Addendum/Erratum for Elliptic Curves 2006

J.S. Milne

Last revised September 7, 2016.

In the blurb and introduction, I should have noted that the group is commutative.

**p28.** The third cubic curve should be
\[ \ell(R, Q) \cdot \ell(P, Q + R) \cdot \ell(PQ, O) = 0 \]
(Dmitriy Zanin).

**p36.** In the definition of \( k[C]_p \), the condition on \( h \) should be \( h \not\equiv p \) (Jochen Gerhard).

**p39.** In the definition of a regular map between projective plane curves, \( a_m \) should read \( a_2 \) (Rankeya Datta).

**p100, 3.23b.** The sign is wrong: it should read \( 4d - c^2 \geq 0 \). As PENG Bo pointed out to me, I forgot to include the proof. Here it is.

Let
\[ X^2 + c' X + d' = \det(X - n\alpha|T_\ell E). \]
By linear algebra, we see that \( c' = nc \) and \( d' = n^2d \). On substituting \( m \) for \( X \) in the equality, we find that
\[ m^2 + cmn + n^2d = \det(m - n\alpha|T_\ell E). \]
According to Proposition 3.22, the right hand side equals the degree of \( m\text{id} - n\alpha \). Therefore
\[ m^2 + cmn + n^2d \geq 0 \]
for all \( m, n \in \mathbb{Z} \), i.e.,
\[ r^2 + cr + d \geq 0 \]
for all \( r \in \mathbb{Q} \). The minimum value of \( r^2 + cr + d \), \( r \in \mathbb{R} \), is \( \left( \frac{c}{2} \right)^2 + c \left( -\frac{c}{2} \right) + d = \frac{c^2}{4} + d \), and so
\[ 4d \geq c^2 \] (happily, this is how I used it on p150 in the proof of the congruence Riemann hypothesis).

**p107, line 2** (exact sequence of cohomology groups): a bracket “\( \)" is missing: \( H^1(G, \mu(k^a_l)) \) instead of \( H^1(G, \mu(k^a_l)) \) (Michael Mueller).

**p148, 9.1b.** Should read: The Frobenius map acts as zero... \( \) (not as zero acts; at least I not think).

**p150, 9.5.** Taylor et al. prove the conjecture of Sato and Tate only for elliptic curves that do not have potential good reduction at some prime \( p \).

**Bibilography:** Fulton’s book, Algebraic Curves, is now freely available on his website http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

**From Stefan Müller:**

page 7, line -7: the coordinates should be small \( x \) and \( y \)

page 9, line -13: \( k[X, Y] \) square brackets also inside the set definition
page 33: in my class I used $K_C$ instead of $W$, since it is "the" usual notation, of course the letter $K$ can be confused with the field $K$

page 36, line 18: $h$ not in $p$, instead of non-zero.

page 37, section on Riemann-Roch: in contrast to the rest of the book the algebraic closure here is $\bar{k}$ not $k^\text{al}$.

page 39, line -6: delete word before $P^2$.

page 51, line -12: in my opinion $c$ must be $u_1/u_2$ not $u_2/u_1$.

page 66, line -8: it is Corollary 4.2 not Prop. 4.2 (perhaps also at other places)

page 100, Corollary 3.23: In (b) the inequality sign seems wrong, at least it contradicts what you use of it later. The sign of the term $c\alpha$ seems also wrong, at least contradicts the proof. The proof of (b) is completely missing, but it is very important in the applications (Hasse-Weil). [See above.]

page 104, proof of Cor. 1.4: in my opinion it must be $\sigma c/c$ not $c/\sigma c$. At the blackboard I was fighting with this problem for about 10 minutes, still not sure.

page 105, footnote: element not elements

page 149, Thm. 9.4: square root of $p$ ! Proof refers to Cor 3.23 (see above).

page 157, line 6: inverse roots not roots

**From Nicholas Wilson:**

On page 167, line -17, there is written "Coates and Wiles (1977)...", which I believe should read "Coates and Wiles (1977)."