REMARKS AND ERRATA

1. Errors that have not been fixed

Genus-two curves with 22 torsion points.

- The displayed definition of the function f is not the right one for its intended purpose. To test whether the point (u, v) is torsion, one needs to express the vector of integrals along γ_u as a linear combination of both the vector of integrals along $X_t(\mathbb{R})$ and the vector of integrals along an 1-cycle representing an independent complex-conjugation-invariant class in $H_1(X(\mathbb{C}), \mathbb{Q})$, and to define $f(t, u)$ as that pair of coefficients. Probably this new f still has a 2-dimensional image, but this has not yet been checked, so the proof as it stands is incomplete.

2. Significant errors that were fixed

The classification of preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture.

- The proof of Proposition 1 in Section 4 contains an error: the point $(2, \sqrt{33})$ is not on $\mathcal{C}$! Instead $(-2, \sqrt{33})$ is; apparently a sign got dropped halfway through the computation. To complete the 2-descent correctly one must use also the 2-adic information. The end result of the computation is the same as before, so the main results of the paper still hold. (Thanks to Ken Kramer for noticing the error.)
- There is typo in the third displayed equation on page 22: the first line should read
$$(\mu, t) \mapsto \left(\frac{t + \mu^2 + 3}{2(\mu - 1)^2}, -\frac{3\mu^3 + \mu t + t - 5\mu^2 + 9\mu + 1}{2(\mu - 1)^3} \right),$$
which includes a missing $+t$ in the numerator of the y-coordinate. (Thanks to John Doyle for noticing this.)

The conjugate dimension of algebraic numbers.

- The data in Table 2 was mostly taken from a table in the cited article by Feit. We had corrected the first row of that table, but Gaël Rémond pointed out to us that Feit's table has at least one other omission: for $(n, \ell) = (6, 4)$, the order of $\mathrm{ST}_8 \wr S_3$ is 5308416, which is $9/5$ times the general formula $\ell^n n! = 2949120$. Thus $(6, 4)$ should be added to the list of exceptions in our Theorem 15. This is now corrected in the online version, but not in the printed version.

The moduli space of commutative algebras of finite rank.

- The proof of Lemma 11.1 relies on an invalid argument from [KP70], so the proofs of the upper bounds in Theorem 11.2 and 11.3 are not complete. The theorems are nevertheless true: they are proved (with improved error terms) in [BM21]. (Thanks to Simon R. Blackburn and K. Robin McLean for pointing out the error.)

Date: August 10, 2021.

Isomorphism types of commutative algebras of finite rank over an algebraically closed field.

- In Case 4b in characteristic 2, the printed version is missing one of the two isomorphism types.
- Marco Pellegrini and Chiara Tamburini pointed out some redundant entries in Table 1 of the printed version; these arose from an incorrect classification of symmetric bilinear forms in characteristic 2.

All these have been corrected in the online version.

Bertini irreducibility theorems over finite fields.

- Jiayu Zhao pointed out a minor error in one proof in the printed version. It has been corrected in the online version. The issue was that in the proof of Lemma 5.1 we were implicitly using Lemma 3.6 of the online version without first reducing to the case of a normal variety. So we added Lemma 3.6, and rewrote the proof of Lemma 5.1 to work with the smooth loci (and we also modified Lemma 5.2 slightly).

3. Typos and minor misstatements

Union-closed families.

- p. 256, Theorem 1, in condition 2: Change $\mathcal{F} \uplus \mathcal{G} = \mathcal{G}$ to $\mathcal{F} \uplus \mathcal{G} \subseteq \mathcal{G}$. A similar change should be made to the beginning of lines -5 and -3 on p. 257, and to the beginning of line 6 on p. 260. (Thanks to Theresa Vaughan.)

Computational aspects of curves of genus ≥ 2.

- In the printed version, "positive integer g" should be changed to "$g \geq 2$" in the statement of the Shafarevich conjecture in Section 11. The statement "For each number field K and set of places S, there are at most finitely many genus 1 curves over K with good reduction outside S" implies that the Shafarevich–Tate group of every elliptic curve over a number field is finite. The latter is not yet proved.

The number of intersection points made by the diagonals of a regular polygon.

- The published version contains a typo introduced while converting a formula to TEX: in Theorem 1, the 232 in the formula for $I(n)$ should be 262, as the routines in ngon.m give. (Thanks to Steve Sommars for noticing this.)

The Cassels–Tate pairing on polarized abelian varieties.

- In the printed version, Section 2 suggests that the maximal divisible subgroup M_{div} of an abelian group M equals the set of $m \in M$ such that for all $n \geq 1$ there exists $x \in M$ such that $nx = m$. This is false in general (the latter set can be larger), but it is true if the p-torsion subgroup $M[p]$ is finite for each prime p. The latter condition holds for each group in the paper for which the notation M_{div} is used, so the rest of the paper is unaffected. (Thanks to Hendrik Lenstra for noticing the error.)

Mordell-Lang plus Bogomolov.

- In the printed version, Remark 1 following Proposition 5 should be replaced by the following, because heights associated to effective divisors are not guaranteed to be bounded below for points on the divisor itself. (Thanks to Najmuddin Fakhruddin for noticing this.)

  "Condition $(*)$ is satisfied for (U, f) if there exists an integral projective variety V containing U as an open dense subset, and an ample line bundle $\mathscr{L}$ on V such that f extends to a morphism $\bar{f}\colon V \to V$ and a height associated to $\mathscr{N} := \bar{f}^*\mathscr{L} \otimes \mathscr{L}^{\otimes -q}$ in $(\operatorname{Pic} V) \otimes \mathbb{Q}$ is bounded below for some $1 < q \in \mathbb{Q}$. The condition on $\mathscr{N}$ is satisfied, for instance, if $\mathscr{N}$ is the pullback of an ample sheaf under some morphism of varieties."

  In the application to semiabelian varieties, one can then take $\bar{f} = [m]$ for some $m \geq 2$, $q = m$, and $\mathscr{N} = \mathscr{L}_1^{\otimes(m^2-m)}$. The results of the paper still hold.

Algebraic families of nonzero elements of Shafarevich-Tate groups.

- Section 2.6 implicitly assumes that A is principally polarized, which is the case in the application. If A is a general abelian variety, Y should be a torsor of $\hat{A}$, and it is $\hat{A}$ that should be identified with $\mathbf{Pic}^0_{X/k}$. (Thanks to my co-author for noticing this.)

Squarefree values of multivariable polynomials. The following changes should be made to the printed version:

- In Theorem 3.2 and Lemma 6.2 the condition "x_n appears in $f(x)$" should be strengthened to "x_n appears in each irreducible factor of $f(x)$".
- The statement of Theorem 8.1 is OK, but some changes are needed in the proof, since one cannot ensure that t will be among the t_{i_α} at the end. One should remark that in the generalization of Lemma 7.2 it suffices to have $t_i/t_j \notin K^p$ for some i, j, and then only allow subsets $\{i_{\alpha_1}, \ldots, i_{\alpha_r}\}$ for which the corresponding t_{i_α} satisfy this condition on ratios: this can be done provided $\deg D$ is sufficiently large.

The William Lowell Putnam Mathematical Competition 1986–2000: problems, solutions, and commentary.

- The "Related question" on page 68 is wrong. Condition (b) should be replaced by the hypothesis that all rows and columns of M have the same sum.

Orbits of automorphism groups of fields. In the printed version:

- In the proof of Lemma 1.6, the statement $M_d = cM_d$ holds but does not follow from the previous lines of the proof. It was used in the last sentence to show that multiplication-by-c maps M_d isomorphically to cM. Luckily, the latter also follows from $M_d = cM$ and $cM = c^2M$ and the fact that cM is torsion-free. (Thanks to E. Mehmet Kiral for noticing the gap.)
- The first paragraph of the proof of Lemma 2.8 should read as follows:

  > Since $M - N$ generates M as a module, the sequence $(f^m M)_{m \geq 1}$ also contains only finitely many sets. But this sequence is decreasing, so $f^m M = f^{m+1} M$ for some m.

  Thanks to P. K. Sharma for noticing the error.

Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$.

- In the printed version, in the proof of Lemma 4.6, “twist by 1/3” should be “twist by $-1/3$”.

Unramified covers of Galois covers of low genus curves.

- In Remark 1.2 of the printed version, it should be assumed that Y has genus at least 2. (Thanks to Amador Martin-Pizarro for noticing this.)

Smooth hypersurface sections containing a given subscheme over a finite field.

- The variable b should be c in a few places in the printed version: in “For $d \geq b$” in the proof of Lemma 2.1, and in the statement and proof of Lemma 3.2.

The set of nonsquares in a number field is diophantine.

- In the printed version, the equation at the end of the proof of Corollary 1.2 should be $A_{n+1} = A_1 \cup \{t^2 : t \in A_n \text{ and } -t \in A_n\}$. (Thanks to Jean-Louis Colliot-Thélène for noticing this.)

Random maximal isotropic subspaces and Selmer groups.

- In the printed version, in the proof of Proposition 2.6(a), “codimension 1 subspaces of W” should be “codimension 1 subspaces of W not containing v”. The same extra condition should be imposed on W_1.
- The observation that a Selmer group could be an intersection of maximal isotropic subspaces in a finite dimensional space (Remark 4.15) appeared earlier in a more limited context, but with a similar proof. Namely, for elliptic curves E over a number field k with $E[2] \subset E(k)$, the 2-Selmer group $\operatorname{Sel}_2 E$ was shown to be an intersection of two subspaces of a finite-dimensional $\mathbb{F}_2$-vector space that were maximal isotropic with respect to a symmetric bilinear pairing (slightly weaker than being maximal isotropic with respect to a quadratic form): in [CTSSD98], see Proposition 1.2.1 in conjunction with Proposition 1.1.1 and the remark following it.
- Warning: The references to “PR11” are to the arXiv version `http://arxiv.org/pdf/1104.2105v1.pdf`, not to the published version [PR11].

Average rank of elliptic curves. The following corrections should be made in the printed version:

- The construction in [BS15, second half of §4.1] of a positive-density family of elliptic curves in which the root number is equidistributed is actually taken from [Won01, p. 25 and §9], so the latter should have been credited.
- In the first paragraph of §4.2, $\mathcal{S}(\mathbb{Q}_p)^{\min}$ should be $\mathcal{S}(\mathbb{Z}_p)^{\min}$. (Thanks to Ruthi Hortsch for noticing this.)
- In Lemma 4.3, it is necessary to add the hypothesis that f is locally solvable. (Thanks to Jack Thorne for noticing this.)

Characterizing integers among rational numbers with a universal-existential formula.

- In the printed version, the third sentence of the second paragraph of the proof of Lemma 2.3 should say “Then $U_q = \{2x : x \in \mathbb{F}_q, y \in \mathbb{F}_q^\times, \text{and } x^2 - cy^2 = 1\}$.”

- In the last sentence of the same paragraph, although $\overline{X}$ has arithmetic genus 1, it may be singular, so "genus 1" should say "genus ≤ 1". In any case, X is $X' - S$ for some smooth projective curve X' of genus ≤ 1 and finite subscheme S having ≤ 12 geometric points, so the proof still goes through.

(Thanks to Dion Leijnse for pointing out the errors.)

The moduli space of commutative algebras of finite rank.

- In the printed version, in Remark 6.9, S_{n-1} should be replaced by gS_ng^{-1}, where g is an element of $\mathrm{GL}_n(\mathbb{Z})$ that maps $\tilde{\mathcal{A}}_{\mathrm{split}}$ to a based algebra consisting of $\mathcal{A}_{\mathrm{split}}$ with a basis whose first element is 1. (Thanks to Andrew O'Desky for the correction.)

4. Remarks

Maximally complete fields.

- Irving Kaplansky told me that the residue field part of his "Hypothesis A," namely the condition that every polynomial of the form

$$a_0x^{p^n} + a_1x^{p^{n-1}} + \cdots + a_{n-1}x^p + a_nx + a_{n+1}$$

  with each a_i in the residue field k have a root in k, was shown by Whaples to be equivalent to the condition that k have no extensions of degree divisible by p. See the "Afterthought" to "Maximal Fields with Valuations" in [Kap95].
- Laurent Moret-Bailly points out that the argument in Section 4 can be used to construct a p-adic Mal'cev–Neumann field even if R is not perfect, because there is still a Cohen ring (complete discrete valuation ring with the prime number p as uniformizer) with residue field R.

The Cassels–Tate pairing on polarized abelian varieties.

- Let X be a smooth projective geometrically integral surface over a finite field of characteristic p, and let ℓ be a prime not equal to p. The question of Tate in Section 11, whether a certain antisymmetric pairing on $\mathrm{Br}(X)_{\mathrm{nd}}(\ell)$ is always alternating, is now known to have a positive answer, thanks to Tony Feng [Fen20]. This implies the earlier theorem of [LLR05] that $\mathrm{Br}(X)$ is of square order if it is finite, or even if $\mathrm{Br}(X)(\ell)$ is finite for any prime ℓ.

Undecidability in number theory.

- The 2008 article mentioned that finding a solution in integers to $x^3 + y^3 + z^3 = 33$ is an unsolved problem. Eleven years later, in March 2019, Andrew Booker found the solution

$$(8866128975287528)^3 + (-8778405442862239)^3 + (-2736111468807040)^3 = 33.$$

  As of December 5, 2020, the smallest positive integer for which it is not known whether it is a sum of three cubes is 114.

Néron–Severi groups under specialization.

- Here is a more detailed explanation of why the homomorphism $\operatorname{Pic} X \to \operatorname{Pic} X_K$ in (3.4) is an isomorphism. (This came out of a discussion with Kęstutis Česnavičius.)

  First, X is smooth over a regular local ring R, so X and X_K are regular. This means that $\operatorname{Pic} X$ and $\operatorname{Pic} X_K$ can be understood as Weil divisor class groups.

  Let $X \to Y \to \operatorname{Spec} R$ be the Stein factorization of $X \to \operatorname{Spec} R$. Then Y is finite over $\operatorname{Spec} R$, and Y is the normalization of $\operatorname{Spec} R$ in X [SP, Tag 03H0], so Y is a semilocal Dedekind scheme.

  Since $X \to \operatorname{Spec} R$ is smooth, the special fiber X_k is a disjoint union of irreducible divisors D of X. Any such D maps to some point y of Y lying above the closed point of $\operatorname{Spec} R$. Since Y is a semilocal Dedekind ring, y is a principal divisor on Y. Let F be the fiber of $X \to Y$ above y, so F is a principal divisor on X. Now F is contained in X_k, and F is connected (by definition of Stein factorization), and F contains a connected component D of X_k (even scheme-theoretically, since X_k is reduced), so $F = D$. Thus D is principal. The kernel of $\operatorname{Pic} X \to \operatorname{Pic} X_K$ is spanned by the classes of such divisors D, so $\operatorname{Pic} X \to \operatorname{Pic} X_K$ is injective.

  It is also surjective, since if E is an irreducible divisor on X_K, its Zariski closure in X is an irreducible divisor of X whose class maps to the class of E.

Modeling the distribution of ranks, Selmer groups, and Shafarevich–Tate groups of elliptic curves.

- Corollary 1.2 of [GGGR19] proves our Conjecture 6.9.

References

[BS15] Manjul Bhargava and Arul Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2) **181** (2015), no. 2, 587–621, DOI 10.4007/annals.2015.181.2.4. MR3275847

[BM21] Simon R. Blackburn and K. Robin McLean, *Enumerating finite rings*, July 28, 2021. Preprint, `arXiv:2107.13215v1`.

[CTSSD98] J.-L. Colliot-Thélène, A. N. Skorobogatov, and Peter Swinnerton-Dyer, *Hasse principle for pencils of curves of genus one whose Jacobians have rational* 2*-division points*, Invent. Math. **134** (1998), no. 3, 579–650, DOI 10.1007/s002220050274. MR1660925 (99k:11095)

[Fen20] Tony Feng, *Étale Steenrod operations and the Artin-Tate pairing*, Compos. Math. **156** (2020), no. 7, 1476–1515, DOI 10.1112/s0010437x20007216. MR4122428

[GGGR19] Florence Gillibert, Jean Gillibert, Pierre Gillibert, and Gabriele Ranieri, *Selmer groups are intersection of two direct summands of the adelic cohomology*, Bull. Lond. Math. Soc. **51** (2019), no. 5, 776–786, DOI 10.1112/blms.12274. MR4022425

[Kap95] Irving Kaplansky, *Selected papers and other writings*, Springer-Verlag, New York, 1995. With an introduction by Hyman Bass. MR1340874 (97a:01074)

[KP70] Robert L. Kruse and David T. Price, *Enumerating finite rings*, J. London Math. Soc. (2) **2** (1970), 149–159. MR0251079 (40 #4310)

[LLR05] Qing Liu, Dino Lorenzini, and Michel Raynaud, *On the Brauer group of a surface*, Invent. Math. **159** (2005), no. 3, 673–676. MR2125738

[PR11] Bjorn Poonen and Eric Rains, *Self cup products and the theta characteristic torsor*, Math. Res. Lett. **18** (2011), no. 6, 1305–1318, DOI 10.4310/MRL.2011.v18.n6.a18. MR2915483

[SP] The Stacks Project authors, *Stacks project*, May 18, 2020. Available at `http://stacks.math.columbia.edu`.

[Won01] Siman Wong, *On the density of elliptic curves*, Compositio Math. **127** (2001), no. 1, 23–54, DOI 10.1023/A:1017514507447. MR1832985 (2002d:11066)