Partial List of Changes for the Second Edition of *The Arithmetic of Elliptic Curves*

Joseph H. Silverman

September, 2008

Major Changes and Additions

Chapter VIII, Section 11. A new section for the second edition entitled *Szpiro's Conjecture and ABC*. [6 pages]

Chapter XI. A new chapter on algorithmic aspects of elliptic curves and applications to cryptography. [45 pages]

Appendix B, Section 21. A new section entitled *Variation of a_p and the Sato–Tate Conjecture.* [2 pages]

Additional Exercises. 34 new exercises in Chapters I–X, plus 18 exercises in the new Chapter XI.

Figures. All figures have been redrawn.

Bibliography. The bibliography has been expanded from 174 items to more than 300 items.

Typesetting. The book has been entirely retypeset using TEX.

Minor Changes and Corrections

Typos. Corrected many minor typographical errors, too numerous to list.

Exercise 2.10. Corrected.

Exercise 2.15. Corrected, one of the criteria was not correct.

Remark III.7.3.1. Added remark. The groups $E[m]$ and $T_\ell(E)$ may be viewed as homology groups with an associated Galois action.

Remark III.8.4. Added remark. Generalized version of Weil pairing, with reference to exercise.

Remark III.8.5. Added remark. Alternative version of Weil pairing, with reference to exercise.

Proposition III.8.6. Added proposition. This proposition is moved from Chapter V, since it is not specific to finite fields. It is restated in Chapter V as (V.2.3) to maintain compatibility of numbering.

Exercise 3.10. Added part (g).

Exercise 3.21. New version. The final conclusion remains the same, but the path to the conclusion is more direct.

Chapter IV, Section 5. The assumption on the ring R has changed from characteristic 0 to torsion free. The problem with merely assuming characteristic 0, i.e., that $\mathbb{Z} \to R$ is injective, is that it does not ensure that the map $R \to R \otimes \mathbb{Q} = K$ is injective.

Chapter V. Changed K and K_n for a finite field and its extensions to the more standard $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$.

Remark V.1.5. Added remark. Computation of $\#E(\mathbb{F}_q)$ is nontrivial.

Remark V.1.6. Added remark. Statement of the elliptic curve discrete logarithm problem.

Theorem V.2.2. Changed the dimension of V from n to N, because lowercase n has been used for $\mathbb{F}_{q^n}$.

Proposition V.2.3. This result has been moved to Chapter III as (III.8.6). The result is restated here in Chapter V to maintain compatibility of numbering with the first edition.

Theorem V.4.7, Conjecture V.4.8, Theorem V.4.9. Expanded discussion from first edition to explicitly state theorems of Serre and Elkies and the conjecture of Lang and Trotter on distribution of supersingular primes.

Exercise 5.7. Corrected.

Proposition VI.5.6. New proposition. Interpretation of Λ and $E[m]$ as homology groups.

Exercies 6.4(f). Corrected, the function $|G(z)|$ is only analytic away from Λ.

Exercise 6.10. Minor change/correction.

Exercise 7.5. Minor change in description of fields.

Theorem 7.6. Remark 7.6 in the first edition is now a theorem, and Conjecture 7.7 in the first edition has been omitted. (In order to maintain compatibility of numbering, the second edition has no item labeled VIII.7.7, it goes directly from VIII.7.6 to VIII.7.8.)

Chapter VIII, Section 9. The "*Néron–Tate pairing*" is now called the "*canonical height* (or *Néron–Tate*) *pairing*."

Chapter VIII, Section 10. Updated the material on curves of high rank, including Elkies's example of rank at least 28.

Exercise 8.10. Changed to a more precise statement.

Exercise 8.17(b). The lower bound is changed to $\frac{1}{8}\log|d| + O(1)$. The lower bound in the first edition is not correct.

Chapter XI, Section 2. The definition of $d_v(P,Q)$ has been changed for the second edition, since in the older definition, the value of $d_v(P,Q)$ may behave badly if P is not close to Q, since then P might be close to some other zero of t_Q. This change does not affect the proofs, since they only use the situation that $P \to Q$.

Proposition XI.2.2. The second edition contains a somewhat more general version. There is also a notational change with a v placed below $P \to Q$ to indicate that the limit is being taken v-adically.

Theorem XI.8.2. Added theorem. An explicit statement of a quantitative version of Roth's theorem, which previously appeared in weaker form as part of Remark XI.8.1.

Exercise 9.2. Added part (c).

Exercise 9.3. (c) Changed "Prove" to "Prove or disprove". Added new parts (d) and (e).

Theorem X.4.9. Changed the definition of S so that it is valid for $a, b \in K$. The previous definition only made sense for $a, b \in R$.

Proposition X.6.5, Case II. Corrected the proof. In the first edition it says that $\gcd(pr^2 + 2Bt^2 + As, pr^2 + 2Bt^2 - As)$ equals $\gcd(A,s)^2$ up to a factor of 2. This need not be true.

Exercise 10.11. Added a new part (g).

Appendix B, Section 2. Corrected the definition of a discrete $G_{\bar{K}/K}$-module.

Appendix C, Theorem 13.6. Changed from a conjecture (credited to Taniyama and Weil) to a theorem (credited to Wiles et. al.), with a more precise statement. Added two paragraphs on the history of Wiles's proof.

Appendix C, Remark 13.6.1. New remark briefly describing the history of the modularity conjecture.

Appendix C, Remark 13.6.1. New remark briefly describing the path from the modularity theorem to Fermat's last theorem.

Appendix C, Evidence 16.5.5. Updated with results of Kolyvagin and Rubin.

Appendix C, Remark 20.2.1. Added remark on a result of Masser.

Appendix C, Conjecture 20.4. Added conjecture of Nagao.

Appendix C, Remark 20.4.1. Added partial results on Nagao's conjecture.

Notes on Exercises. Included a solution sketch of exercise 3.16(c).