possible", in the sense that for every prime ℓ, the image of the Galois representation on its ℓ-adic Tate module V_ℓ is open in the group $Gsp(2g)$ of symplectic similitudes. In particular, the Galois representation remains irreducible when restricted to any open subgroup of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, and hence the Jacobian, even over $\mathbb{C}$, is simple.

Here are some ad hoc examples. For odd $n \geq 5$, we take for X the curve $y^2 - y = x^n - 2x$, with its section at ∞ tacked on, viewed as a scheme over $\mathbb{Z}$. It is proper over $\mathbb{Z}$, with geometrically reduced and irreducible fibres (because n is odd). It visibly has good reduction at $p = 2$. Over $\mathbb{Z}[1/2]$, we complete the square to get the equation $y^2 = x^n - 2x + 1/4$. Because n is odd, the geometric fibres of $X/\mathbb{Z}$ are all geometrically reduced and irreducible. According to Magma, the polynomial $x^n - 2x + 1/4$ has galois group S_n for each odd $n \leq 111$. According to Mathematica, for each odd $n \leq 35$, the discriminant of $4x^n - 8x + 1$ has its odd part square free.

Lemma 10.1. *For n odd, $5 \leq n \leq 35$, the scheme X is regular.*

Proof. We have already remarked that $X/\mathbb{Z}$ is lisse over $p = 2$, and hence over $\mathbb{Z}[1/N]$ for some odd N, which we may take to be the odd part of the discriminant of $4x^n - 8x + 1$. The regularity now results from the following lemma, which is surely well known.

Lemma 10.2. *Let p be an odd prime, k a perfect field of characteristic p, $W = W(k)$ the Witt vectors, and $f(x) \in W[x]$ a monic polynomial whose discriminant Δ has $ord_p(\Delta) = 1$. For any integer $d \geq 2$ prime to p, in particular for $d = 2$, the W-scheme $y^d = f(x)$ is regular.*

Proof. Regularity is invariant under completion and under finite etale base change, so we may enlarge the field k and reduce to the case when $\overline{f(x)} \in k[x]$ factors completely. Our scheme is lisse over $W[1/p]$, so what we must show is that the complete local ring at any singular point of the special fibre is regular. A singular point of the special fibre is a point $(x = a, y = 0)$ with $a \in k$ a multiple zero of $\overline{f(x)}$. Making an additive translation, we may assume $a = 0$ is a multiple root of $\overline{f(x)}$. Factor $\overline{f(x)}$ as $x^r \overline{h(x)}$ with $\overline{h(0)} \neq 0$ in k, and $r \geq 2$. By Hensel's Lemma, we may lift this to a factorization of $f(x)$ as $h(x)g(x)$ with g and h monic, $g(0) \in W^\times$, and $h(x) = x^r + \sum_{i=1}^r pa_i x^{r-i}$. The discriminant $\Delta(f)$ is then, up to sign, the product $\Delta(g)\Delta(h)g((h))^2$. Since g and h are relatively prime, the term $g((h))$ is a unit. As $\Delta(f)$ has $ord_p = 1$, while $\Delta(h)$ has $ord_p \geq 1$, it follows that $\Delta(g)$ is a unit, and $ord_p(\Delta(h)) = 1$. The discriminant of $h(x) = x^r + \sum_{i=1}^r pa_i x^{r-i}$ is a $\mathbb{Z}$-polynomial in the quantities $pa_i, i = 1, ..., r$ which is isobaric of weight $r(r-1)$ with pa_i having weight i. If $r \geq 3$, $\Delta(h)$ has $ord_p \geq 2$. Thus $r = 2$, $h(x) = x^2 + pa_1 x + pa_2$, and $\Delta(h) = p^2 a_1^2 - 4pa_2$, which has $ord_p = 1$ precisely when a_2 is a unit. Thus the

constant term of $h(x)$ has $ord_p = 1$. Because $g(0)$ is a unit, the constant term of $f(x)$ has $ord_p = 1$. So the equation has the form $-y^n + (\text{elt. in } (x)) + p(\text{elt. in } W^\times)$. So the complete local ring at this singular point is $W[[x,y]]/(\text{eqn.})$, in which x, y generate the maximal ideal. □

□

Lemma 10.3. *For n odd, $3 \leq n \leq 35$, the Jacobian J of the curve $y^2 - y = x^n - 2x$ has $J(\mathbb{Q})$ torsion free.*

Proof. Over $\mathbb{Z}[1/2]$, we may write this curve as $y^2 = 4x^n - 8x + 1$. It (with its ∞ section tacked on) is smooth over $\mathbb{Z}[1/2\Delta]$ for Δ the discriminant of $4x^n - 8x + 1$. For each odd prime p not dividing Δ, the reduction mod p map from $J(\mathbb{Q})_{tors} = J(\mathbb{Z}[1/2\Delta])_{tors}$ to $J(\mathbb{F}_p)$ is injective. On the other hand, the polynomial $4x^n - 8x + 1$ is $\mathbb{Q}$-irreducible, so $J(\mathbb{Q})_{tors}$ has odd order. So it suffices to exhibit, for each n in our range, a short list of good primes p_i such that the gcd of the $\#J(\mathbb{F}_{p_i})$ is a power of 2. We computed $\#J(\mathbb{F}_p)$ in Magma using the command

$$\mathrm{P} < \mathrm{x} >:= \mathrm{PolynomialRing}(GF(p)); f := 4*x^n - 8*x + 1; \mathrm{J} := \mathrm{Jacobian}(\mathrm{HyperellipticCurve}(f)); \#J;$$

for various values of p and n. Here is such a list:

$$n = 3, use\ 3, 7.$$
$$n = 5, use\ 5, 7.$$
$$n = 7, use\ 3, 7.$$
$$n = 9, use\ 3, 5$$
$$n = 11, use\ 5, 7.$$
$$n = 13, use\ 3, 5.$$
$$n = 15, use\ 3, 5.$$
$$n = 17, use\ 7, 17.$$
$$n = 19, use\ 3, 5.$$
$$n = 21, use\ 3, 19.$$
$$n = 23, use\ 7, 37.$$
$$n = 25, use\ 3, 5.$$
$$n = 27, use\ 3, 7.$$
$$n = 29, use\ 5, 7.$$
$$n = 31, use\ 3, 5.$$
$$n = 33, use\ 3, 5.$$
$$n = 35, use\ 5, 11.$$

□

The upshot of this discussion, is that for n odd, $5 \leq n \leq 35$, the divisor class $(0,1) - \infty$ on the Jacobian of $y^2 = 4x^n - 8x + 1$ generates a Zariski dense subgroup, and we have the explicit model $H^1(X, \mathcal{O}_X)$ for the Lie algebra of its Neron model, X now $y^2 - y = x^n - 2x$ with its ∞ section as scheme over $\mathbb{Z}$.

11. other Jacobians with big monodromy

By a theorem of Osada [Osada], apparently discovered earlier by Nart and Vila [Na-Vi], the polynomial $x^n - x - 1$ has Galois group S_n for all $n \geq 2$. Moreover, its discriminant is squarefree for $n \leq 51$ (though not for all n; for example, $n = 130$ has its discriminant divisible by 83^2, and each of $n = 257, 487, 528$ has its discriminant divisible by 59^2). With a bit of attention to the prime 2, one finds

Lemma 11.1. *Suppose $n \geq 3$ is odd and the discriminant of $x^n - x - 1$ is squarefree. Then the curve $y^2 = x^n - x - 1$, with its section at ∞ tacked on, as a scheme over $\mathbb{Z}$ is regular.*

Unfortunately, this curve does not have a visible rational point P other than ∞. If we consider instead the curve $y^2 = 1 + x - x^n$, its quadratic twist by -1, then we have six visible rational points ($x = 0, 1, -1,\ y = \pm 1$) other than ∞, but we lose regularity over $\mathbb{Z}_2$. The Jacobian of both the original curve and of its quadratic twist curve has $J(\mathbb{Q})$ torsion free for all n in the range $3 \leq n \leq 72$ (again using Magma and computing a gcd).

It is however **not** a general phenomenon that for a hyperelliptic curve of the form $y^2 = f(x)$ with $f(x) \in \mathbb{Q}[x]$ a polynomial of degree $n \geq 5$ whose galois group is A_n or S_n, its $J(\mathbb{Q})$ is torsion free. Here are some examples. We begin by explaining the idea. Fix an odd integer $n \geq 5$.Take a polynomial $A(x) \in \mathbb{Q}[x]$ of degree $< n/2$, and consider the polynomial $f_{n,A}(x) = x^n + A(x)^2$. If $f_{n,A}$ is squarefree, we have a hyperelliptic curve $y^2 = f_{n,A}(x)$. On this curve, call it $C_{n,A}$, functions holomorphic except at ∞ can be written uniquely as $g(x) + yh(x)$, with $g(x), h(x) \in \mathbb{Q}[x]$. Here x has a double pole at ∞, and y has a pole of odd order n at ∞. If such a function $g(x) + yh(x)$ has an odd order pole at ∞, then its order of pole is $n + 2\deg(h) \geq n$.

Now consider the point $P := (x = 0, y = A(0))$ on $C_{n,A}$. The function $A(x) - y$ is easily seen to have divisor $n([P] - [\infty])$, simply because $(A(x) - y)(A(x) + y) = A(x)^2 - f_{n,A}(x) = -x^n$. Thus $[P] - [\infty]$ is a nontrivial $\mathbb{Q}$-point on the Jacobian $J_{n,A}$, of order dividing n. Its order cannot be any proper divisor of n, by the previous paragraph (which indeed shows that any nontrivial $\mathbb{C}$-point of odd order in the Jacobian $J_{n,A}$ of the form $[Q] - [\infty]$ with $Q \in C_{n,A}(\mathbb{C})$ must have order $\geq n$).

It remains only to write down examples of $A(x)$ for which $f_{n,A}(x) = x^n + A(x)^2$ has galois group S_n. We tried $A(x) = x + 1$. According to Magma, with this choice of A, $f_{n,A}(x) = x^n + (x+1)^2$ has galois group S_n for each odd n in the range $5 \leq n \leq 29$.

Remark 11.2. Our reluctance to use the curve $y^2 = 1 + x - x^n$, with its visible points is only because we do not know an explicit description of the Lie algebra of its Neron model over $\mathbb{Z}$. Other families of candidates which are disqualified by this ignorance of an explicit model are the Schur families

$$y^2 = n!(\sum_{i=0}^{n}(x^i/i!),$$

and the Osada families

$$y^2 = x^n - x - 1$$

but now with n **even**. Schur proved that the truncated exponential polynomials have galois group A_n if $4|n$, and S_n otherwise, cf. [Coleman] for a beautiful exposition. Because n is even, there are two "points at infinity", and their difference,

$\infty_+ - \infty_-$, is a candidate divisor class to generate a Zariski dense subgroup of the Jacobian. Again, numerical experiments show that these Jacobians, for low values of n, have no nontrivial rational torsion.

12. A variant lattice for *Lie* of Jacobians

Suppose we are given $X/\mathbb{Z}$ which is proper, with fibres of dimension one, and which over $\mathbb{Z}[1/N]$ is smooth, with geometrically connected fibres of genus $g \geq 1$. So over $\mathbb{Z}[1/N]$, *Lie* of the Neron model of the Jacobian, i.e. of $Pic^0_{X_{\mathbb{Z}[1/N]}/\mathbb{Z}[1/N]}$, is $H^1(X, \mathcal{O}_X) \otimes_{\mathbb{Z}} \mathbb{Z}[1/N]$. We may not know *Lie* of the Neron model; e.g., X may not be regular with geometrically reduced and irreducible fibres. One way around this ignorance is to use $H^1(X, \mathcal{O}_X)/(\text{torsion})$ as $\mathbb{L}ie$ to formulate a variant Wieferich conjecture for Jacobians. As we write this, the biggest obstacle to carrying out any sort of computer experiment is the computational difficulty of dealing with Jacobians when $g \geq 2$. The question of which lattice to use for $\mathbb{L}ie$ seems minor compared to this.

13. The case of semiabelian varieties

A semiabelian variety is an extension of an abelian variety by a torus. One knows [Bo-Lu-Ra] that given $B/\mathbb{Z}[1/N]$ a semiabelian variety, it has a Neron model $\mathcal{B}/\mathbb{Z}$.

Conjecture 13.1. (Wieferich Conjecture for semiabelian varieties) *Suppose given $P \in \mathcal{B}(\mathbb{Z}[1/N]) = B(\mathbb{Q})$ which generates a Zariski dense subgroup of $B_{\mathbb{Q}}$. Then the situation $(B/\mathbb{Z}[1/N], P \in \mathcal{B}(\mathbb{Z}[1/N]), Lie(\mathcal{B}/\mathbb{Z}))$ has Wieferich equidistribution.*

The case when B is the product of an abelian variety A with a torus T is as amenable (or not amenable) to testing as are the separate cases of A and of T; the first problematic, the second straightforward.

But already in the case of a nontrivial extension of an abelian variety by $\mathbb{G}_m$, it is not clear how to proceed. Recall [Se-GACC, VII, &16] that such an extension, a nonzero element of $H^1(A, \mathbb{G}_m) = Pic(A)$ which is primitive, is precisely an element of $Pic^0(A)$. More explicitly, given an invertible sheaf $\mathcal{L}$ on A which lies in $Pic^0(A)$, one considers the "theta group" $\Theta(\mathcal{L})$, whose S-valued points are the pairs (ϕ, R) with $R \in A(S)$ and ϕ an isomorphism of line bundles on A_S from $\mathcal{L}$ to its translate by R. This theta group is the corresponding extension of A by $\mathbb{G}_m$. But from this general perspective, it is hard to see how to test conjectures.

Here is another way to obtain extensions of a Jacobian by $\mathbb{G}_m$. Start with a curve $C/\mathbb{Q}$ of genus $g \geq 1$, and two distinct points P and Q in $C(\mathbb{Q})$. Consider the generalized Jacobian J_m with modulus $m = P + Q$, classifying line bundles $\mathcal{L}$ of degree zero on C together with trivializations at **both** P and Q. The obvious map $J_m \to J$, "forget the trivializations", makes J_m an extension of J by $\mathbb{G}_m$. A key fact is that this extension is nontrivial, cf. [Ro, Thm. 13]. Its extension class is a point in $Pic^0(J)$. Which point is it? For a base point $0 \in C(\mathbb{Q})$, and $\phi : C \to J$ the embedding $R \mapsto [R] - [0]$, the pullback map on line bundles gives an isomorphism $Pic^0(J) \cong Pic^0(C)$, cf. [La-AV, VI, &3, Thm.3]. [The isomorphism does not depend on the choice of base point $0 \in C(\mathbb{Q})$.] Thus the extension class of J_m gives, under $\phi^\star$, an element of $Pic^0(C)$. This element is, up to sign, the class of the invertible sheaf $I(P) \otimes I^{-1}(Q)$ on C, cf. [Se-MU, &1, Thm. 1 and Exemple] or [Ram, part (ii) of Prop., page 9]. The "up to sign" proviso comes from fact that

"the" $\mathbb{G}_m$ in the extension is intrinsically the quotient $(\mathbb{G}_m \times \mathbb{G}_m)/(\text{diagonal } \mathbb{G}_m)$, which has two isomorphisms to $\mathbb{G}_m$.

Let us denote by $L \in J(\mathbb{Q})$ the class of the invertible sheaf $I(P) \otimes I^{-1}(Q)$ on C. Choose any element L_m in J_m which maps to L, i.e., choose trivializations at both P and Q of $I(P) \otimes I^{-1}(Q)$. We claim that if $L \in J(\mathbb{Q})$ generates a Zariski dense subgroup of J, then L_m generates a Zariski dense subgroup of J_m. To see this, consider the Zariski closure Z of the subgroup of J_m generated by L_m. Its identity component Z^0 maps onto J. So the dimension of Z^0 is either $g+1$ or g. In the former case, Z^0 must be J_m, and so Z is J_m. In the latter case, we get a contradiction as follows. Z^0 is itself a g-dimensional connected group scheme which maps onto J, so Z^0 is an abelian variety inside J_m and its projection onto J is an isogeny, call it π. The pullback by π of the extension becomes trivial. There is a map ρ of J to Z^0 such that $\pi\rho$ is multiplication by some integer $d \geq 1$. So the extension class of J_m in $Ext^1(J, \mathbb{G}_m)$ is killed by d. But the extension class is the class of L in J, which is not of finite order (because L generates a Zariski dense subgroup of J).

Again in this J_m case, there is a brutal way to construct a $\mathbb{Z}$-form of $Lie(J_m)$. Suppose that our curve is the generic fibre of a proper smooth $C/\mathbb{Z}[1/N]$, and that the two points P and Q, which by properness extend to sections over $\mathbb{Z}[1/N]$, are disjoint. Then J_m is a smooth group scheme over $\mathbb{Z}[1/N]$, whose Lie algebra $Lie(J_m/\mathbb{Z}[1/N])$ is $H^1(C, I(P) \otimes I(Q))$. For any proper $\mathcal{X}/\mathbb{Z}$ extending $C/\mathbb{Z}[1/N]$, and any coherent sheaf $\mathcal{F}$ on $\mathcal{X}$ extending $I(P) \otimes I(Q))$, we can take $H^1(\mathcal{X}, \mathcal{F})/(\text{torsion})$ as a $\mathbb{Z}$-form of Lie. The arguably simplest choice of such an $\mathcal{F}$ on a given $\mathcal{X}$ is $I(P) \otimes I(Q)$. Much remains to be done.

References

[Ba-Ho] Bateman, P., and Horn, R., A heuristic asymptotic formula concerning the distribution of prime numbers,Math. Comp. 17, no. 84 (1963), 445-447.

[Bo-Lu-Ra] Bosch, S., Lütkebohmert, W., and Raynaud, M., Néron models. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 21. Springer-Verlag, Berlin, 1990. x+325 pp.

[Coleman] Coleman, R., On the Galois groups of the exponential Taylor polynomials. Enseign. Math. (2) 33 (1987), no. 3-4, 183-189.

[Cr-Di-Po] Crandall, R., Dilcher, K., and Pomerance, C., A search for Wieferich and Wilson primes. Math. Comp. 66 (1997), no. 217, 433-449.

[Do-Kl] Dorais, F. G., and Klyve, D., A Wieferich prime search up to 6.7?1015. J. Integer Seq. 14 (2011), no. 9, Article 11.9.2, 14 pp., available at http://www.cs.uwaterloo.ca/journals/JIS/VOL14/Klyve/klyve3.html.

[Gr-Mo] Granville, A., and Monagan, M. B., The first case of Fermat's last theorem is true for all prime exponents up to 714,591,416,091,389. Trans. Amer. Math. Soc. 306 (1988), no. 1, 329-359.

[Ha-Wr] Hardy, G.H., and Littlewood, J.E., Some Problems of 'Partitio Numerorum'; III:On the expression of a number as a sum of primes. Acta Math. 44 (1923), 1-70.

[Ito] Ito, K., Introduction to probability theory. Cambridge University Press, Cambridge, 1984. x+213 pp.

[Ka-Gal] Katz, N., Galois properties of torsion points on abelian varieties. Invent. Math. 62 (1981), no. 3, 481-502.

[Ka-LTR] Katz, N., Lang-Trotter revisited. Bull. Amer. Math. Soc. (N.S.) 46 (2009), no. 3, 413-457.

[La-AV] Lang, S., Abelian Varieties, Springer Science+Business Media, New York, 1983, x+256pp.

[L-T] Lang, S., and Trotter, H., Frobenius distributions in GL2-extensions, Springer Lecture Notes in Mathematics 504, 1976.

[Na-Vi] Nart, E. and Vila, N. Equations of the type $X^n + aX + b$ with absolute Galois group S_n. Proceedings of the sixth conference of Portuguese and Spanish mathematicians, Part II (Santander, 1979). Rev. Univ. Santander No. 2, part 2 (1979), 821-825.

[Osada] Osada, H., The Galois groups of the polynomials $X^n + aX^\ell + b$. J. Number Th. 25 (1987), 230-238.

[Ram] Ramachandran, N., From Jacobians to one-motives: exposition of a conjecture of Deligne. The arithmetic and geometry of algebraic cycles (Banff, AB, 1998), 215-234, CRM Proc. Lecture Notes, 24, Amer. Math. Soc., Providence, RI, 2000.

[Rib] Ribet, K., Galois action on division points of Abelian varieties with real multiplications. Amer. J. Math. 98 (1976), no. 3, 751-804

[Ro] Rosenlicht, M., Generalized Jacobian Varieties. Ann. Math., Second Series 59 (1954), no. 3, 505-530.

[Shim-Tan] Shimura, G., and Taniyama, Y., Complex multiplication of abelian varieties and its applications to number theory. Publications of the Mathematical Society of Japan, 6, Tokyo, 1961. xi+159 pp.

[Se-GACC] Serre, J.-P., Groupes algébriques et corps de classes. Publications de l'institut de mathématique de l'université de Nancago, VII. Hermann, Paris, 1959. 202 pp.

[Se-MU] Serre, J.-P., Morphismes universels et différentielles de troisième espèce, Séminaire Claude Chevalley, tome 4(1958-59), exp. n° 11, 1-8.

[Sh] Shioda, T., Constructing Curves with High Rank via Symmetry. Amer. J. Math 120, no. 3, 551-566.

[Si] Silverman, J., Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994. xiv+525 pp.

[Son] Sondow, J.,Lerch Quotients, Lerch Primes, Fermat-Wilson Quotients, and the Wieferich-non-Wilson Primes 2, 3, 14771. http://arxiv.org/pdf/1110.3113.pdf

[Weil] Weil, A., Number theory. An approach through history. From Hammurapi to Legendre. Birkhäuser Boston, Inc., Boston, MA, 1984. xxi+375 pp.

[Zarhin] Zarhin, Yuri G., Very simple 2-adic representations and hyperelliptic Jacobians, Mosc.Math. J. 2 (2002), no. 2, 403-431.

Princeton University, Mathematics, Fine Hall, NJ 08544-1000, USA
E-mail address: nmk@math.princeton.edu