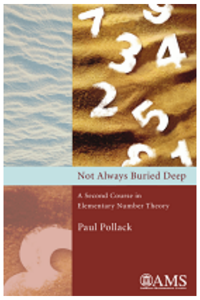

Not always buried deep

Lies, Damned Lies, and Typos (Errata)
Last updated: July 27, 2020

p. 4, line below the first displayed equation: Replace "$2^i \mid (\mathbf{Z}/p\mathbf{Z})^\times$" with "$2^i \mid \#(\mathbf{Z}/p\mathbf{Z})^\times$".

p. 8, Hacks's proof: The reference to the transcendence of π was a bit glib. Replace the last sentence of the proof with the following:

> The known proofs of the transcendence of π rely fairly explicitly on the infinitude of primes, so it is somewhat dangerous to appeal to this result directly. However, a weaker result which does not rely in an obvious way on this fact, and which nevertheless suffices for the current application, appears as Exercise 6 (cf. [**AZ04**, Chapter 6, Theorem 2]).

p. 17, first display: The first strict inequality should be non-strict, i.e., should read $\frac{4A-1}{4} \geq \frac{7}{4}$.

p. 17, next-to-last centered equation: "$N(\alpha)$" should be "$\mathcal{N}(\alpha)$".

p. 20, Figure 3: The slope of line e_2 is a bit off; e_2 should be the reflection of e_1 about the y-axis.

p. 22, Theorem 1.15: This result should be starred, since it is not proved in the text.

p. 25, line below (1.12): The degree condition should read "$\deg R < \deg G$".

p. 26, Theorems 1.21 and 1.22: The way Theorem 1.21 is currently stated, $F = \Phi_m$ always satisfies the conclusion. Before the final sentence, one should add: "Conversely, p is a prime divisor of F whenever $p \bmod m \in H$."

Theorem 1.22 should have the extra condition on F that infinitely many prime divisors p of F satisfy $p \equiv a \pmod{m}$.

p. 28, last line: It is claimed that Iwaniec's result (that $n^2 + 1$ is infinitely often a product of at most two primes) applies to every quadratic polynomial satisfying the conditions of

Hypothesis H. This was actually not established by Iwaniec, but it is true, as shown a few decades later by Lemke Oliver.

p. 30, first full paragraph: The claim that we know no even number $a > 1$ for which $a^{2^n} + 1$ is infinitely often composite is false; e.g., if $a = 8$, then

$$8^{2^n} + 1 = (2^{2^n} + 1)(2^{2^{n+1}} - 2^{2^n} + 1).$$

More generally, whenever a is a kth power for some odd $k > 1$, there is an analogous algebraic factorization. The correct claim is that no *other* such a are proved to have the stated property.

p. 43, hint to Ex. 35: Delete "with respect to the same prime".

p. 55, eq. (2.4): The first group of terms should read

$$\zeta^{g^0} + \zeta^{g^2} + \cdots + \zeta^{g^{p-3}};$$

in other words, the final term $\zeta^{g^{p-1}}$ should not be there.

p. 58, penultimate step in (2.5): Replace the summand "ζ^e" with "ζ^u".
In the second line of the next display: delete the 1 from the parenthesized expression "$1 + \zeta + \cdots + \zeta^{p-1}$".

p. 60, last two line: End the last display with a period (not a comma). Replace the last line with of the proof with "By Lemma 2.17, $0 \equiv j \pmod e$. But this contradicts our choice of j."

p. 62, proof of Theorem 2.18: Right below "we have," the expansion of η_0 should only go to $\zeta^{g^{p-3}}$, not $\zeta^{g^{p-1}}$.

p. 65, proof of Lemma 2.24: In the displayed equation, replace the condition of summation "$\alpha \in \mathbf{F}_p \setminus \{0, 1\}$" with "$\alpha \in \mathbf{F}_p \setminus \{0, -1\}$".

p. 69, first two words: The reference should be to Theorem 2.26, not Theorem 7.5.

p. 83, Exercise 13: The condition on p should be that the order of $2 \pmod p$ is not divisible by 3, **not** the order of $3 \pmod p$.

p. 83, Exercise 14: In the first sentence, replace the conditions on p and q with "$q = 4n+1$ and $p = 24n + 7$". Throughout the problem, replace "$q \mid 2^p - 1$" with "$p \mid 2^q - 1$".

p. 87, Table: There are 455,052,511 primes up to 10^{10}, not 455,052,512.

p. 91, Lemma 3.9: We prove that "$\sum_{d|n} \Lambda(d) = \log n$", not "$\sum_{d|n} \Lambda(n) = \log n$".

p. 108, Exercise 12(a): There is a "p" missing from the inside of the product.

p. 116, Exercise 34: The "$O(1/n)$" in the claim should be should be "$O(1/n^2)$". In other words, you should show that $\prod_{\deg P \le n}(1-1/|P|) = e^{-\gamma}/n + O(1/n^2)$.

p. 127, Theorem 4.2: In (4.16), the condition "$\chi = \psi^{-1}$" should read "$\chi = \psi$".

p. 143, Exercise 9: In (b), the term $\frac{1}{\phi(q)}$ in the displayed equation should be $\frac{1}{\phi(m)}$. The left-hand sum should be over $p \le x$ with $p \equiv a \pmod{m}$.

p. 145, remark to Exercise 17: Remove the words "infinitely many" from the description of the Deshouillers–Iwaniec theorem.

p. 146, Exercise 21(d): Insert absolute value signs around the sum in the statement of the Pólya–Vinogradov inequality.

p. 147, remark: The result of Graham and Ringrose is that the least quadratic nonresidue modulo p is infinitely often $\gg (\log p)(\log\log\log p)$. The text incorrectly has $\log p \log\log p$.

p. 173, equation (6.21): Replace $2^{\log z}$ with $2^{\log x}$.

p. 180, remark: Replace "sum of the twin prime pairs past 10^{16}" with "sum over the twin prime pairs past 10^{16}".

p. 223, equations (7.18): Change "$\sum_{ab=n}\mu(a)(\sum_{d|b}\Lambda(b))^2$" to "$\sum_{ab=n}\mu(a)(\sum_{d|b}\Lambda(d))^2$".

p. 237, Exercise 3: The definition of $F(s)$ in part (a) should read $F(s) := (-1)^k(P^{(k)}(s) + \zeta^{(k-1)}(s))$. (In other words, the "$-$" sign should be a "$+$" sign.)

p. 257, final paragraph: Replace "number $(\log x)$-smooth" with "number of $(\log x)$-smooth".

p. 258, end of proof of Theorem 8.4: Delete one occurrence of "most" in "number of perfect numbers $\le x$ is at most most $x^{W/\log\log x}$".

Five lines from the bottom: "Supposing that p^e does exactly divide m^2" should read "Supposing that p^e does exactly divide $\sigma(m^2)$".

p. 264, bottom of the proof of Lemma 8.19: Replace "the primes $p_1, \dots, p_{K+1}$ satisfy (8.15) ..." with "the primes $p_0, \dots, p_{K+1}$ satisfy (8.15) ...".

pp. 272–273: Exercise 29. Ignore the reference to Exercise 6.25. That estimate is only necessary to prove the quantitative result that for some $\delta > 0$, there are $\gg x^\delta$ values of $n \le x$ for which $\sigma(n)$ is a square.

Acknowledgements

Thanks to everyone who pointed out errors, especially Lior Bary-Soroker, Rebecca Black, David Harden, Jackson Hopper, Mizan Khan, Mits Kobayashi, Adam Lizzi, Nathaniel Mon-

son, Carl Pomerance, and Enrique Treviño.