Errata, Changes, and Addenda for the Books “Number Theory” Volumes I and II

by Henri Cohen

Last modified: November 30, 2008

Errata: errors, mathematical or otherwise, which *must* be corrected.

Changes: modifications which improve the presentation.

Addenda: additions of relevant, useful, and/or interesting material.

Errata:

In Volume I:

p. 4 line 9 and 19, replace “finite (this can...exercise).” by “finite.”
p. 13 line -11, replace “$V \in dkA_1$” by “$V = dkA_1$”
p. 37 middle, add an “=” sign between $\left(\frac{a}{|m|}\right)$ and $\operatorname{sign}(a+km)$
p. 44 line 2, replace “$n = 1 + |D|/2$” by “$n = 1 + D/2$”
p. 49 lines -3 to -1, replace “, and one can... Exercise 17).” by “; see also Exercise 17.”
p. 55 line -11, replace “Elkies et al.” by “Cohn et al.”
p. 80 line 7, add a white square at the end of the proof of Lemma 2.5.13
p. 85 line -16, replace “$a + b \equiv p - 2 \pmod 9$” by “$a + b \equiv q - 2 \pmod 9$”
p. 86 line 5, replace “$a^2 - ab + b^2 = p$” by “$a^2 - ab + b^2 = q$”
p. 95 replace Exercise 17 (which is false) by the following (hopefully correct) exercise:

“17.

(a) Show that for any one of the four primitive characters χ modulo 16, the root number $W(\chi)$ is a 16th root of unity.

(b) Assume that $m > 3$ and $m \not\equiv 2 \pmod 4$. Show that if $W(\chi)$ is a root of unity for all primitive characters χ modulo m, then in fact $W(\chi)^m = 1$, and furthermore that $\lambda(m) \mid m$, where $\lambda(m)$ is Carmichael’s function as defined in Exercise 6 (I do not know how to prove this, but it must be true and not too difficult).”

p. 179 in Exercise 4, replace “$f(x + a^2) = f(x) + f(a)^2$” by “$\sigma(x + a^2) = \sigma(x) + \sigma(a)^2$”
p. 210 lines 3 to 13, replace “$v_p($... as claimed” by the following:

“

$$\begin{aligned} v_p\left(n!\binom{a}{n}\right) &\ge \sum_{0\le k<q} k \sum_{\substack{0\le i<n\\ v_p(i)=k}} 1 + v_p(a) \sum_{\substack{0\le i<n\\ v_p(i)\ge q}} 1 \\ &= \sum_{0\le k<q} k(\lceil n/p^k\rceil - \lceil n/p^{k+1}\rceil) + v_p(a)\lceil n/p^q\rceil \\ &= \sum_{1\le k\le q} \lceil n/p^k\rceil - \theta\lceil n/p^q\rceil \end{aligned}$$

again by Abel summation. Transforming the ceiling into the floor function it is clear that this gives

$$v_p\left(n!\binom{a}{n}\right) \ge \max(q-\theta-v_p(n),0) - \sum_{1\le k\le q} \lfloor n/p^k\rfloor - \theta\lfloor n/p^q\rfloor\ ,$$

and since by (1) we have $v_p(n!)=\sum_{k\ge1}\lfloor n/p^k\rfloor$, it follows that

$$v_p\left(\binom{a}{n}\right) \ge \max(v_p(a)-v_p(n),0) - \theta\lfloor n/p^q\rfloor - \sum_{k\ge q+1}\lfloor n/p^k\rfloor\ .$$

In addition

$$\sum_{k\ge q+1}\lfloor n/p^k\rfloor \le \sum_{k\ge q+1} n/p^k \le n/(p^q(p-1))\ ,$$

so that

$$v_p\left(\binom{a}{n}\right) \ge \max(v_p(a)-v_p(n),0) - \frac{n}{p^q}\left(\frac{1}{p-1}+\theta\right)\ ,$$

as claimed.”

p. 242 lines -17 and -16, replace “, so that $\mathbb{Q}_q/\mathbb{Z}_q=\mathbb{F}_q$” by “.”

p. 268 line -15, replace “$|z|<\delta$” by “$|\zeta|<\delta$”

p. 269 line -2, replace “$|z^{p^N}/(1-z^{p^N})$” by “$|z^{p^N}/(1-z^{p^N})|$”

p. 280 suppress Exercise 30

p. 300 line -3, replace “the the” by “the”

p. 360 line 9, replace “trivial solution” by “nontrivial solution”

p. 361 lines -12 to -10, replace “It is easy... weakened to” by the following: “For $p=3$, it is clear that conditions (a) and (b) of (5) are equivalent to $\ell\ne p$, and it is easy to see that condition (c) can be replaced by $-b/a\in G_\ell$, $-c/a\in G_\ell$, or $-c/b\in G_\ell$; see Exercise 32. For $p=5$, condition (b) can be weakened to”

p. 377 middle, replace “infinitely many integers” by “infinitely many cube-free integers”

p. 380 line -11 and following, replace “K. Yarbrough” by “K. Jensen”, add “see [BPTJ]”, and in the references add at the appropriate place the reference “[BPTJ] M. Beck, E. Pine, W. Tarrant, and K. Jensen, *New integer representations as the sum of three cubes*, Math. Comp. **76** (2007), 1683–1690.”

p. 380 line -8, replace "$n = 33$, 42, 52, and 74" by "$n = 33$, 42, and 74" (the solution $52 = 60702901317^3 + 23961292454^3 + (-61922712865)^3$ was in fact found in 2007 by A. S. Elsenhaus and J. Jahnel)

p. 387 line 13, replace "sox" by "so"

p. 420 line -14, replace "$-D(fy)^2 + 1 = 4y^p$" by "$-D(fy)^2 + 1 = 4x^p$"

p. 420 line -6, replace "$\alpha = (a + b\sqrt{-3})/2$" by "$\alpha = (a + b\sqrt{-t})/2$"

p. 446 line -11, replace ",n which" by ", which"

p. 452 in line 3 of the proof of Proposition 6.12.2 add "and $q > 0$"

p. 452 in lines 6 and 7 of the proof of Proposition 6.12.2, replace

"so they are all squares... $p_1^4 - q_1^4 = w^2$." by

"so there exist $\varepsilon = \pm 1$ and integers p_1 and q_1 such that $p = \varepsilon p_1^2$, $q = q_1^2$, and $p^2 - q^2 = \varepsilon w^2$, from which we obtain the equation $p_1^4 - q_1^4 = \varepsilon w^2$."

p. 457 lines 3 and 4 of Exercise 12, replace "two-parameter" by "one-parameter"

p. 458 lines 3 and 4 of Exercise 16, replace "$\varepsilon_1 \equiv 1 \pmod{3\mathbb{Z}_K}$" by

"$\varepsilon_1 \equiv \pm 1 \pmod{3\mathbb{Z}_K}$"

p. 460 lines -8 and -7, replace "Show that... removed;" by

"Show that if there exists $m \in G_\ell$ such that $-(c + am)/b \in G_\ell$, then either $-b/a$, $-c/a$, or $-c/b$ is in G_ℓ, so that this additional condition in (c) can be removed;"

p. 510 line 12 and 13, replace "the the" by "the"

p. 512 line 2 of Exercise 1 (a), replace "degree 24" by "degree dividing 24"

p. 529 line -8, replace "mightn" by "might"

p. 532 line 12, replace "$\max(1, \log(|x|))$" by "$\log(\max(1, |x|))$"

p. 555 middle, replace "the the obstruction" by "the obstruction"

p. 564 line -5, replace "$ax^3 + by^3 + cz^3$" by "$ax^3 + by^3 + cz^3 = 0$"

p. 568, replace "$x^3 = y^2 - 1$ is equal to $1 + \chi(y^2 - 1) + \overline{\chi}(y^2 - 1)$" by

"$x^3 = y^2 - N$ is equal to $1 + \chi(y^2 - N) + \overline{\chi}(y^2 - N)$"

p. 578 line 1, replace "thatn" by "that"

p. 610 last line of Exercise 16, replace "c_q odd" by "$c_q(E)$ even"

In Volume II:

p. 40 middle, in the last two factors of the displayed formula, replace a total of three times "t" by "mh"

p. 42 line -13, replace "practice" by "in practice"

p. 55 lines -16, -15, -14, and -12, replace "$pS_k(\chi)$" by "$S_k(\chi)$"

p. 96 line -1, replace "$1 \le k \le v(\alpha)$" by "$1 \le k \le -v(\alpha)$"

p. 101 line 3, replace "$\zeta(s, x + u))$" by "$\zeta(s, x + u)$"

p. 105 line 2, replace "for all x, where f" by "for all x at which f"

p. 112 line 10, remove the superfluous "x"

p. 125 line 2, replace "$\pm iT$" by "$a \pm iT$"

p. 137 in (b) of Exercise 80, replace "$f(1/2)$" by "$|f(1/2)|$"

p. 174 line 10, replace "the the" by "the"

p. 183 line -6, replace "the the" by "the"

p. 193 line -4, replace "thatn" by "that"

p. 198 line 7, replace "σ_2 functions" by "σ_k functions"

p. 219 line -6 and -5, replace “The result follows by letting s tend to 1.” by

“By letting s tend to 1 we deduce that $L(\chi_D, 1) \geq 0$, and the strict inequality follows from the third proof of Theorem 10.5.29 that we will give below.”

p. 255 line 2, replace “ideal” by “idea”

p. 259 in Exercise 2 (c), add the assumption that $P' \neq 0$

p. 261 line -3, replace “Λ_{n+1}” by “$\Lambda_{n+1}(s)$”

p. 270 suppress Exercise 54

p. 295 line 8, replace “$0 \leq r < x$” by “$0 \leq r < n$”

p. 299 line 3, replace “$\binom{1-s}{k}$” by “$\binom{-s}{k}$”, and line -7 (last line of proof), replace “$\dfrac{1}{s-1}$” by “$\dfrac{1}{s+k-1}$”

p. 314 line -2, replace “x modulo p^v” by “x modulo p^{v-1}”

p. 316 line -1, replace “proof of the theorem” by “proof of the corollary”

p. 341 line 10, replace

“$\mathrm{Log}\Gamma(\chi, x) = L_p'(\chi\omega, 0) = 0$” by “$\mathrm{Log}\Gamma_p(\chi, 0) = L_p'(\chi\omega, 0) = 0$”

p. 353 and following, unfortunately statement (2) of Theorem 11.5.30 is false (but statement (3), which is the only one that we use, is correct). This implies the following changes, which of course are errata:

– p. 353 replace the whole of statement (2) by the following:

(2) Let ζ be a p^vth root of unity different from 1. Then

$$S(\zeta^r) - S(\zeta) = \begin{cases} \log_p\left(\dfrac{\zeta^r - 1}{\zeta - 1}\right) - \dfrac{1}{p}\log_p\left(\dfrac{\zeta^{pr} - 1}{\zeta^p - 1}\right) & \text{if } \zeta^p \neq 1 \\ \log_p\left(\dfrac{\zeta^r - 1}{\zeta - 1}\right) & \text{if } \zeta^p = 1\ . \end{cases}$$

– p. 354–355, in all the proof of (2) replace z by ζ.

– p. 354 line -12, replace “Thus” by “Thus, for N sufficiently large (so that $\zeta^{p^N} = 1$)”, and lines -11 and -5, in both formulas, replace “$S_N(z)$” by “$S_N(1/\zeta)$”.

– p. 354 remove lines -4 to -1

– p. 355 line 1, replace “and since” by “Since”, and lines 2 and 3 replace “$S(z)$” by “$S(1/\zeta)$”

– p. 355 between the formulas of line 2–3 and line 4 insert the following:

“Now it immediately follows from Lemma 11.5.29 that $S(1/z) = S(z)$ (see Exercise 27.5), so we can replace $S(1/\zeta)$ by $S(\zeta)$ in the above formulas.”

– p. 355 middle, replace “We have $\log_p(\zeta) = 0$, hence $L(\zeta, r) = \delta_{v,1}\log_p(r)/p$, where we set” by “Set”

– p. 356 lines 3–4, remove “since when $v = 1$ ... cancels with $L(\zeta, r)$.” and change the preceding comma to a period.

– p. 402, between Exercises 27 and 28 insert the following exercise:

“27.5. By replacing a by $p^N - a$, prove that $S_N(1/z) = S_N(z) + O(p^{N-B})$ for some B independent of N, so that $S(1/z) = S(z)$.”

p. 372 line 1 of Theorem 11.6.14, replace “n” by “N” twice

p. 395 line -6 and -5, replace twice “strongly differentiable” by "strictly differentiable"

p. 403 line -3, replace "$\left\lceil \frac{ar}{p^N} \right\rfloor$" by "$\left\lceil \frac{ar}{p^N} \right\rceil$"

p. 449 line -7, replace "withn" by "with"

p. 452 line 12, replace "best-nknown" by "best-known"

p. 453 line -9, replace ", This" by ", this"

p. 453 line -4, replace "have been" by "has been"

p. 464 line 1, replace "*parabolic*" by "*parabolic* case"

Changes:

In Volume I:

p. 39 line -6, replace "we need the results that we will prove elsewhere" by "we need elsewhere the results that we are going to prove"

p. 39 line -4, replace "denominators" by "moduli"

p. 62 replace "10^{-67}" by "$1.5{\cdot}10^{-67}$" three times, and in the middle, replace "154" by "153"

p. 66 line 1, replace "**Theorem 2.4.2.**" by "**Theorem 2.4.2 (Wedderburn).**"

p. 208 line -1, after "notation." add "We have $\binom{x}{0} = 1$ for all x, and $\binom{0}{n} = 0$ when $n \geq 1$."

p. 209 line 6, replace "$a \in \mathcal{K}$" by "$a \in \mathcal{K}^*$"

p. 209 statement (2) (b), replace the formula by

$$v_p\left(\binom{a}{n}\right) \geq \max(v_p(a) - v_p(n), 0) - \frac{n}{p^q}\left(\frac{1}{p-1} + \theta\right) ,$$

p. 209 middle, replace ", $a \neq 0$ and $n \geq 1$" by "$n \geq 1$,"

p. 318 line -3, remove ", and that we ... places"

p. 330 Exercise 10 (b), replace "Then there exist $(\alpha_i)_{1 \leq i \leq n}$ with" by "Show that there exist $(\alpha_i)_{1 \leq i \leq n}$ such that"

p. 338 line 13, replace "in K" by "in some number field K"

p. 354 lines -5 and -4, replace "the corresponding element $x + y\sqrt{D}$ of the quadratic field" by "a complete system of representatives (up to multiplication by units) of elements $x + y\sqrt{D}$ of norm N (which can also be easily obtained using a CAS)"

p. 362 line 5, remove "over an integral domain of characteristic zero"

p. 362 middle, replace
"it is the *only* method that enables us to study" by
"it is by far the most important method for studying the"

p. 368 line 6, replace "α" by "β"

p. 401 line 11, replace "Since $c \equiv 1$ or 2 modulo 16 it follows" by
"It follows"

p. 418 lines -9 and -8, replace "$A_p(t)$" by "$A_p(-1)$" twice

p. 420 line -11, replace "a pth power" by "the pth power"

p. 458 line 5 of Exercise 16, replace twice "α" by "β"

p. 488 line 10 to the end of the page, replace "that $N \mid (DM' - 2MD')$

and ... Exercises 19 and 20." by the following, and add Chapman, R. in the index of names:

"that $N \mid (DM' - 2MD')$; in other words, if $H = X'/Y = (DM' - 2MD')/N$, then H is a polynomial. But $(X(1/T), Y(1/T))$ is also in $E(K)$, so we deduce that $(d/dT)(X(1/T))/Y(1/T) = -T^{-2}H(1/T)$ is also a polynomial, which is impossible unless $H = 0$. Thus $X'(T) = 0$, so by the reduction made above we deduce that X and Y are constant. □

The above simplified proof was sent to me by R. Chapman, and an interesting alternative proof of this proposition has been communicated to me by J. Cremona; see Exercises 19 and 20."

p. 508 line 3, replace "." by ", and is denoted $c_{\mathfrak{p}}(E)$ (or simply $c(E)$ if $\mathfrak{p}$ is understood)."

p. 518 line -19 and -18, replace ", using a method...version." by

"; see Exercise 11 for a weaker but nontrivial result due to Mestre."

p. 554 line 2, replace "c_q" by "$c_q(E)$"

p. 567 lines 1 to 5, replace by the following:

"*Proof.* The case $p \mid 2N$ being immediate, assume that $p \nmid 2N$. When $p \equiv 3 \pmod 4$ we have $\left(\frac{-1}{p}\right) = -1$, so for each x not equal to 0 or ± 1 there is exactly one value in $\{x, -x\}$ such that $x^3 - x$ is a square. It follows that $a_p(N) = 0$ in that case (this is a special case of a general fact on curves with CM that we will state in Proposition 8.5.5 below)."

p. 570 line 11, replace "by the group $\mathbb{Q}^*/{\mathbb{Q}^*}^2$" by "by an element of the group $\mathbb{Q}^*/{\mathbb{Q}^*}^2$"

p. 573 lines 9–10, replace "computing $L(E, s)$ and its derivatives numerically." by "computing numerically $L(E, s)$ and its derivatives."

p. 578 line -3, reduce the size of the big parentheses

p. 578 replace "k" by "r" everywhere in Proposition 8.5.17, and make the corresponding changes in the proof

p. 580 make similar changes in Proposition 8.5.19 and its proof

p. 584 line -1, replace "c_p" by "$c_p(E)$"

p. 590 line -7, replace "c_∞" by "$c_\infty(E)$"

p. 608 line 1 of Exercise 9, replace "$Y^2 = X^3 - 34992$." by

"$Y^2 = X^3 - 34992$ (note that $34992 = 2^4 \cdot 3^7$)."

p. 608 line 4 of Exercise 9, replace "Proposition 7.2.3." by

"Proposition 7.2.3 (you may want to work on the simpler model $Y^2 = X^3 - 48$)."

p. 610 in Exercise 16 replace "$c_5 = 3$" by "$c_5(E) = 3$"

In Volume II:

p. 100 replace line 1 of Proposition 9.6.50 by "Let $n \in \mathbb{Z}$, $x \in \mathbb{R}_{\geq 0}$, $s \in \mathbb{C}$, assume that $x \neq 0$ when $\Re(s) \geq 1$, and set"

p. 100 and 101, replace everywhere "$C_n(x)$" by "$Z_n(s, x)$", "C_n" by "$Z_n(s)$", "I_n" by "$I_n(s)$" and so on, adding the variable s when necessary and replacing derivatives by $\partial/\partial x$

p. 100 line 4 of the proposition and p. 101 middle, replace "$i(1-s)\pi/2\,\mathrm{sign}(n)$" by "$i(1-s)(\pi/2)\,\mathrm{sign}(n)$"

p. 100 replace the first three lines of the proof by:

"*Proof.* Assume first that $0 < \Re(s) < 1$, so that the integral defining $Z_n(s,x)$ converges for $x \geq 0$. We have"

p. 102 and 103, replace both times "$C_n(x)$" by "$G_n(x)$"

p. 106 lines -8 and -7, replace "See Exercise 101" by "See Exercise 101 of the present chapter and Exercise 21 of Chapter 10"

p. 125 line 1, replace "Assume that f satisfies the assumptions of Proposition 9.2.11." by

"Assume that f is a holomorphic function on $\Re(z) > 0$ and that $f(z) = o(\exp(2\pi|\Im(z)|))$ as $|\Im(z)| \to \infty$ uniformly in vertical strips of bounded width."

p. 125 Exercise 33 (a), replace "$\int_{\mathcal{C}} \mathrm{cotan}(\pi t) f(t)\,dt$" by "$\int_{\mathcal{C}} (\mathrm{cotan}(\pi t) + i\,\mathrm{sign}(\Im(t))) f(t)\,dt$."

p. 144 in Exercise 100, replace four times "$\pi^2 + \log^2(x)$" by "$\log^2(x) + \pi^2$"

p. 157 line 1, add a space before "(1)"

p. 167 line 2, replace "for that" by "that"

p. 176 lines 11 to 13, replace "and it seems ... we can simply" by "and although $\theta(\overline{\chi}, i)$ may vanish, it seems to be a very rare occurrence; see Exercise 29.5. In any case, if this happens we simply"

p. 182 line -11, replace "131/416" by "64/205", line -10, replace "$\varepsilon > 0$." by "$\varepsilon > 0$, see [Hux].", and in the bibliography, at the appropriate place, add

"[Hux] M. Huxley, *Exponential sums and the Riemann zeta function V*, Proc. London Math. Soc. **99** (2005), 1–41."

p. 193 line -14, replace "n times" by "$n = [K : \mathbb{Q}]$ times"

p. 200 lines 11 to 13, replace "*odd* order.... ERH." by

" *odd* order g. More precisely, they show that we may replace it by $\log(f)^{1-\delta_g}$ for some $\delta_g > 0$ and by $\log(\log(f))^{1-\delta_g}$ under the ERH, where

$$\delta_g = \frac{1}{2}\left(1 - \frac{\sin(\pi/g)}{\pi/g}\right) > 0\ ."$$

p. 221 line -6, replace "D." by "D, let $\mathcal{A}$ be an ideal class of K, and let $\tau = \tau_{\mathcal{A}}$ be as in Proposition 10.5.7."

p. 234 line -2 and p. 235 middle, replace "Res(" by "R("

p. 234 line -1, replace "Res *denotes the resultant of the two polynomials*"

by "*as usual $R(A,B)$ denotes the resultant of the polynomials A and B*"

p. 259 in (e) of Exercise 2, replace "polynomial H" by "polynomial $H \in \mathbb{F}_5[X]$"

p. 262, after Exercise 29, add the following exercise:

"29.5. (I do not know of a clean answer to question (b) of this exercise.) Let χ be the character modulo 300 defined by $\chi(277) = e^{4i\pi/5}$ and $\chi(101) = \chi(151) = -1$.

(a) Show that this does define a unique character, and that χ is a primitive and even character modulo 300.

(b) Show that $\theta(\chi, i) = 0$, where as in the text $\theta(\chi, i) = 2\sum_{n\geq 1}\chi(n)e^{-\pi n^2/5}$.

(c) By using a computer program, show that for all characters of conductor less than 5000 and different from χ, $\overline{\chi}$, and from two conjugate characters modulo 600 analogous to χ, we have $\theta(\chi, i) \neq 0$."

p. 266 end of (d) of Exercise 38, replace "$1/(8\pi)$" by "$-1/(8\pi)$"
p. 337 line 8, replace "we ask that $\chi_0(p) = 0$" by "$\chi_0(p) = 0$",
and line 9 replace "it is clear that the definition then does not" by
"it is then clear that the definition does not"
p. 489 line 5, replace "reason for which" by "reason that"
p. 491 middle, replace "the *abc* conjecture" by "a strong form of the *abc* conjecture"
p. 534 in both formulas of Lemma 16.1.8, remove the outermost parentheses

Addenda:

In Volume I:

p. 80 after the end of the proof of Lemma 2.5.13, insert the following:

"**Lemma 2.5.13.5** *For $k \geq 2$ we have*

$$J_k(\chi_1, \dots, \chi_k) = J_{k-1}(\chi_1, \dots, \chi_{k-1})J_2(\chi_1 \cdots \chi_{k-1}, \chi_k)\ .$$

Proof. By the preceding lemma we have

$$\begin{aligned} J_k(\chi_1, \dots, \chi_k) &= \sum_{x_k \in \mathbb{F}_q} \chi_k(x_k) \sum_{\substack{x_i \in \mathbb{F}_q \\ x_1+\cdots+x_{k-1}=1-x_k}} \chi_1(x_1)\cdots\chi_{k-1}(x_{k-1}) \\ &= \sum_{x_k \in \mathbb{F}_q} \chi_k(x_k)J_{k-1}(\chi_1, \dots, \chi_{k-1}; 1-x_k) \\ &= \sum_{x_k \in \mathbb{F}_q} \chi_k(x_k)(\chi_1\cdots\chi_{k-1})(1-x_k)J_{k-1}(\chi_1, \dots, \chi_{k-1}) \\ &= J_2(\chi_k, \chi_1\cdots\chi_{k-1})J_{k-1}(\chi_1, \dots, \chi_{k-1})\ , \end{aligned}$$

proving the lemma. □

Note that the inductive use of this lemma gives the fastest way to compute multiple Jacobi sums $J_k(\chi_1, \dots, \chi_k)$ in practice."

p. 87 after the end of the proof of Proposition 2.5.20, insert the following:

"When $q \equiv 1 \pmod 3$ and the characteristic of $\mathbb{F}_q$ is a prime $p \equiv 2 \pmod 3$, we can be more precise than (2) and give in fact the exact value of $J(\chi, \chi)$:

Proposition 2.5.20.5. *Let $p \equiv 2 \pmod 3$ be prime, assume that $q = p^{2m}$, so that $q \equiv 1 \pmod 3$, and let χ be one of the two characters of order 3 on $\mathbb{F}_q^*$. We have $J(\chi, \chi) = (-1)^{m-1}p^m = (-1)^{m-1}q^{1/2}$.*

Proof. We have $J(\chi,\chi)=a+b\rho$ with $a^2-ab+b^2=q=p^{2m}$. By symmetry, we can assume that $v=v_p(a)\le v_p(b)$, so $m\ge v$, and dividing by p^{2v} we obtain $a_1^2-a_1b_1+b_1^2=p^{2m-2v}$ with $a_1=a/p^v$ and $b_1=b/p^v$. I first claim that $m=v$. Indeed, if $m>v$ we have in particular $a_1^2-a_1b_1+b_1^2\equiv 0\pmod{p}$. Since $v=v_p(a)$ we have $p\nmid a_1$, so also $p\nmid b_1$, so $((2a_1-b_1)/b_1)^2\equiv -3\pmod{p}$, in contradiction with the assumption that $p\equiv 2\pmod{3}$ since for such primes -3 is not a quadratic residue modulo p, and proving my claim. Thus $p^{2m-2v}=1$, so that $\varepsilon=a_1+b_1\rho$ is an algebraic integer of norm 1, in other words it is a unit in $\mathbb{Z}[\rho]$. Now by (2) of the above proposition we have $3\mid b$, so that $3\mid b_1$, and since the units of $\mathbb{Z}[\rho]$ are ±1, $\pm\rho$, and $\pm\rho^2=\mp(1+\rho)$, we must have $\varepsilon=\pm1$, so that $J(\chi,\chi)=a=\pm p^m$. Finally, again by (2) we know that $a\equiv -1\pmod{3}$, and since $p\equiv 2\pmod{3}$ we have $p^m\equiv(-1)^m\pmod{3}$, so the sign must be $(-1)^{m-1}$, proving the proposition. □

See Exercise 40.5 for a generalization of this result."

p. 86 line -4, replace "and 3.7.4" by "and 3.7.4, the latter being related to Proposition 2.5.20.5"

p. 99, between Exercises 40 and 41 insert the following exercise:

"40.5 Let $k\in\mathbb{Z}_{\ge3}$, let p be a prime not dividing k, assume that $q=p^{m\phi(k)}$ for some m, so that $q\equiv 1\pmod{k}$, and let χ be a character of order k on $\mathbb{F}_q$. Generalizing Proposition 2.5.20.5, show that under a suitable condition on p and k we have $J(\chi,\chi,\dots,\chi)=\pm q^{(k-2)/2}$ for some sign $\pm$, where χ is repeated $k-1$ times, and determine the sign."

p. 170 after the end of the proof of Theorem 3.6.38 insert the following:

"Although there exist more general or different reciprocity laws, Eisenstein's is one of the most useful; For instance, we will see that it implies Wieferich's criterion, see Section 6.9.6. Of course it immediately implies the quadratic reciprocity law, and also the *cubic* reciprocity law as follows:

Corollary 3.6.39 (Cubic Reciprocity). *If α and β are two primary and prime elements coprime to* 3 *and of coprime norm we have* $\left(\frac{\alpha}{\beta}\right)_3=\left(\frac{\beta}{\alpha}\right)_3$.

Proof. If $\alpha\in\mathbb{Z}$, in other words if α is a prime congruent to 2 modulo 3 this is nothing else than the theorem. Otherwise, let $p=\mathcal{N}(\alpha)=\alpha\overline{\alpha}$, where $\overline{}$ denotes complex conjugation in $\mathbb{Z}[\zeta_3]$. By the above theorem we have

$$\left(\frac{\alpha}{\beta}\right)_3\left(\frac{\overline{\alpha}}{\beta}\right)_3=\left(\frac{\beta}{\alpha}\right)_3\left(\frac{\beta}{\overline{\alpha}}\right)_3\ ,$$

in other words $f(\alpha,\beta)=f(\overline{\alpha},\beta)^{-1}$, where we have set

$$f(\alpha,\beta)=\left(\frac{\alpha}{\beta}\right)_3\left(\frac{\beta}{\alpha}\right)_3^{-1}\ .$$

Applying the equality of the theorem once again, using the antisymmetry of $f(\alpha,\beta)$ we obtain

$$f(\alpha,\overline{\beta})=f(\overline{\beta},\alpha)^{-1}=f(\beta,\alpha)=f(\alpha,\beta)^{-1}\ .$$

However, by definition or by Lemma 3.6.24 we have evidently $\left(\frac{\overline{\alpha}}{\overline{\beta}}\right)_m = \left(\frac{\alpha}{\beta}\right)_m^{-1}$, so in particular $f(\alpha,\overline{\beta}) = f(\overline{\alpha},\beta)^{-1} = f(\alpha,\beta)$ by the theorem. Thus $f(\alpha,\beta) = f(\alpha,\beta)^{-1}$, so $f(\alpha,\beta)=1$ since it is a cube root of unity, proving the corollary. □

As for all other reciprocity laws, to be able to apply cubic reciprocity we also need to compute $\left(\frac{\alpha}{\beta}\right)_3$ for the special cases not covered by the above corollary, the so-called *complementary laws*, and we give the result without its proof, which is not difficult.

Proposition 3.6.40. *Let $\alpha = -1 + 3(a + b\zeta_3)$ be a primary and prime element.*

1. *We have*
$$\left(\frac{\zeta_3}{\alpha}\right)_3 = \zeta_3^{a+b} \quad \text{and} \quad \left(\frac{1-\zeta_3}{\alpha}\right)_3 = \zeta_3^{2a}\ .$$

2. *If $\overline{\alpha}$ is coprime to α (in other words if the norm of α is a prime congruent to 1 modulo 3) we have*
$$\left(\frac{\alpha}{\overline{\alpha}}\right)_3 = \left(\frac{\overline{\alpha}}{\alpha}\right)_3 = 1\ .''$$

p. 276 between Exercises 5 and 6 insert the following exercise:

"5.5. Let a and b be elements of $\mathbb{Q}_3$ such that $v_3(a) = v_3(b) = 0$. Using Hensel's lemma, show that the equation $X^3 + 3aX^2 + b = 0$ has a solution in $\mathbb{Q}_3$ if and only if either $c \equiv 7 \pmod 9$, $c \equiv 50 \pmod{81}$, or $c \equiv 77 \pmod{81}$, where $c = b/a^3$."

p. 415 line 9, replace ". Then if t is squarefree but of any sign," by

", in both cases t having any sign. Then if either t is squarefree, or if no prime congruent to 3 modulo 4 divides b,"

p. 415 middle, replace "b and y. I claim" by "y and b, which is a contradiction if b is not divisible by primes congruent to 3 modulo 4, so we may assume that t is squarefree. I claim"

p. 415 line -9, replace "$\left(\frac{-1}{p}\right) = 1$." by "$\left(\frac{-1}{p}\right) = 1$, solving the first equation."

p. 416 line 1, replace "y_1 and b. I claim" by "y_1 and b, which is a contradiction if b is not divisible by primes congruent to 3 modulo 4, so we may assume that t is squarefree. I claim"

p. 416 between lines 5 and 6 add the following:

"A slightly more subtle result is the following.

Proposition 6.7.6.3. *Let a and b be nonzero integers such that $a \not\equiv 1 \pmod 3$, $3 \nmid b$, and 2 is a cubic residue modulo every prime $p \equiv 1 \pmod 3$ dividing a. The equation $y^2 = x^3 + t$ with $t = 2a^3 - 3b^2$ has no integral solution.*

Proof. Assume that x and y are integers such that $y^2 = x^3 + t$, in other words $z = y^2 + 3b^2 = x^3 + 2a^3$. I first claim that $3 \nmid z$. Indeed, otherwise $3 \mid y$, and since $3 \nmid b$ we have $z \equiv 3 \pmod{9}$. In particular $x \equiv a \pmod{3}$, so $z = x^3 + 2a^3 \equiv 3a^3 \pmod{9}$, hence $a \equiv a^3 \equiv 1 \pmod{3}$, in contradiction with the assumption. We can thus write

$$z = \prod_{p \equiv 1 \pmod{3}} p^{v_p} \prod_{q \equiv 2 \pmod{3}} q^{v_q} \;.$$

Since -3 is not a quadratic residue modulo $q \equiv 2 \pmod{3}$, v_q is even for each q. Furthermore, for each $p \equiv 1 \pmod{3}$ we can write $p = \pi\overline{\pi}$, where $\pi \in \mathbb{Z}_K$ (with $K = \mathbb{Q}(\sqrt{-3})$) is unique up to conjugation and multiplication by a unit of K. Now let $p \equiv 1 \pmod{3}$ be a prime dividing z. If $p \nmid a$ then $(-x/a)^3 \equiv 2 \pmod{p}$ so 2 is a cubic residue modulo p, and by assumption the same is true if $p \mid a$. By Proposition 2.5.20 this means that $p = \pi\overline{\pi}$, where $\pi = u + 3v\sqrt{-3}$, in other words $\pi \in R = \mathbb{Z}[3\sqrt{-3}]$, and of course we also have $\overline{\pi} \in R$. Thus, for any decomposition $z = \alpha\overline{\alpha}$ with $\alpha \in K$ then necessarily

$$\alpha = \pm\rho^j \prod_{p \equiv 1 \pmod{3}} \pi^{v_p} \prod_{q \equiv 2 \pmod{3}} q^{v_q/2}$$

for some unit $\pm\rho^j \in K$, in other words $\alpha = \rho^j(u + 3v\sqrt{-3})$ for some integers u and v and $j \in [-1, 1]$. Since $z = y^2 + 3b^2$, we may apply this to $\alpha = y + b\sqrt{-3}$. Since by assumption $3 \nmid b$ we cannot have $j = 0$. On the other hand, if $j = \pm 1$ then $\alpha = (-u \mp 9v + (\pm u - 3v)\sqrt{-3})/2$, and since y and b are integers we must have $u \equiv v \pmod{2}$. However this would imply that $z = \alpha\overline{\alpha} = u^2 + 27v^2 \equiv 0 \pmod{2}$. However since 2 is a prime congruent to 2 modulo 3 this means that $2 \mid y$ and $2 \mid b$, so $4 \mid z = x^3 + 2a^3$, hence $2 \mid x$, so $2 \mid a$, a contradiction since we assume that a and b are not both even, proving the proposition. □

A similar result is as follows.

Proposition 6.7.6.6. *Let a and b be integers such that $3 \nmid b$ and 3 is a cubic residue modulo every prime $p \equiv 1 \pmod{3}$ dividing a. Assume that either $t = 3a^3 - 27b^2$ and $3 \nmid a$, or that $t = 9a^3 - 27b^2$ and $a \equiv 2 \pmod{3}$. Then the equation $y^2 = x^3 + t$ has no integral solution.*

Proof. The proof is similar to the preceding one, but now using the cubic character of 3. Assume that x and y are integers such that $y^2 = x^3 + t$, in other words $z = y^2 + 27b^2 = x^3 + 3^k a^3$ with $k = 1$ or 2. I first claim that $3 \nmid z$. Indeed, otherwise $3 \mid x$ and $3 \mid y$. If $k = 1$, we deduce that $3 \mid a$, in contradiction with our assumption, and if $k = 2$ we deduce that $(y/3)^2 \equiv a^3 \equiv a \pmod{3}$, also a contradiction if $a \equiv 2 \pmod{3}$. As above if we set $\alpha = y + 3b\sqrt{-3}$ then $\alpha\overline{\alpha} = z$, and α is of the form

$$\alpha = \pm\rho^j \prod_{p \equiv 1 \pmod{3}} \pi^{v_p} \prod_{q \equiv 2 \pmod{3}} q^{v_q/2} \;,$$

where here we choose all the factors π of the form $(u + 3v\sqrt{-3})/2$, which are now unique up to conjugation. Since α is also of this form, it is clear that we must have $j = 0$. Now if $p \equiv 1 \pmod 3$ divides z, then either $p \nmid a$ in which case $(-x/a)^3 \equiv 3^k \pmod p$, which implies that 3 is a cubic residue modulo p since $3 \nmid k$, or $p \mid a$, in which case 3 is also a cubic residue by assumption. Since $3 = -\zeta_3(1 - \zeta_3)^2$, Proposition 3.6.40 implies that all the factors π are of the form $(u + 9w\sqrt{-3})/2$, so α is also of this form, in other words $3 \mid b$, contrary to our assumption." □

p. 416 line 8, replace "proposition solves" by "propositions solve"

p. 416 lines 10 and 11, replace "$t = -241$, ... $(t > 0)$." by

"$t = -246, -241, -240, -225, -201, -198, -192, -189, -171, -169, -132, -129, -117, -111, -99, -84, -75, -59, -50, -36, -24, -9$ (class number divisible by 3, t not squarefree, or $t \equiv 1 \pmod 8$)), 6, 7, 11, 13, 23, 39, 42, 45, 47, 51, 53, 58, 61, 67, 69, 83, 84, 87, 95, 103, 109, 123, 135, 139, 155, 157, 159, 165, 167, 175, 191, 202, 213, 215, 238, 239, 243, 247 $(t > 0)$. Of course this still leaves many values of t unresolved, such as $t = 14$ or $t = -31$, which can all be solved individually with no difficulty either by using Thue equations or elliptic curves; see Sections 12.10 and 8.7."

p. 420, just before Section 6.7.6 add the following:

" On the other hand, if we do not assume $H(t)$, and in particular if $t > 0$, little is known. For instance, we have the following conjecture:

Conjecture 6.6.13.5. *For $p \geq 3$ the equation $y^2 = x^p + 2$ does not have any integer solution.*

By solving Thue equations it is easy to show that this is true for small values of p, for instance for $p = 3$ and 5; see Exercise 42.5. Using techniques from transcendental number theory one can show that it is true for $p \geq p_0$ with an explicit value of p_0, but p_0 is so large that it is impossible in practice to test all smaller values of p."

p. 455 just before (5), insert the following:

"(4.5) Prove that for $p \geq 3$ the equation $y^2 = x^p + 2$ does not have any integer solution (Conjecture 6.6.13.5)."

p. 458 between Exercises 18 and 19 insert the following exercise:

"18.5. In the text we have considered in detail the representation of primes p as the sum of two rational cubes. In this exercise, we consider instead the representation of p as the sum of a rational cube and twice a rational cube, in other words the Diophantine equation $p = x^3 + 2y^3$ with x and y in $\mathbb{Q}$. Prove the following:

(a) If $p \equiv \pm 4 \pmod 9$ the equation has no solution.

(b) If $p \equiv 2$ or $8 \pmod 9$, then if we assume BSD the equation has a solution.

(c) If $p \equiv 1$ or $7 \pmod 9$ and $2^{(p-1)/3} \not\equiv 1 \pmod p$ the equation has no solution.

(d) If $p \equiv 1$ or $7 \pmod 9$ and $2^{(p-1)/3} \equiv 1 \pmod p$ the equation may or may not have solutions: using `mwrank`, give examples of both.

(e) If $p = 3$ the equation has infinitely many solutions, and give one where $x \notin \mathbb{Z}$ (recall that on the contrary the equation $2 = x^3 + y^3$ has the unique solution $(x, y) = (1, 1)$) .

(f) Solve the analogous exercise for the Diophantine equation $p = x^3 + 4y^3$."

p. 461 last line of Exercise 36, replace "find all the integral solutions to $y^2 = x^3 - 4$." by "find all the integral solutions to $y^2 = x^3 - 4$ and show that there are no integral solutions to $y^2 = x^5 - 4$".

p. 461 after Exercise 42 insert the following exercise:

"42.5. Using the Thue equation solver of `Pari/GP` (the functions `thueinit` and `thue`), show that the equations $y^2 = x^3 + 2$ and $y^2 = x^5 + 2$ do not have any integer solutions."

p. 462 between Exercises 47 and 48 insert the following exercise:

"47.5. Assume that $x^p + y^p + z^p = 0$ with $p \nmid xyz$ and x, y, and z pairwise coprime (in other words FLT I). We know that there exist integers a, b, and c such that $y + z = a^p$, $z + x = b^p$, and $x + y = c^p$ (see the proof of Proposition 6.9.6). Show in this order that $a^p \equiv -x^p \pmod{p^2}$, that $x+y+z \equiv 0 \pmod{p^2}$, and finally that $x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \equiv 1 \pmod{p^2}$. Note that this is a much easier but weaker version of Furtwängler's Theorem 6.9.9."

p. 421 lines 13 to 17, replace Corollary 6.7.15 and its proof by the following slightly more general statement:

Corollary 6.7.15 (Nagell). *Let $t \in \mathbb{Z}_{\geq 1}$ be squarefree and let $p \geq 3$ be a prime not dividing the class number of $\mathbb{Q}(\sqrt{-t})$. The equation $y^2+y+(t+1)/4 = tx^p$ has no integer solutions, except for $t = 3$, for which the only solutions are $(x, y) = (1, 1)$ and $(x, y) = (1, -2)$.*

Proof. This equation is equivalent to $(2y+1)^2+t = 4tx^p$, so that if a solution exists we have $t \equiv 3 \pmod 4$ and $t \mid (2y + 1)^2$. Since t is squarefree it follows that $t \mid (2y + 1)$, so setting $2y + 1 = tz$ we obtain $tz^2 + 1 = 4x^p$, and the result follows from the proposition. □

p. 610 between Exercises 16 and 17 insert the following exercise:

"16.5. Let $y^2 = x^3 + d(ax + b)^2$ be the equation of an elliptic curve E defined over $\mathbb{Q}$ having a rational subgroup of order 3.

(a) Show that E has an equation of the form $y^2 = x^3 + D(AX + B)^2$, where A and B are in $\mathbb{Z}$ and D is a fundamental discriminant (including 1).

(b) Show that E has (necessarily two opposite) rational 3-torsion points other than $\mathcal{O}$ if and only if either $D = 1$, in which case the points are $(0, \pm B)$, or if $D = -3$ and $2(9B + 4A^3) = T^3$ is the cube of $T \in \mathbb{Z}$, in which case the points are $(6B/(T - 2A), \pm 3BT/(T - 2A))$."

In Volume II:

p. 91, before Corollary 9.6.36, insert the following:

"One of the problems with defining $\Gamma(s)$ by the above formula is that it is valid only for $\Re(s) > 0$, and that one must extend it by the functional equation $\Gamma(s+1) = s\Gamma(s)$. The first formula of the following corollary avoids this problem, and in addition immediately gives the residues at negative integers:

Corollary 9.6.35.3. *For any $s \in \mathbb{C}$ and any $a > 0$ (in particular for $a = 1$) we have*

$$\begin{aligned}\Gamma(s) &= \int_a^\infty t^s e^{-t}\frac{dt}{t} + \sum_{n\ge0}(-1)^n\frac{a^{s+n}}{n!(s+n)}\\ &= \int_a^\infty t^s e^{-t}\frac{dt}{t} + e^{-a}\sum_{n\ge0}\frac{a^{s+n}}{s(s+1)\cdots(s+n)}\ .\end{aligned}$$

Proof. Assume first that $\Re(s) > 0$. By the proposition we have

$$\int_a^\infty t^s e^{-t}\frac{dt}{t} = \Gamma(s) - \int_0^a t^{s-1}e^{-t}\,dt = \Gamma(s) - \int_0^a \sum_{n\ge0}(-1)^n\frac{t^{s-1+n}}{n!}\ ,$$

and since the series converges normally on the compact interval $[0,a]$ we can integrate term by term, giving the first formula. For the second, by integration by parts we have

$$\int_0^a t^{s-1}e^{-t}\,dt = \frac{t^s}{s}e^{-t}\Big|_0^a + \frac{1}{s}\int_0^a t^s e^{-t}\,dt = e^{-a}\frac{a^s}{s} + \frac{1}{s}\int_0^a t^s e^{-t}\,dt\ ,$$

so by induction we obtain

$$\int_0^a t^{s-1}e^{-t}\,dt = e^{-a}\sum_{n=0}^N \frac{a^{s+n}}{s(s+1)\cdots(s+n)} + \frac{I(N)}{s(s+1)\cdots(s+N)}\ ,$$

with $I(N) = \int_0^a t^{s+N}e^{-t}\,dt$. Since clearly $|I(N)| < a^{s+N+1}/(s+N+1)$, and since $a^{s+N}/(s(s+1)\cdots(s+N))$ tends to 0 as N tends to infinity, we deduce that

$$\int_0^a t^{s-1}e^{-t}\,dt = e^{-a}\sum_{n\ge0}\frac{a^{s+n}}{s(s+1)\cdots(s+n)}\ ,$$

proving the second formula when $\Re(s) > 0$. Since $a > 0$, the right hand sides are clearly meromorphic functions on all of $\mathbb{C}$ with poles on $\mathbb{Z}_{\le0}$, so these formulas are valid in general by uniqueness of meromorphic continuation. Alternatively, it is easy to show that the right hand sides satisfy the functional equation of the gamma function. Note that the equality

$$\sum_{n\ge0}(-1)^n\frac{a^{s+n}}{n!(s+n)} = e^{-a}\sum_{n\ge0}\frac{a^{s+n}}{s(s+1)\cdots(s+n)}$$

is an easy combinatorial exercise; see Exercise 75.3. □

Corollary 9.6.35.6. *For any $x > 0$ and $a > 0$ (in particular for $x = a = 1$) we have*

$$\gamma = -\int_0^\infty e^{-t}\log(t)\,dt = \int_0^a \frac{1-e^{-xt}}{t}\,dt - \int_a^\infty \frac{e^{-xt}}{t}\,dt - \log(ax)\ .$$

Proof. By normal convergence on compact subsets of $]0,\infty[$ we can differentiate the formula of the proposition. Setting $s = 1$ and using $\Gamma'(1) = -\gamma$ gives the first formula. For the second, for $X > 0$ we write

$$\begin{aligned}\int_0^\infty e^{-t}\log(t)\,dt &= \int_0^X e^{-t}\log(t)\,dt + \int_X^\infty e^{-t}\log(t)\,dt\\ &= (1-e^{-t})\log(t)\Big|_0^X - \int_0^X \frac{1-e^{-t}}{t}\,dt - e^{-t}\log(t)\Big|_X^\infty + \int_X^\infty \frac{e^{-t}}{t}\,dt\\ &= \log(X) - \int_0^X \frac{1-e^{-t}}{t}\,dt + \int_X^\infty \frac{e^{-t}}{t}\,dt\ ,\end{aligned}$$

proving the second formula after replacing X by ax and changing t into t/a. □

"

p. 93, just before Proposition 9.6.39, replace "A direct classical ... 95" by the following:

"**Remarks.**

1. A direct classical proof of the first formula is given in Exercise 95.
2. It is easy to give a unified formula including both Corollary 9.6.35.6 and the above proposition; see Exercise 75.6."

p. 132 between Exercises 52 and 53 insert the following exercise:

"52.5. For this exercise it may be necessary to use Corollary 11.4.2. Let χ be a primitive character of conductor f with $4 \mid f$.

(a) With the notation of Section 9.4.2, show that $B_k(\chi, \{f/2\}_\chi) = -B_k(\chi)$.

(b) Deduce that if f is not a power of 2, we have

$$\sum_{0\le r<f/2} \chi(r)r^k \equiv -2\frac{B_{k+1}(\chi)}{k+1} \pmod{f}\ .$$

(c) By what must this be replaced if f is a power of 2?

(d) Show that the above results imply Corollary 9.5.10."

p. 136 between Exercises 75 and 76 insert the following exercises:

"75.3. This is a complement to the proof of Corollary 9.6.35.3.

(a) Prove directly that

$$f(s)=\sum_{n\ge0}(-1)^n\frac{a^{s+n}}{n!(s+n)}+\int_a^\infty t^se^{-t}\frac{dt}{t}$$

satisfies the functional equation $f(s+1)=sf(s)$.

(b) By expanding $1/(s(s+1)\cdots(s+n))$ into partial fractions, show that

$$\sum_{n\ge0}(-1)^n\frac{a^{s+n}}{n!(s+n)}=e^{-a}\sum_{n\ge0}\frac{a^{s+n}}{s(s+1)\cdots(s+n)}\ .$$

75.6.

(a) Show that Corollary 9.6.35.6 is still valid for $x\in\mathbb{C}^*$ with $\Re(x)\ge0$ (and $a>0$), with the principal determination of the logarithm.

(b) Deduce that for $a>0$, $x\ge0$, and $y\in\mathbb{R}$ with $(x,y)\ne(0,0)$ we have

$$\int_0^a\frac{1-e^{-xt}\cos(yt)}{t}\,dt-\int_a^\infty\frac{e^{-xt}\cos(yt)}{t}\,dt=\gamma+\log(a)+\frac{1}{2}\log(x^2+y^2)$$

and

$$\int_0^\infty\frac{e^{-xt}\sin(yt)}{t}\,dt=\operatorname{atan}\left(\frac{y}{x}\right)\ ,$$

where $\operatorname{atan}(y/0)$ is to be interpreted as $(\pi/2)\operatorname{sign}(y)$."

p. 147 in Exercise 105 (f) and (g), add at the appropriate places

$$I(2,4)=\frac{261}{8}\pi\zeta(6)+3\pi\zeta(3)^2=\frac{29}{840}\pi^7+3\pi\zeta(3)^2\ ,$$

$$I(3,4)=\frac{1935}{64}\pi^2\zeta(6)+\frac{9}{2}\pi^2\zeta(3)^2=\frac{43}{1344}\pi^8+\frac{9}{2}\pi^2\zeta(3)^2\ ,$$

and at the end of Exercise 105, add the following:

"More generally, one can give an explicit finite formula expressing $I(a,b)$ as a polynomial in π and the $\zeta(k)$ for $k\in\mathbb{Z}_{\ge2}$."

p. 207 lines -3 and -2, replace "In fact, it can...instance" by

"In fact, it is easy to see that the γ_m may be exponentially large; see Exercise 50.5. For instance"

p. 261 after Exercise 21, add the following exercise:

"21.5. Set

$$S=\sum_{n\ge1}e^{-(n/10)^2}\ .$$

(a) By a direct computation (the series converging very quickly), show that at least to 100 decimals of accuracy we have $S \approx 5\sqrt{\pi} - 1/2$. By computing to 500 decimals, show however that we do not have exact equality.

(b) Using the functional equation of the theta function, explain why $S - (5\sqrt{\pi} - 1/2)$ is so small, and give a very precise estimate for it."

p. 261 after Exercise 24, add the following exercises:

"24.3. Let $m \in \mathbb{Z}_{\geq 3}$, and let χ be a not necessarily primitive odd character modulo m, in other words such that $\chi(-1) = -1$.

(a) Show that

$$L(\chi, 1) = \frac{i\pi}{m^2} \sum_{r=1}^{m-1} r\tau(\chi, r) ,$$

where as usual $\tau(\chi, r) = \sum_{x \bmod m} \chi(x) \exp(2i\pi r/m)$. Since, when χ is primitive, we have by Corollary 2.1.42

$$\tau(\chi, r) = \overline{\chi}(r)\tau(\chi) = \overline{\chi}(r) i m^{1/2} W(\chi) ,$$

this generalizes Corollary 10.3.2.

(b) Deduce that

$$L(\chi, 1) = \frac{i\pi}{m} \sum_{a \bmod m} \frac{\chi(a)}{\zeta_m^a - 1} = \frac{\pi}{2m} \sum_{a \bmod m} \chi(a) \operatorname{cotan}\left(\frac{a\pi}{m}\right) ,$$

where as usual ζ_m denotes a primitive mth root of unity in $\mathbb{C}$.

24.6. Let $m \in \mathbb{Z}_{\geq 3}$, and recall that there are $\phi(m)/2$ odd characters modulo m.

(a) Let $r \in \mathbb{Z}$. Show that

$$\sum_{\chi(-1)=-1} \chi(r) = \begin{cases} 0 & \text{if } r \not\equiv \pm 1 \pmod{m} \\ \pm\dfrac{\phi(m)}{2} & \text{if } r \equiv \pm 1 \pmod{m} , \end{cases}$$

where the sum is over all odd characters modulo m (this is easy but not completely trivial).

(b) Using for instance the preceding exercise, show that the average of $L(\chi, 1)$ over all odd characters modulo m is equal to

$$\frac{\pi}{m} \operatorname{cotan}\left(\frac{\pi}{m}\right) = 1 - \frac{\pi^2}{3m^2} + O\left(\frac{1}{m^4}\right) .$$

(c) By computing in two different ways the sum of the squares of the roots of the polynomial $(x+i)^m-(x-i)^m$, show that

$$\sum_{1\le a\le m-1}\operatorname{cotan}^2\left(\frac{a\pi}{m}\right)=\frac{(m-1)(m-2)}{3}\ .$$

(d) Deduce that the average of $|L(\chi,1)|^2$ over all odd characters modulo m is equal to

$$\frac{\pi^2}{6}\prod_{p\mid m}\left(1-\frac{1}{p^2}\right)-\frac{\pi^2\phi(m)}{2m^2}\ .$$

Compare the results of (b) and (d) with those of Proposition 10.3.17."

p. 261 after Exercise 25, add the following exercise:

"25.5. Denote as usual by χ_{-3} the quadratic character $\left(\frac{-3}{.}\right)$.

(a) Show that

$$L'(\chi_{-3},-1)=\frac{3^{3/2}}{4\pi}L(\chi_{-3},2)\ .$$

(b) In relation with Wendt's criterion for FLT I (Proposition 6.9.6), denote by R_k the resultant of the polynomials X^k-1 and $(X+1)^k-1$. Show that when $k\equiv\pm 2\pmod 6$ (which is the domain of applicability of the criterion) we have as $k\to\infty$

$$R_k\sim -3^{1/2}\exp(L'(\chi_{-3},-1)k^2)\ ."$$

p. 262 at the end of Exercise 28, replace "." by "; see also [Lag-Suz].", and in the bibliography of both volumes, at the appropriate place add:

"[Lag-Suz] J. Lagarias and M. Suzuki, *The Riemann hypothesis for certain integrals of Eisenstein series*, J. Number Theory **118** (2006), 98–122."

p. 265 after question (f), add the following additional question:

"(g) Deduce that

$$\Omega_4=\frac{B(1/4,1/2)}{2}=\frac{\Gamma(1/4)^2}{2(2\pi)^{1/2}}\quad\text{and}\quad\Omega_6=\frac{B(1/6,1/3)}{2}=\frac{\Gamma(1/3)^3 3^{1/2}}{2^{4/3}\pi}\ ,$$

where B is the beta function."

p. 267 at the end of Exercise 43, replace "(note that... $\log(4e/(3\pi))$)" by the following additional question:

"(c) Using Euler–MacLaurin instead of (a), show that one can improve the constant $\log(4e/(3\pi))=0.14295...$ to $\gamma-\log(\pi/2)=0.12563...$, and show also that

$$\sum_{n=1}^{m-1}\frac{1}{\sin(\pi n/m)}=\frac{2}{\pi}(m\log(m)+(\gamma-\log(\pi/2))m)-\frac{\pi}{36m}+O\left(\frac{1}{m^3}\right)\ .''$$

p. 269 between Exercises 50 and 51, add the following exercise:

"50.5.

1. Using the functional equation, show that there cannot exist a constant $C > 0$ such that $\zeta(s) - 1/(s-1) = O(e^{Cs})$.
2. Deduce from this that the γ_m can be exponentially large, more precisely, for any fixed $c \neq 0$ the sequence $|\gamma_m/c^m|$ is unbounded."

p. 271 Exercise 60 (b), replace the formula "$L(4+\sqrt{15}) =$..." by

$$\begin{aligned}
L(4+\sqrt{15}) &= \log(2)\log(\sqrt{3}+\sqrt{5}) + \log((1+\sqrt{5})/2)\log(2+\sqrt{3}) \\
&\quad + \frac{\pi^2}{2} - \frac{\pi^2}{12}(4+\sqrt{15})\ , \\
L(6+\sqrt{35}) &= \log(2)\log(\sqrt{5}+\sqrt{7}) + \log((1+\sqrt{5})/2)\log(8+3\sqrt{7}) \\
&\quad + \frac{3\pi^2}{4} - \frac{\pi^2}{12}(6+\sqrt{35})\ , \text{ and} \\
L(12+\sqrt{143}) &= \log(2)\log(\sqrt{11}+\sqrt{13}) + \log((3+\sqrt{13})/2)\log(10+3\sqrt{11}) \\
&\quad + \frac{3\pi^2}{2} - \frac{\pi^2}{12}(12+\sqrt{143})
\end{aligned}$$

p. 398 between Exercises 9 and 10, add the following exercise:

"9.5. For this exercise, you will need to use the results of Section 11.4.2. Let p be an odd prime, let ω be the Teichmüller character modulo p, and as usual set $S_k(\omega) = \sum_{1\le a\le p-1}\omega(a)a^k$ with $k \ge 0$.

(a) Prove that, modulo $p^2\mathbb{Z}_p$, when k is even we have

$$S_{k-1}(\omega) \equiv p\left(1-\frac{1}{k}\right)B_k + \begin{cases} 0 & \text{if } (p-1)\nmid k \\ \dfrac{p-1}{k} & \text{if } (p-1)\mid k \text{ and } p>3 \\ \dfrac{p-1}{k} + 3(k+2)^2 & \text{if } p=3\ , \end{cases}$$

while when k is odd

$$S_{k-1}(\omega) \equiv \begin{cases} 0 & \text{if } (p-1)\nmid(k-1) \\ -\dfrac{p(k-1)}{2} & \text{if } (p-1)\mid(k-1)\ . \end{cases}$$

In particular, if $p > k+1$ we have

$$S_{k-1}(\omega) \equiv p\left(1-\frac{1}{k}\right)B_k \pmod{p^2\mathbb{Z}_p}\ .$$

(b) Deduce that if we set

$$L_k = \sum_{1\le a\le p-1} a^k \log_p(a)$$

then when k is even we have

$$L_k \equiv \frac{p}{k}B_k - \begin{cases} 0 & \text{if } (p-1) \nmid k \\ \dfrac{p-1}{k} & \text{if } (p-1) \mid k \text{ and } p > 3 \\ \dfrac{p-1}{k} + 3(k+2)^2 & \text{if } p = 3 \end{cases} \pmod{p^2\mathbb{Z}_p}\ ,$$

while when k is odd we have

$$L_k \equiv \begin{cases} 0 & \text{if } (p-1) \nmid (k-1) \\ -\dfrac{p}{2} & \text{if } (p-1) \mid (k-1) \end{cases} \pmod{p^2\mathbb{Z}_p}\ .$$

(c) Deduce that if $p > k+1$ (and also for some smaller p) then

$$L'_p(\omega^k, 1-k) \equiv 0 \pmod{p\mathbb{Z}_p}\ .$$

(d) Generalize to $\sum^{(p)}_{0 \le a < p^N} a^{k-1}\omega^j(a)$ and to $L'_p(\chi\omega^k, 1-k)$ for suitable characters χ."

p. 398 between Exercises 10 and 11, add the following exercises (or add the statements in the main text):

"10.3. Let p be an odd prime and $v \geq 2$. Show that the number of primitive p-adically wild characters of conductor p^v is equal to $(p-1)p^{v-2}$, and that they are all even characters.

10.6.

(a) Show that the statements of Corollary 11.3.20 (1) and (2) can be made more precise as follows:

For $n \geq 2$ we have $T_n(\chi) \equiv 0 \pmod{pm\mathcal{Z}_p}$, except when $n = 2$ and χ is p-adically wild, in which case $T_n(\chi) \equiv pm\chi(1+p)/(1-\chi(1+p))^2 \pmod{pm\mathcal{Z}_p}$, and when $n = p = 3$ and χ is one of the two 3-adically wild characters of conductor 9, in which case $T_n(\chi) \equiv pm/(\chi(1+p)(\chi(1+p)-1)) \pmod{pm\mathcal{Z}_p}$.

(b) Deduce in particular that Theorem 11.3.21 (1) can be replaced by:

For $j \geq 2$ we have $p \mid a_j$ (in other words $|a_j/p| \leq 1$), except if $j = 2$, $p = 3$, and χ is one of the two 3-adically wild characters of conductor 9, in which case we have only $|a_2| \leq 1$."

Add in the index of notation:
"$\delta(\chi)$: 0 if $\chi \neq \chi_0$, 1 if $\chi = \chi_0$", referenced on p. 293 of Volume II
Add in the general index:
"Clausen–von Staudt congruence", referenced on p. 63 of Volume II
In the bibliography, for the entry [Gra-Sou], replace ", to appear" by
" **20** (2007), 357–384"