UPDATES FOR "NUMBER THEORY AND GEOMETRY"

Dear Readers,

Here is a list of updates (known typos, errors and omissions, expanded paragraphs, etc.), with the text as it appeared in the first edition, followed by the corrected text (as it will/should appear in a revised edition).

Acknowledgements: I'd like to thank Mia Campbell, Keith Conrad, Giacomo De Leva, Fernando Gouvêa, Tom Roby, Jeremy Rouse, Hanson Smith, Guohua Wen, and Cindy Zhang for identifying a number of typos and errors listed below.

(1) **Page 10. Example 1.3.2.** There is an issue with the paragraph that starts with "In particular, $3r = 0, 3, 6$, or 12." The issue is that the statement "Hence, $(mb)^2 = 7((na)^2 + 3k)$, or $A^2 = 7B^2$, where $A = mb$ and $B = (na)^2 + 3k$ are integers." is not true.

The argument can be finished in a different way. In the previous paragraph we have reached $(mb)^2 = 3(ab)^2 + 7(na)^2$, so let us show that the equation $A^2 = 3B^2 + 7C^2$ only has one integral solution, namely $A = B = C = 0$. Suppose $A^2 = 3B^2 + 7C^2$ for $A, B, C \in \mathbb{Z}$, and choose solutions A, B, C smallest in absolute value. Then, A^2 and $3B^2$ have the same remainder when divided by 7. Previously we have seen that a square (so A^2 and B^2) can only have remainder of $0, 1, 2$, or 4. Thus the remainder of A^2 is $0, 1, 2$, or 4, and the remainder of $3B^2$ is $0, 3, 6$, or 12 (which would mean a reminder of 5). Since the remainders of A^2 and $3B^2$ must coincide, we have that the remainder must be 0, i.e., A^2 and $3B^2$ are divisible by 7. Hence, $A = 7A'$ and $B = 7B'$ and we obtain

$$7^2 A'^2 = 3 \cdot 7^2 \cdot B'^2 + 7C^2.$$

It follows that 7^2 is a divisor of $7C^2$, and therefore C is divisible by 7, say $C = 7C'$. It follows that

$$A'^2 = 3B'^2 + 7C'^2$$

and the solutions A', B', C' would be smaller than A, B, C in absolute value (which contradicts our choice of A, B, C) unless $A = B = C = 0$, as desired.

(2) **Page 11. Example 1.4.1.** The line L is $y = x + 1$.

- (**Old text**) With a little bit of basic plane geometry, we find an equation for $L : y = x - 1$ (see Exercise 1.8.8).

- (**New text**) With a little bit of basic plane geometry, we find an equation for $L : y = x + 1$ (see Exercise 1.8.8).

(3) **Page 12. Example 1.4.2.** The numbers 383/1000 and −383/1000 are mixed up.

- (**Old text**) ... and their y-coordinates are 5 and $-\frac{383}{100}$, respectively. Hence, we have found a new *rational* point on E', namely $Q = (\frac{129}{100}, -\frac{383}{100})$. By symmetry of the graph of E' with respect to the y-axis, there is an additional point $Q' = (\frac{129}{100}, \frac{383}{100})$.

- (**New text**) ... and their y-coordinates are 5 and $\frac{383}{100}$, respectively. Hence, we have found a new *rational* point on E', namely $Q = (\frac{129}{100}, \frac{383}{100})$. By symmetry of the graph of E' with respect to the y-axis, there is an additional point $Q' = (\frac{129}{100}, -\frac{383}{100})$.

(4) **Page 24. Exercise 1.8.6.** In part (3), it should specify that the result is for a non-zero complex number α.

- (**Old text**) Show that any complex number α can be written uniquely as...

- (**New text**) Show that any non-zero complex number α can be written uniquely as...

(5) **Page 38. Proof of Theorem 2.3.14.** There are a couple of issues with the second paragraph of the proof, which should read like this instead:

- (**New text**) Next, let us show the induction step. Let us assume that the theorem is true for sets with more than k elements, and let S be a set with more than $k + 1$ elements. Let $S_1, S_2, \ldots, S_k, S_{k+1}$ be $k + 1$ subsets of S, such that $\bigcup_{i=1}^{k+1} S_i = S$. If the set S_{k+1} has more than one element, then we are done. Otherwise, suppose that S_{k+1} contains only one element of S, or $S_{k+1} = \emptyset$. Then, the union $S' = \bigcup_{i=1}^{k} S_i$ contains at least $k + 1$ elements (since S contains $k + 2$ elements, and the missing subset S_{k+1} contains ≤ 1 elements, so S' contains $\geq k + 2 - 1 = k + 1$ elements). Hence, using our induction hypothesis on the set S', we conclude that one of $S_1, \ldots, S_k$ contains at least two elements.

(6) **Page 40. Line 5**

- (**Old text**) Since $r \in S$, there must be...

- (**New text**) Since $r_1 \in S$, there must be...

(7) **Page 71. Theorem 3.3.11**
- (**Old text**) Let $m > 0$ and $a \geq 0$ be fixed integers...
- (**New text**) Let $m > 0$ and $a > 0$ be fixed integers...

(8) **Page 74. Definition 3.4.5** The statement should be for $k \geq 1$.
- (**Old text**) Let $k \geq 0$,...
- (**New text**) Let $k \geq 1$,...

(9) **Page 74. Conjecture 3.4.7** The statement should be for $k \geq 1$.
- (**Old text**) Let $k \geq 0$ be an integer,...
- (**New text**) Let $k \geq 1$ be an integer,...

(10) **Page 75. Conjecture 3.4.10.** The statement of the Bateman-Horn conjecture needs two additional assumptions:
- Each factor $f_i(x)$ should have a positive leading coefficient, i.e., if $f_i(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then $a_n \geq 1$.
- The values of $f(x)$ on $\mathbb{Z}$ must not all share a common prime factor.

(11) **Page 77.** In the displayed formula with a limit, there should be # symbols outside of the brackets to indicate "cardinality of."
- (**Old text**)

$$\lim_{x\to\infty} \frac{\{2n \in \mathbb{N} : 2n \leq x \text{ and } 2n = p + q \text{ for some prime numbers } p, q\}}{\{2n \in \mathbb{N} : 2n \leq x\}} = 1.$$

- (**New text**)

$$\lim_{x\to\infty} \frac{\#\{2n \in \mathbb{N} : 2n \leq x \text{ and } 2n = p + q \text{ for some prime numbers } p, q\}}{\#\{2n \in \mathbb{N} : 2n \leq x\}} = 1.$$

(12) **Page 80. Exercise 3.5.15.** The statement is not true for $n = 1$ so the exercise is to prove it for $n \geq 2$.
- (**Old text**) ... then $p_{n+2} < p_n + p_{n+1}$, for all $n \geq 1$.
- (**New text**) ... then $p_{n+2} < p_n + p_{n+1}$, for all $n \geq 2$.

(13) **Page 80. Exercise 3.5.20.** $k \geq 1$.
- (**Old text**) ... then there is some $k \geq 0$ such that...
- (**New text**) ... then there is some $k \geq 1$ such that...

(14) **Page 81. Exercise 3.5.22**
- (**Old text**) Show that if $a > 0$ and...
- (**New text**) Show that if $a > 1$ and ...

(15) **Page 114. Exercise 4.7.26**
- (**Old text**) ...let $k \in \mathbb{Z}$ such that $1 \leq k \leq p$...
- (**New text**) ...let $k \in \mathbb{Z}$ such that $1 \leq k < p$...

(16) **Page 150. Exercise 5.6.6 part (3)**
- (**Old text**) (Hint: if $a * H$ and $b * H$ are two...
- (**New text**) (Hint: if $g_1 * H$ and $g_2 * H$ are two...

(17) **Page 183.** In the first line of the second paragraph a "u" should be a "v."
- (**Old text**) Also, let $(u \bmod m, u \bmod n)$ be an arbitrary pair...
- (**New text**) Also, let $(u \bmod m, v \bmod n)$ be an arbitrary pair...

(18) **Page 231. Exercise 8.10.10 part (b)**
- (**Old text**) ..., then $p = 2$ and $a = 1$.
- (**New text**) ..., then $p = 2$ and $a \equiv 1 \bmod 2$.

(19) **Page 254. Corollary 9.2.12.** There is a typo (a minus sign is missing) in the formula for φ in part (b).
- (**Old text**) $\varphi(x, y) = (2ax + by + d, (4ae - 2bd)y + 4af - d^2)$,
- (**New text**) $\varphi(x, y) = (2ax + by + d, -(4ae - 2bd)y - (4af - d^2))$,

(20) **Page 262. Theorem 9.4.3.** There is a typos in the formulas in part (2).
- (**Old text**) The congruence
$$be'K^2 + (2bn_1 - e')K + bt + d - n_1 \equiv 0 \bmod 2a,$$
has a solution $K \equiv k_1 \bmod 2a$, where $t = (n_1^2 - f')/e'$.
- (**New text**)The congruence
$$be'K^2 + (e' - 2bn_1)K + bt - d + n_1 \equiv 0 \bmod 2a,$$
has a solution $K \equiv k_1 \bmod 2a$, where $t = (n_1^2 + f')/e'$.

(21) **Page 277. Example 10.2.6.** The table is missing the prime 19. The number -1 is a QNR (quadratic non-residue) for $p = 19$, so the table should reflect that, as follows

p	3	5	7	11	13	17	19	23	29	31	37	41
$\sqrt{-1}$	QNR	± 2	QNR	QNR	± 5	± 4	QNR	QNR	± 12	QNR	± 6	± 9

(22) **Page 388. Corollary 13.3.4.** In part (2) of the statement, d should be t.

- (**Old text**) If $|\alpha - s/t| < |\alpha - p_k/q_k|$ for some $k \geq 1$, then $d > q_k$.
- (**New text**) If $|\alpha - s/t| < |\alpha - p_k/q_k|$ for some $k \geq 1$, then $t > q_k$.

(23) **Page 391. Exercise 13.4.14.** Here e should also be d, because otherwise $\overline{\alpha + \beta}$ is not defined with the definition we have given for conjugation in the statement.

- (**Old text**) ... $\alpha = u + v\sqrt{d}$ and $\beta = x + y\sqrt{e}$, where $u, v, x, y \in \mathbb{Q}$ and d, e are non-zero integers that are not perfect squares.
- (**New text**) ... $\alpha = u + v\sqrt{d}$ and $\beta = x + y\sqrt{d}$, where $u, v, x, y \in \mathbb{Q}$.

(24) **Page 391. Exercise 13.4.20.** Here d should be $n^2 + 2n$.

- (**Old text**) Let d be a positive integer such that $d = n^2+1$, for some integer $n > 1$.
- (**New text**) Let d be a positive integer such that $d = n^2 + 2n$, for some integer $n > 1$.

(25) **Page 407. Proof of 14.3.17.** A $+$ should be a $\cdot$ in the last line of the previous to last displayed equation, because they are elements living in the group $U = (U, \cdot)$ where the operation is multiplication.

- (**Old text**) $\psi((a \bmod 2, n)) + \psi((b \bmod 2, m))$.
- (**New text**) $\psi((a \bmod 2, n)) \cdot \psi((b \bmod 2, m))$.