Short Corrections to *Elliptic Curves* and Some Remarks

SHORT CORRECTIONS

Page 4, line 8. Change "cz" to "c".

Page 7, statement of Theorem 1.2. Change the attribution from Diophantus to Euclid.

Page 13, last sentence of statement of Theorem 1.4. Change the sentence so that it reads:
"If a different identity element O' is chosen, then the resulting two group structures are canonically isomorphic."

Page 38, last sentence of statement of Proposition 2.12. Change "Then (x_0, y_0, w_0) is a flex if and only if the Hessian matrix of F satisfies $\det H(x_0, y_0, w_0) = 0$" to
"If (x_0, y_0, w_0) is a flex, then the Hessian matrix of F satisfies $\det H(x_0, y_0, w_0) = 0$; conversely if the Hessian matrix of F satisfies $\det H(x_0, y_0, w_0) = 0$ and if the characteristic of k does not divides $d - 1$, then (x_0, y_0, w_0) is a flex".

Page 38, last sentence of second paragraph of proof of Proposition 2.12. Change "By Lemma 2.11, $\det H(x_0, y_0, w_0) = 0$" to
"Consequently either $H(x_0, y_0, w_0) = 0$ and $\det H(x_0, y_0, w_0) = 0$ trivially, or else $H(x_0, y_0, w_0) \neq 0$ and Lemma 2.11 shows that $\det H(x_0, y_0, w_0) = 0$".

Page 38, first sentence of third paragraph of proof of Proposition 2.12. Change "Conversely suppose $\det H(x_0, y_0, w_0) = 0$" to
"Conversely suppose that $\det H(x_0, y_0, w_0) = 0$ and that $d - 1$ is $\neq 0$ in k".

Page 38, second sentence of third paragraph of proof of Proposition 2.12. Change "By Lemma 2.11 the conic $C(x, y, w)$ defined by the matrix $H(x_0, y_0, w_0)$ is reducible" to
"If $H(x_0, y_0, w_0) = 0$, then (2.12) shows immediately that L divides Q_Φ; if $H(x_0, y_0, w_0) = 0$, then Lemma 2.11 shows that the conic $C(x, y, w)$ defined by the matrix $H(x_0, y_0, w_0)$ is reducible".

Page 39, statement of Corollary 2.13. Change "while a nonsingular plane curve of degree > 2" to "while a nonsingular cubic".

Page 39, line -12. Change "If $\deg F > 2$" to "If $\deg F = 3$".

Page 41, line -3. Change "$a_3 y w$" to "$a_3 y w^2$".

Page 41, line -1. Change "$\alpha x + \beta y$" to "$\alpha x + \beta w$".

Page 47, line 6 of Proof of second conclusion. Change "$[z, y]$" to "$[x, y]$".

Page 47, line -9. Change "Suppose $(x_i, y_i) = (x_j, y_j)$" to
"Suppose $(x_i, y_i) = (x_j, y_j)$ with $i \neq j$".

Page 47, line -1. Change "depend on Bezout's" to "depend on the second conclusion of Bezout's".

Page 50, next line after first display. Change "Proposition 2.13" to "Proposition 2.14".

Page 53, Example with $n = 5$. Change $\left(\dfrac{29}{12}\right)^2$ to $\left(\dfrac{31}{12}\right)^2$.

Page 61, line 10. Change "Corollary 3.34" to "Corollary 3.4".

Page 61, line 13. Change "Corollary 3.34" to "Corollary 3.4".

Page 67, last sentence of statement of Theorem 3.8. Change the sentence so that it reads:
"If a different base point O' is chosen, then the map $\varphi : (F(k), +) \to (F(k), +')$ given by $\varphi(P) = P + O'$ exhibits the two group structures as isomorphic."

Page 68, lines 11 to 17. Change this paragraph so that it reads:
"Let O' be given, and define a map $\varphi : (F(k), +) \to (F(k), +')$ by $\varphi(P) = P + O' = O(PO')$. Then φ is a homomorphism because multiple use of Lemma 3.9 gives

$$\varphi(P + Q) = O((P + Q)O') = O(O(PQ) \cdot O') = (O \cdot OO)(O(PQ) \cdot O')$$
$$= (O' \cdot OO)(O \cdot O(PQ)) = (O' \cdot OO)(PQ) = (O' \cdot OO)(O'O' \cdot (O'O' \cdot PQ))$$
$$= (O' \cdot O'O')(OO \cdot (O'O' \cdot PQ)) = O'(OO \cdot (O'O' \cdot PQ)) = O'(OO \cdot (PO' \cdot QO'))$$
$$= O'(O(PO') \cdot O(QO')) = O' \cdot \varphi(P)\varphi(Q) = \varphi(P) +' \varphi(Q).$$

The formula $\varphi(P) = P + O'$ shows that φ is one-one and onto."

Page 78, statement of Proposition 3.10. Change the second sentence to read,
"It is k rational if

   (i) char(k) is neither 2 nor 3, or
   (ii) char$(k) = 2$ and k is closed under the operation of taking square roots (as is the case when k is a finite field of characteristic 2), or
   (iii) char$(k) = 3$ and k is closed under the operation of taking cube roots (as is the case when k is a finite field of characteristic 3)."

Page 78, end of second paragraph of proof. Add the text
"If g has degree 3, then $g = f$. Hence $f' = 0$, char$(k) = 3$, and $f(x) = x^3 - a$ for some a in k. By hypothesis (iii), $a = x_0^3$ for some x_0 in k. Then $f(x) = (x - x_0)^3$, and $(x_0, 0)$ is the unique singular point.

Page 86, line 15. Change "$-\gamma - \gamma_1^2$" to "$-\gamma = \gamma_1^2$".

Page 91, lines 7 and 8. Change "Proposition 4.28" to Proposition 4.8".

Page 109, line -6. Change "diag$(\mathbb{Z})$" to "diag$(\mathbb{Z}_2)$".

Page 132, line 7. Change "$-2^{13}13$" to "$-2^{15}13$".

Page 132, line 8. Change "$2^{13}13$" to "$2^{15}13$".

Page 132, line 9. Change "or 4096" to "or 4096 or 16384".

Page 132, line -13. Change "Using the doubling formula" to "Making repeated use of the doubling formula".

Page 140, line -8. Change "$p^{3n}R$" to "$p^{2n}R$".

Page 140, line -7. Change "$|a_1x_3 + a_3w_3|_p \le 1$" to
"$|a_1x_3 + a_3w_3|_p \le |x_3|_p \le p^{-1}$".

Page 147, line 4. Change "nonsingular" to "singular".

Page 161, line 3. Change "$\omega\left(\frac{1}{2}(\omega_2)\right)$" to "$\wp\left(\frac{1}{2}\omega_2\right))$", and change "$\omega\left(\frac{1}{2}(\omega_1+\omega_2)\right)$" to "$\wp\left(\frac{1}{2}(\omega_1+\omega_2)\right)$".

Page 161, line 11. Change "$\omega'(z)^2$" to "$\wp'(z)^2$".

Page 168, line 12. Change "$\left(\gamma[t_{i-1},t_i],D_{i-1}^c\right)$" to "$\left(\gamma[t_{j-1},t_j],D_{j-1}^c\right)$".

Page 197, line -12. Change "all primes c" to "all primes p".

Page 216, line -8. Change "then to χ'" to "then to $\bar{\chi}$".

Page 272, lines 5 to 8. Change this paragraph so that it reads:
"Choose a disc D in $\mathcal{H}$ that maps one-one in the passage from $\mathcal{H}$ to $\mathcal{R}=\Gamma_0(N)\backslash\mathcal{H}$. Now let f and therefore F vary. Select $k\mu+1$ distinct points in D and consider the linear map $M_k(\Gamma_0(N)))\to\mathbb{C}^{k\mu+1}$ given by $f\to(F(p_1),\ldots,F(p_{k\mu+1}))$. By the above, this map has 0 kernel. Hence $\dim M_k(\Gamma_0(N))\le k\mu+1$."

Page 282, line -7. Change "Each space of equivalent eigenforms has a member that is an" to
"Each space of equivalent eigenforms has at least one member that is an".

Pages 305, line before first numerical display. Change "$\tau_0=.125+.025i$" to "$-\tau_0=.125+.025i$".

Pages 305–306. In addition to the above-mentioned correction on page 305, Allan Trojan has kindly pointed out that the remarks about the precision of the calculations is incorrect in various ways. In addition, the real part of $H(e^{2\pi iV_6(\tau_0)})$ was transcribed incorrectly. Discussion and revised numerical results appear in the Remarks at the end of this file of corrections.

Page 312, formula (11.20a). Change "$=(\omega_j\circ\varphi_i^{-1})(\varphi_j\circ\varphi_i^{-1})'$" to
"$=(\omega_j\circ\varphi_j^{-1})(\varphi_j\circ\varphi_i^{-1})'$".

Page 314, line -3. Change "$=(\omega_j\circ\varphi_i^{-1})(t_i)$" to "$=(\omega_j\circ\varphi_j^{-1})(t_i)$".

Page 339, line -5. Change "ω" to "y" twice.

Page 339, line -3. Change "ω" to "y" twice.

Page 375, statement of Lemma 11.75. Change the first sentence so as to read, "Let $\mathcal{T}$ be a finite-dimensional associative algebra with identity over a field k of characteristic 0, and let $\mathcal{R}$ be its **nilradical** (largest nilpotent two-sided ideal)."

Page 376, third paragraph, line 1. Change "maps J into A" to "maps A into A".

Page 376, third paragraph, line 3. Change "$(\ker(\nu\circ T(n))\subseteq\ker\nu$" to
"$\ker\nu\subseteq\ker(\nu\circ t(n))$".

Page 392, lines 4 and 5. Change "a theorem of Serre allows us to conclude that E and E' are isogenous over $\mathbb{Q}$ provided $j(E)$ is not an integer" to "theorems of Serre and Faltings allow us to conclude that E and E' are isogenous over $\mathbb{Q}$".

Page 404, lines 2 and 3. Change "Birch discovered an error in Manin's proof, and the error is corrected in Cassels [1957] and here" to
"Birch discovered an apparent gap in Manin's proof, and Cassels [1957] showed how to follow a different path to fix the argument. We follow the line suggested by Cassels. The version of Manin's proof in the book of Gelfond and Linnik [1962] is closer to what Manin may have intended".

Page 406, line 17. Change "Swinnerton-Dyer, Stephens, et al. [1975]" to "Birch, Swinnerton-Dyer, Stephens, et al. [1975]". See the correction to page 415 listed below.

Page 406, line 21. Change "121 to 124" to "121 to 124; the omitted page turns out to be present but was printed out of order".

Page 406, lines 26 and 27. Change "Serre's Isogeny Theorem, which is on p. IV-14 of Serre [1968]" to "Serre's Isogeny Theorem, which is on p. IV-14 of Serre [1968] and which handles the case that $j(E)$ is not an integer, and to the work of Faltings [1983], which handles arbitrary $j(E)$".

Page 406, lines -4 and -3. Change "Swinnerton-Dyer, Stephens, et al. [1975]" to "Birch, Swinnerton-Dyer, Stephens, et al. [1975]". See the correction to page 415 listed below.

Page 407, third paragraph. Insert the following between the sentence about Frey and the sentence about Serre: "Earlier Hellegouarch [1975] had studied a special case of (12.12) in connection with a case of the Fermat equation."

Page 415, last reference. The name "B. J. Birch" is added as the first author of these tables, despite what is listed in the Antwerp volume and what is listed in MathSciNet. Thus the correct authorship is "Birch, B. J., H. P. F. Swinnerton-Dyer, N. M. Stephens, J. Davenport, J. Vélu, F. B. Coghlan, A. O. L. Atkin, and D. J. Tingley".

Add the following four items to the section of References:

Hellegourarch, Y., Points d'ordre $2p^h$ sur les courbes elliptiques, *Acta Arithmetica* 26 (1975), 253–263.

Faltings, G., Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* 73 (1983), 349–366, and 75 (1984), 381.

Gelfond, A. O., and Ju. V. Linnik, *Elementary Methods in Analytic Number Theory*, Gosudarstv. Izdat. Fiz.-Math. Lit., Moscow, 1962 (Russian); Rand McNally and Co., Chicago, 1965.

Weil, A., *Number Theory: An Approach through History, From Hammurapi to Legendre*, Birkhäuser, Boston, 1983.

Remarks

Attribution of Theorem 1.4 (= Theorem 3.8): Awareness of this theorem has to be regarded as an evolutionary process, and Abel was certainly aware of the result on some level, well before Poincaré.

———-

Numerical calculations on pages 305—306, including the comments about them: These remarks are prompted by comments by Allan Trojan. In the middle of page 305, the text reads, "Judicious choice of τ_0 cuts down considerably on the number of terms needed." Indeed the series for $H(q)$ is to be truncated for purposes of computation. Since each c_n is an integer, q^n/n had better be quite small at the point of truncation for the three q values $e^{2\pi i \tau_0}$, $e^{2\pi i V_4(\tau_0)}$, and $e^{2\pi i V_6(\tau_0)}$. For $\tau_0 = i$, $V_6(\tau_0)$ has a small imaginary part, and the corresponding value of $|q^n/n|$ is about 10^{-6} for $n = 3000$. Thus at least 3000 terms of the series for $H(q)$ would be needed for single-precision results.

The series for $H(q)$ is difficult to compute, and it is desirable to use fewer terms. With the choice $\tau_0 = -.125 + .025i$, the three values of $|q^n/n|$ are less than 10^{-10} for $n = 300$. Estimating the actual error term would require knowing something about the size of the coefficients of $\prod_{n=1}^{\infty}(1 - q^n)$; the first 300 coefficients are all 0, $+1$, or -1, but the author does not know whether this phenomenon persists for all coefficients. Without this kind of control, the sum of tail of the series for $H(q)$ has no useful evident estimate, and we shall be content with the calculations of $H(q)$ as the sum of the first 300 terms, the results being truncated after 11 decimal places. The results are

$$H(e^{2\pi i \tau_0}) \doteq .26281060793 + .52304554449i$$
$$H(e^{2\pi i V_4(\tau_0)}) \doteq .89741526007 - .93577107244i$$
$$H(e^{2\pi i V_6(\tau_0)}) \doteq 1.53201991181 + .52304554470i$$
$$\omega_1 = \Phi_f(V_4) \doteq -.23217787565 - .10100046730i$$
$$\omega_2 = \Phi_f(V_6) \doteq .00000000003 - .20200093453i$$

The corresponding numerical results on page 306 are

$$g_2(\Lambda) \doteq 64419.8790 - .00000i$$
$$g_3(\Lambda) \doteq -5699400.00 + .000i$$
$$j(\Lambda) \doteq -757.6726 + .000000i$$

———-

Title of Chapter XII: What was known as the "Taniyama–Weil Conjecture" at the time *Elliptic Curves* was written has come to be known, more fairly, as either the "Taniyama–Shimura–Weil Conjecture" or the "Shimura–Taniyama–Weil Conjecture." The conjecture has since been completely proved by A. Wiles and others.

———-

Additional reference: The Cremona book listed below was published at about the same time as *Elliptic Curves* and has bearing on a number of topics in it. One thing that the book contains is extensive tables of information beyond the ones in Birch, Swinnerton-Dyer, Stephens, et al. [1975].

————-

Cremona, J. E., *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1992.

2/17/09