

**ERRATA AND CORRECTIONS TO
A FRIENDLY INTRODUCTION TO NUMBER THEORY
THIRD EDITION**

JOSEPH H. SILVERMAN

Acknowledgements Page vii (Corrected in 2nd Printing)

Thanks to the following people who have sent me comments and corrections used for the corrected second printing of the third edition: Rex Cheung, Gove Effinger, F. Izadi, Lars Hellvig, Colm Mulcahy, Russ Merris, Sarah Meiklejohn, Erik Rosenthal, Yuan-Yuan Shen, Michael Somos, Paul Stanford, Paul van Wamelen,

Acknowledgements Page vii (Corrected in 3rd Printing)

Thanks to the following people who have sent me comments and corrections used for the corrected third printing of the third edition: Ann Bledsoe, Jim Brennan, Pete Clark, Alex Kraus, David Marshall, Jeffrey Nunemacher,

Acknowledgements Page vii (Corrected in 3rd Printing)

Thanks to the following people who have sent me comments and corrections used for the corrected fourth printing of the third edition: Arthur Baragar, Colm Mulcahy, Steve Paik,

Page 3, Chapters 29–37 & 39–40 (Corrected in 2nd Printing)

In list of topics, missing comma between “Gaussian integers” and “transcendental numbers”.

Page 5, Third Bullet Item

Instead one might define $\gcd(0, 0)$ to equal 0. This is a good interpretation if $\gcd(a, b)$ is defined to be the (unique) integer $d \geq 0$ with the property that $c|a$ and $c|b$ if and only if $c|d$. In more advanced terms, this means that $\gcd(a, b)$ is the unique integer $d \geq 0$ that generates the ideal $a\mathbb{Z} + b\mathbb{Z}$. However, this does not agree with the more intuitive definition of $\gcd(a, b)$ as the largest integer d satisfying $d|a$ and $d|b$, in which case $\gcd(0, 0)$ clearly does not exist.

Page 9 and following

The preferred spelling for Gauss’s first name is “Carl”, not “Karl”.

Pages 13–14 (Corrected in 2nd Printing)

The paragraph at the bottom of page 16 first mentions Babylonia, then Egypt, then repeats information about Babylonia. It should read as follows:

The study of these *Pythagorean triples* began long before the time of Pythagoras. There are Babylonian tablets that contain lists of such triples, including quite large ones, indicating that the Babylonians probably had a systematic method for producing them. Even more amazing is the fact that the Babylonians appear to have used their lists of Pythagorean triples as primitive trigonometric tables. Pythagorean triples were also used in ancient Egypt. For example, a rough-and-ready way to produce a right angle is to take a piece of string, mark it into 12 equal segments, tie it into a loop, and hold it taut in the form of a 3-4-5 triangle, as illustrated in Figure 2.2. This provides an inexpensive right angle tool for use on small construction projects (such as marking property boundaries or building pyramids).

Page 19, Exercise 2.5(a) (Corrected in 2nd Printing)

There should be 4's in front of T_5 , T_6 , and T_7 . Also triple should be singular. Thus it should read:

(a) Find a primitive Pythagorean triple (a, b, c) with $b = 4T_5$. Do the same for $b = 4T_6$ and for $b = 4T_7$.

Page 19, New Problem

Let m and n be numbers that differ by 2 and write the sum $\frac{1}{m} + \frac{1}{n}$ as a fraction in lowest terms. For example, $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$ and $\frac{1}{3} + \frac{1}{5} = \frac{8}{15}$.

- (a) Compute the next three examples.
 - (b) Examine your data from (a) and formulate a conjecture that relates the answer to Pythagorean triples
 - (c) Prove that your answer is correct.
- (Thanks to Henning Broge for suggesting this problem.)

Page 22, Bottom (Corrected in 2nd Printing)

The text says that

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2).$$

This is another way of describing all Pythagorean triples, although...

This formula does *not* describe all triples, for example, it misses $(9, 12, 15)$, and more generally it misses most triples of the form (ua, ub, uc) where (a, b, c) is a primitive triple and u is not a perfect square.

Page 26 (Corrected in 3rd Printing)

Alexander Grothendieck is not Belgian. He was born in Germany and spent most of his mathematical career in France.

Pages 27, 150, 428 (Corrected in 2nd Printing)

The preferred spelling for Jacobi's first name is "Carl", not "Karl".

Page 34, Exercise 5.5(c,d,e)

For these parts, add the assumption that the algorithm terminates at 1, not simply that it terminates. Further, for (c) need to assume that $k \geq 1$, since for $k = 0$ we have $L(4) = 3$ and $L(5) = 6$.

Pages 42, Exercise 6.5 (Corrected in 2nd Printing)

In the hint, $au + by = 1$ should be $au + bv = 1$.

Page 46, Line 8 (Corrected in 2nd Printing)

“in the \mathbb{E} -Zonewe can” should be “in the \mathbb{E} -Zone we can” (missing space).

Page 66, First displayed formula (Corrected in 2nd Printing)

There should be question marks as an exponent on a . Thus

$$a^{??} \equiv 1 \pmod{m}.$$

Page 67, Line 1 (Corrected in 2nd Printing)

“The number of integers between 0 and m ” should be “The number of integers between 1 and m ”.

Page 69, Exercise 10.2 (Corrected in 2nd Printing)

The solution to this exercise was supposed to be $343 + m$, but this is not necessarily correct, because there are values of m larger 2000 satisfying $\phi(m) = 1000$. Indeed, the full list of such m is

$$1111, 1255, 1375, 1875, 2008, 2222, 2500, 2510, 2750, 3012, 3750.$$

Change the exercise to the following.

One can check that the number 3750 satisfies $\phi(3750) = 1000$. Find a number a that has the following three properties:

- (i) $a \equiv 7^{3003} \pmod{3750}$.
- (ii) $1 \leq a \leq 5000$.
- (iii) a is not divisible by 7.

Page 77, new exercise (Corrected in 2nd Printing)

Add the following exercise as new parts of Exercise 11.11.

Suppose that the integer n satisfies $\phi(n) = 1000$.

- (a) Make a list of all of the primes that might possibly divide n .
- (b) Use the information from (a) to find all integers n that satisfy $\phi(n) = 1000$.

Page 77, Exercise 11.13(c) (Corrected in 2nd Printing)

It should be “Prove that your criterion in (b) is correct.”

Page 84, Exercise 12.4(b,c) (Corrected in 2nd Printing)

Replace (b) and (c) with the following:

Generate some data for the value of $A_m \pmod{m^2}$, try to find patterns, and then try to prove that the patterns you observe are true in general. In particular, can you determine conditions on m that lead to $A_m \equiv 0 \pmod{m^2}$?

Page 88, Line -3 (Corrected in 3rd Printing)
 “Hendrik Iwaniec” should be “Henryk Iwaniec”.

Page 94, Table 14.1 (Corrected in 2nd Printing)
 There are new Mersenne primes: $p = 25964951$ discovered by Nowak in 2005 and $p = 30402457$ discovered by Boone and Cooper in 2005. There are nine record primes found by the GIMPS project. It might be appropriate to add an asterisk to the Mersenne primes discovered as a result of GIMPS (which are the nine primes starting with 1398269) and include a footnote indicating that credit for their discovery is also shared by Woltman, Kurokowski and the many others who have contributed to the GIMPS project.

Page 94, Table 14.1 (Corrected in 3rd Printing)
 Boone and Cooper have discovered another one! Add another line to the table:
 $2^{32582657}$ Boone, Cooper 2006

Page 101, Line 9 (Corrected in 2nd Printing)
 “We have now prove that if n is an even perfect number then” should be “We have now proved that if n is an even perfect number then” (missing “d” on “prove”).

Page 112, Line -4 (Corrected in 2nd Printing)
 “We know a solution exists, since $\gcd(k, \phi(m)) = 1$ ” should read, “We know a solution exists, since for our example, $\gcd(k, \phi(m)) = \gcd(131, 1008) = 1$ ”.

Page 115, Exercise 17.3(b) (Corrected in 2nd Printing)
 Put in a note that this is a hard problem with the material covered so far.

Page 130, Line 3 (Corrected in 2nd Printing)
 p_1, p_2, \dots, p_t should be p_1, p_2, \dots, p_r . (The upper index should be r , not t .)

Page 132, Line 6 (Corrected in 2nd Printing)
 0.75^{100} should be 0.25^{100} , since there is at most a 25% chance of a false positive for each test. This probability is approximately $6 \cdot 10^{-61}$.

Page 132, Paragraph 2 (Corrected in 3rd Printing)
 The probability calculation is not quite correct, since we should really be computing a conditional probability. Add the following footnote: We have cheated a little bit. We really need to compute what is called a conditional probability, in this case the probability that n is composite given that 100 values of a fail to be witnesses. The correct bound for the probability is approximately $0.25^{100} \cdot \ln(n)$.

Page 132, Line 9 (Corrected in 3rd Printing)
 “reveal this fact” should be “reveals this fact”.

Page 133, Exercise 19.1(a) (Corrected in 2nd Printing)

The hint suggests taking a to be a primitive root modulo p . Unfortunately, primitive roots are not discussed until the following chapter. (Originally the chapter on primality testing was to be later in the book.) Either move this problem to Chapter 20, or change the hint to the following: [*Hint.* We will prove in Chapter 21 that for every prime p there is at least one number g whose powers $g, g^2, g^3, \dots, g^{p-1}$ are all different modulo p . (Such a number is called a *primitive root*.) In order to solve this problem, try putting $a = g$ into the Carmichael congruence $a^n \equiv a \pmod{n}$.]

Page 133, Exercise 19.3 (Corrected in 2nd Printing)

“Kursolt’s” should be “Korselt’s”

Page 137, Proof of Theorem 20.2

The letter r is being used for two different things. It is the number of divisors of n and it is the number of primes dividing n . Change so that the factorization of n into primes is $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$. Then the calculation reads:

$$\begin{aligned} F(n) &= F(p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}) \\ &= F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_t^{k_t}) && \text{from the multiplication formula,} \\ &= p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t} && \text{since } F(p^k) = p^k \text{ for prime powers,} \\ &= n. && \square \end{aligned}$$

Page 137, Exercise 20.1

The letter r is being used for two different things. It is the number of divisors of n and it is the number of primes dividing n . Change so that the factorization of n into primes is $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$. Then the first part of the exercise reads:

20.1. Liouville’s lambda function $\lambda(n)$ is defined by factoring n into a product of primes, $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$, and then setting

$$\lambda(n) = (-1)^{k_1 + k_2 + \cdots + k_t}.$$

Page 140, Proof of Theorem 21.1

This proof is needlessly complicated. Here is an easier proof.

Verification. The definition of the order $e_p(a)$ tells us that

$$a^{e_p(a)} \equiv 1 \pmod{p},$$

and we are assuming that $a^n \equiv 1 \pmod{p}$. We divide n by $e_p(a)$ to get a quotient and remainder,

$$n = e_p(a)q + r \quad \text{with } 0 \leq r < e_p(a).$$

Then

$$1 \equiv a^n \equiv a^{e_p(a)q+r} \equiv \left(a^{e_p(a)}\right)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{p}.$$

But by definition, $e_p(a)$ is the smallest positive exponent e that makes $a^e \equiv 1 \pmod{p}$, and $r < e_p(a)$, so we must have $r = 0$. Therefore $n = e_p(a)q$, which shows that $e_p(a)$ divides n .

Finally, Fermat’s Little Theorem (Chapter 9) tells us that $a^{p-1} \equiv 1 \pmod{p}$, so taking $n = p - 1$, we conclude that $e_p(a)$ divides $p - 1$.

Page 153, Line 10

“lograrithm” should be “logarithm”

Page 159, Lines 14 and 22 (Corrected in 2nd Printing)

“QRor” should be “QR or” and “NRor” should be “NR or”

Page 160, Line –5 (Corrected in 2nd Printing)

“For any numbers a and b relatively prime to $p!$ the Product Rule” should be “For any numbers a and b relatively prime to p , the Product Rule” (change the exclamation mark to a comma).

Page 182, Theorem 25.2 (Corrected in 2nd Printing)

The hypotheses on a and b should include the assumption that they are positive. Thus change “Let a and b be odd numbers” to “Let a and b be odd positive integers.”

Page 187, Line 5 (second displayed formula) (Corrected in 2nd Printing)

Change

$$m - 1^2, \quad m - 2^2, \quad m - 3^2, \quad m - 4^2, \dots$$

to

$$m - 0^2, \quad m - 1^2, \quad m - 2^2, \quad m - 3^2, \quad m - 4^2, \dots$$

This checks whether m itself being a square.

Page 187, footnote (Corrected in 2nd Printing)

Change “between 1 and $\sqrt{m/2}$ ” to “between 0 and $\sqrt{m/2}$ ”.

Page 200, Line –9 (Corrected in 2nd Printing)

After the sentence “The prime 7 is not a sum of two squares, so m is not a sum of two squares.” add “(See Exercise 27.4.)”, since we have not yet proven this direction.

Page 202, Exercise 27.3 (Corrected in 2nd Printing)

The problem asks for two solutions in positive integers. In fact, there are four solutions. But only two of the solutions are primitive, that is, satisfy $\gcd(a, c) = 1$.

Page 215, New Exercise (Corrected in 2nd Printing)

Add the following as the first part of Exercise **29.3**.

Let (x_k, y_k) for $k = 0, 1, 2, 3, \dots$ be the solutions to $x^2 - 2y^2 = 1$ described in Theorem 29.1. Fill in the blanks with positive numbers so that the following formulas are true:

$$x_{k+1} = ______ x_k + ______ y_k \quad \text{and} \quad y_{k+1} = ______ x_k + ______ y_k.$$

Prove that your formulas are correct.

Page 229–230 (Corrected in 3rd Printing)

The book says that γ “was called the *Golden Ratio* by the Greeks.” In fact, there is no historical evidence that the Greeks used this name. The ancient term for this ratio appears to have been the *extreme and mean ratio*.

Page 236, Line 3 (Corrected in 3rd Printing)

In the verification that (x, y) satisfies Pell's equation, in the second line of the displayed equation, the second Y_j should be Y_k . Thus the displayed equation should read:

$$\begin{aligned} x^2 - Dy^2 &= \left(\frac{X_j X_k - Y_j Y_k D}{M} \right)^2 - D \left(\frac{X_j Y_k - X_k Y_j}{M} \right)^2 \\ &= \frac{(X_j^2 - DY_j^2)(X_k^2 - DY_k^2)}{M^2} \\ &= 1. \end{aligned}$$

Page 251, Lines 3–4 (Corrected in 2nd Printing)

Bad page break in the middle of $(u + vi)^2 = 95 - 168i$.

Page 251, Line –5 (Corrected in 2nd Printing)

'define the "norm" of α to be' should be 'define the "norm" of α to be' (the quote marks around "norm" are misplaced).

Page 257, Theorem 34.4 (Corrected in 2nd Printing)

In the statement of the Gaussian Prime Divisibility Property, "suppose the π divides the product $\alpha\beta$ " should be "suppose that π divides the product $\alpha\beta$ "

Page 266, displayed equation (line 15) (Corrected in 2nd Printing)

Change the displayed equation

$$(D_1 - D_3 \text{ for } N) = (D_1 - D_3 \text{ for } n).$$

to read

$$(D_1 \text{ for } N) - (D_3 \text{ for } N) = (D_1 \text{ for } n) - (D_3 \text{ for } n).$$

Page 274, Line –12 (Corrected in 2nd Printing)

Change "Liouville's brilliant idea is that if a number is the root of a polynomial" to "Liouville's brilliant idea is that if an irrational number is the root of a polynomial".

Page 282, Exercise 35.5 (Corrected in 2nd Printing)

The polynomial should be $f(X) = X^d + c_1 X^{d-1} + c_2 X^{d-2} + \cdots + c_{d-1} X + c_d$, not $f(X) = X^n + c_1 X^{d-1} + c_2 X^{d-2} + \cdots + c_{d-1} X + c_d$. (The top exponent on X should be d , not n .)

Page 283, Exercise 35.9(d) (Corrected in 2nd Printing)

"to program , redo" should be "to program, redo" (delete the space after "program").

Page 283, Exercise 35.7 (Corrected in 2nd Printing)

The polynomial should be $f(X) = X^d + c_1 X^{d-1} + c_2 X^{d-2} + \cdots + c_{d-1} X + c_d$, not $f(X) = X^n + c_1 X^{d-1} + c_2 X^{d-2} + \cdots + c_{d-1} X + c_d$. (The top exponent on X should be d , not n .)

Page 297, First paragraph (Corrected in 2nd Printing)

The book mentions “Europeans who were still laboring under the handicap of doing calculations with Roman numerals.” This is not historically accurate. Calculations would have been done using some sort of mechanical process (pebbles, rods, abacus, . . .) and then the results recorded using Roman numerals. Paper cost too much to be used for scratch calculations.

Page 303 (Corrected in 3rd Printing)

Much of the material in the “Historical” Interlude on page 303 turns out to be folklore, rather than history.

For further information, see for example *A Mathematical History of the Golden Number*, Roger Herz-Fischler, Dover Publications, 1998, or the book review by George Markowsky of the book *The Golden Ratio* in the Notices of the American Mathematical Society **53**(3), March 2005.

Page 314, Line –5 (Corrected in 2nd Printing)

Change “leaving it in gives a slightly stronger estimate” to “leaving it in gives only a slightly stronger estimate”.

Page 318, paragraph after bullet items (Corrected in 2nd Printing)

“It is thus interesting and somewhat surprising that we can compute the quantity $a^n \pmod{m}$ in time $O(\log(n))$, since it already takes time $O(\log(n))$ simply to input the number n .” This is only true if we suppose that a and m are fixed and that n is large. Otherwise, if (say) m and n are of comparable size, then each multiplication modulo m takes time at least $O(\log(m))$, and possibly longer. Notice that the $m \approx n$ case is the one required by RSA.

Page 336, Lines 2 and 4 (Corrected in 2nd Printing)

The three instances of a_N should all be a_{N+1} .

Page 339, New Exercise (Corrected in 3rd Printing)

The following new exercise really belongs between Exercises **39.4** and **39.5**, but it has been added to the end of the exercises for Chapter 39.

Suppose that we use the recursion for p_n backwards in order to define p_n for negative values of n . What are the values of p_{-1} and p_{-2} ? Same question for q_{-1} and q_{-2} .

Page 348, Table 40.2 (Corrected in 3rd Printing)

This is a table of convergents to $\sqrt{71}$, not to $\sqrt{17}$. So the heading of the third column should read $p^2 - 71q^2$ and the caption for the table should read “Convergents p/q to $\sqrt{71}$.”

Page 362, Exercise 41.1 (Corrected in 2nd Printing)

The notation $O(x)$ for the generating function of the odd integers is confusing, since it looks like big-oh notation. Change it to another letter. Thus:

- (a) Find a simple formula for the generating function $E(x)$ for the sequence of even numbers $0, 2, 4, 6, 8, \dots$.
- (b) Find a simple formula for the generating function $J(x)$ for the sequence of odd numbers $1, 3, 5, 7, 9, \dots$.
- (c) What does $E(x^2) + xJ(x^2)$ equal? Why?

Page 373, New Exercises

Add the following exercises. They give a “closed” expression for the sum of k^{th} powers that was studied in this chapter. (Or as an alternative, put the Stirling number exercise in the earlier chapter on recurrence sequences.)

Exercise 42.12 *Stirling numbers (of the second kind)* are defined to be the integers $S(k, j)$ that make the following polynomial equation true:

$$x^k = \sum_{j=0}^k S(k, j)x(x-1)(x-2)\cdots(x-j+1).$$

For example, taking $k = 1$ gives

$$x = S(1, 0) + S(1, 1)x, \quad \text{so } S(1, 0) = 0 \text{ and } S(1, 1) = 1.$$

Similarly, taking $k = 2$ gives

$$\begin{aligned} x^2 &= S(2, 0) + S(2, 1)x + S(2, 2)x(x+1) \\ &= S(2, 0) + (S(2, 1) + S(2, 2))x + S(2, 2)x^2, \end{aligned}$$

so

$$S(2, 0) = 0 \text{ and } S(2, 2) = 1 \text{ and } S(2, 1) = -1.$$

- (a) Compute the value of $S(3, j)$ for $j = 0, 1, 2, 3$ and $S(4, j)$ for $j = 0, 1, 2, 3, 4, 5$.
- (b) Prove that the Stirling numbers satisfy the recurrence

$$S(k, j) = S(k, j-1) + jS(k, j).$$

- (c) Prove that the Stirling numbers are given by the following formula:

$$S(k, j) = \frac{1}{j!} \sum_{i=0}^j (-1)^{j-i} \binom{j}{i} i^k.$$

Exercise 42.13 Prove that the sum of k^{th} powers is given by the following explicit formula using the Stirling numbers $S(k, j)$ defined in the previous exercise.

$$1^k + 2^k + \cdots + n^k = \sum_{j=0}^k \frac{S(k, j)}{j+1} (n+1)n(n-1)(n-2)\cdots(n-j+1).$$

Page 374, Line 1–2

Exercise 42.4(c). The indicated sum is 0 if $p - 1 \nmid k$, but it is congruent to -1 if $p - 1 \mid k$. Also, the most natural way to do this exercise is using primitive roots, not using (b). Indeed, although it is true that $P_k(-1) = 0$, the argument

$$P_k(p - 1) \equiv P_k(-1) \equiv 0 \pmod{p}$$

is not correct, because the coefficients of the polynomial $F_k(x)$ may have p in their denominators.

The corrected exercise should read as follows:

If p is a prime number and if $p - 1 \nmid k$, prove that

$$1^k + 2^k + \cdots + (p - 1)^k \equiv 0 \pmod{p}.$$

What is the value when $p - 1$ divides k ?

Page 377, Line 1 (Corrected in 2nd Printing)

“we weill study” should be “we will study”.

Page 400, Line 1 (Corrected in 2nd Printing)

“we make a table giving the number N_p of points on E_2 modulo p ” should be “we make a table giving the number N_p of points on E_1 modulo p ” (change E_2 to E_1 at the end of the line).

Page 407, Line 6 (Corrected in 2nd Printing)

“Subsituting” should be “Substituting”.

Page 412, Line 4 (Corrected in 2nd Printing)

“the elliptic curve E_1 with equation $y^2 = x^3 + x$ ” should be “the elliptic curve E_2 with equation $y^2 = x^3 + x$ ”. (The curve is E_2 , not E_1 .)

Page 414, footnote

In the displayed equation, the $1/(Cz + D)^2$ should be $1/(CNz + D)^2$ and it should be on the other side of the equation (or replace it by $(CNz + D)^2$). Thus the displayed equation should read

$$f\left(\frac{Az + B}{CNz + D}\right) = (CNz + D)^2 f(z).$$

Page 418, second Ribenboim reference (Corrected in 2nd Printing)

through the centuries (missing word “the”).

Page 430, Index (Corrected in 2nd Printing)

Index entry for “Poussin” should be “Poussin, Ch. de la Vallée” (missing “la”).

Suggested Additional Chapter(s)

It has been suggested that one or more chapters be added on *Mathematical Induction*. This would be useful because FRINT is often used in students' first "proof" course, and also because induction is important for students studying computer science.

It has been suggested to add a chapter on factorization methods that exploit $x^2 \equiv y^2 \pmod{N}$. This could include sieves and/or the continued fraction method as a followup to Chapters 39 and 40 on continued fractions.