ERRATA AND SUPPLEMENTARY MATERIAL FOR A FRIENDLY INTRODUCTION TO NUMBER THEORY FOURTH EDITION

JOSEPH H. SILVERMAN

Acknowledgements Page vii
Thanks to the following people who have sent me comments and corrections to the fourth edition: Benjamin Atchison, Joseph Bak, Chase Banta, Matt Baker, Jennifer Beineke, Wei-Chih Chung, Somjit Datta, Jason Dyer, Derek Garton, Nezih Geckinli, Jacob Hicks, David Krumm, Thomas Kurian, Joey Lee, SongSong Lu, Sam McCoy, John Perry Arvind Suresh, Arianna Zikos.

Page ix, Chapter Dependencies
Chapter 29 is not in the picture. The box that says 27–28 should say 27–29.

Page ix, Chapter Dependencies
Theorem 35.4 (Gaussian Prime Theorem) in Chapter 35 requires the Sums of Two Squares Theorem in Chapter 24 and also uses Quadratic Reciprocity from Chapter 21 (although only the easy fact that if $p \equiv 3 \pmod 4$, then -1 is not a square mod p). Of course, the Sums of Two Squares Theorem uses the converse. So it should be noted in the dependency diagram that the last part of Chapter 35 uses Chapters 21 and 24.

Page 9
The anecdote about Gauss should be described as "possibly apocryphal". There's an interesting discussion of the story at `http://www.americanscientist.org/issues/id.3483,y.0,no.,content.true,page.1,css.print/issue.aspx`

Page 25, Exercise 3.5(f)
The procedure described in this exercise won't give all square-triangular numbers, since it essentially creates a new pair from an old pair by squaring $u + v\sqrt{2}$. (This is explained more fully later in the book when we do Pell's equation.)

Page 35, Exercise 5.3
The conclusion should be that the Euclidean algorithm terminates in at most $2\log_2(b) + 1$ steps. One should also find an example of a pair (a, b) that takes strictly more than $2\log_2(b)$ steps.

Date: June 2, 2017.

Page 40
"We can create additional solutions by subtracting a multiple of b from x_1 and adding the same multiple of a onto y_1 . In other words, for any integer k we obtain a new solution $(x_1 + kb, y_1 - ka)$." The first sentence needs to be reversed to match the second sentence. So it should read "We can create additional solutions by adding a multiple of b from x_1 and subtracting the same multiple of a onto y_1 . In other words, for any integer k we obtain a new solution $(x_1 + kb, y_1 - ka)$."

Page 48–49, $\mathbb{E}$-Zone
According to the definition, negative even numbers can be $\mathbb{E}$-primes, too, for example -2 and -6 are $\mathbb{E}$-primes. But then 12 has two factorizations into $\mathbb{E}$-primes, $12 = 2 \cdot 6 = (-2) \cdot (-6)$. So should stick to factorization of positive even numbers into products of positive $\mathbb{E}$-primes. Alternatively treat two factorizations as the same if they arise from inserting pairs of minus signs.

Page 60–62, Proof of Theorem 8.2
Since this is the books first proof by contradiction, it is probably worth also pointing out that B_0 is equal to A_0, so that the condition that the leading coefficient not be divisible by p is preserved.

Page 76, Line -13
"all this" should be "All this".

Page 80, Lines 10 and 14
In order to get $x_1 = my_1 + b$ between 0 and mn, we can't take y_1 between 0 and n. So on Line 10 change the inequality to $-\frac{b}{m} \le y_1 < n - \frac{b}{m}$, and on Lines 13–14 say that "there is only one y_1 between $-\frac{b}{m}$ and $n - \frac{b}{m}$.

Page 94, Line 9
The value of C is half of what it should be. Thus C is approximately equal to 1.72032

Page 99, Table 14.1
New Mersenne prime: $p = 57885161$, discovered by Curtis Cooper, 2013 (as part of GIMPS)

Page 99, Table 14.1
New Mersenne prime: $p = 74207281$, discovered by Curtis Cooper, 2016 (as part of GIMPS)

Page 172, Lines −6 and following
First, "each another" should be "each other." Next, it has been suggested that the use of e for ± 1 is confusing. So replace the entire paragraph with the following:

Suppose that two of the r_k values are either the same or negatives of each other, say $r_i = \pm r_j$ with $1 \le i \le j \le P$. Suppose first that $r_i = r_j$. Then

$$ia - ja = (pq_i + r_i) - (pq_j + r_j) = p(q_i - q_j),$$

so p divides $(i-j)a$. Similarly, if $r_i = -r_j$, then

$$ia + ja = (pq_i + r_i) + (pq_j + r_j) = p(q_i + q_j),$$

so p divides $(i+j)a$. But p is prime and a is not divisible by p, so we conclude that p divides one of $i-j$ or $i+j$. However

$$2 \le i + j \le P + P = p - 1,$$

which shows that p does not divide $i+j$. It follows that p divides $i-j$, and then the fact that

$$-\frac{p-3}{2} = 1 - P \le i - j \le P - 1 = \frac{p-3}{2}$$

shows that we must have $i = j$.

Page 174, Lines 7–8
"proof of quadratic identity" should be "proof of quadratic reciprocity"

Page 174, Proof of Lemma 23.3, Line −3 and −5
The $<$ signs should be $\le$. So Line −5 should read

$$ka = q_k p + r_k \quad \text{with} \quad -P \le r_k \le P.$$

And Line −3 should read

$$\frac{ka}{p} = q_k + \frac{r_k}{p} \quad \text{with} \quad -\frac{1}{2} \le \frac{r_k}{p} \le \frac{1}{2}.$$

Page 171, Chapter 23
This chapter, new to the 4th edition, contains one of the deepest and most difficult proofs in the book. It might be helpful to describe the overall pattern of the proof and to explain how one might be led, step-by-step, to finding it.

The proof may be divided into five main components:

Step 1. Euler's formula $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p$

Fermat's little theorem says that $a^{p-1} \equiv 1 \pmod p$, so it is natural to look at the quantity at $a^{(p-1)/2} \pmod p$. The fact that $a^{(p-1)/2} \pmod p$ squared is equal to 1 implies that $a^{(p-1)/2} \equiv \pm 1 \pmod p$. Further, if a is a quadratic residue, say $a \equiv b^2 \pmod p$, then

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod p.$$

This, and experiments, suggest that if a is a non-residue, then $a^{(p-1)/2} \pmod p$ equals -1, which leads to Euler's formula.

Step 2. Gauss' criterion

In view of Euler's formula, we want to get our hands on the quantity $a^{(p-1)/2} \pmod p$. Looking back at our proof of Fermat's little theorem, we took the multiples $a, 2a, \dots, (p-1)a$ of a modulo p and multiplied them together. This got us a^{p-1}, which was good, multiplied by $(p-1)!$, which we were able to cancel. So in order to get $a^{(p-1)/2} \pmod p$, we might try multiplying half of the multiples together, i.e., let $P = (p-1)/2$ and multiply $a, 2a, \dots, Pa$. This gives the desired $a^P \pmod p$, multiplied by $P!$. We can again cancel the $P!$, and counting the number of minus signs gives Gauss' criterion.

Step 3. A sum associated to Gauss' criterion

Okay, now we're looking at $a, 2a, \dots, Pa$, and we want to reduce these numbers modulo p into the range from $-P$ to P and count how many are negative. As in the proof of Lemma 23.2, which came up naturally when we proved Gauss' criterion, we write each multiple ka as

$$ka = pq_k + r_k \quad \text{with } -P \le r_k \le P,$$

and we want to count how many of the r_k are negative. We note that

$$\frac{ka}{p} = q_k + \frac{r_k}{p} \quad \text{with } -\frac{1}{2} < \frac{r_k}{p} < \frac{1}{2},$$

so

$$\left\lfloor \frac{ka}{p} \right\rfloor = \begin{cases} q_k & \text{if } r_k > 0, \\ q_k - 1 & \text{if } r_k < 0. \end{cases}$$

This gives the crucial equation (which appears in the proof of Lemma 23.3)

$$\sum_{k=1}^{P} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{P} q_k - \begin{pmatrix} \text{number of } k \text{ such that} \\ r_k \text{ is negative} \end{pmatrix}.$$

Since we only need to know whether the number of negative r_k is odd or even, we are led to study the sum $\sum_{k=1}^{P} q_k$ modulo 2. And after some experimentation and some work, we figure out that the sum is always even, which when combined with Gauss' criterion, gives the interesting formula

$$\sum_{k=1}^{P} \left\lfloor \frac{ka}{p} \right\rfloor \equiv \begin{cases} 0 \pmod 2 & \text{if } \left(\frac{a}{p}\right) = 1, \\ 1 \pmod 2 & \text{if } \left(\frac{a}{p}\right) = -1. \end{cases}$$

Step 4. Relating a sum to a triangle

Suppose that we graph the points in the sum appearing in Step 3, i.e., we graph the points

$$\left(1, \left\lfloor \frac{a}{p} \right\rfloor\right), \left(2, \left\lfloor \frac{2a}{p} \right\rfloor\right), \left(3, \left\lfloor \frac{3a}{p} \right\rfloor\right), \dots, \left(P, \left\lfloor \frac{Pa}{p} \right\rfloor\right).$$

These points lie just below the line $y = \frac{a}{p}x$, and if we want to add up their y-coordinates, that's the same as counting how many points with integer coordinates lie below each one. In other words, the sum that we want to compute is equal to the number of points with integer coordinates that lie inside the triangle formed by the x-axis, the line $x = P$, and the line $y = \frac{a}{p}x$.

Step 5. Using two triangles to form a rectangle

Quadratic reciprocity is a relation between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$, so we want to compare the sums

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor \quad \text{and} \quad \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor.$$

Step 4 says that each of these sums is the number of points in a certain triangle. If you draw these triangles and stare at them for a while, you'll say "Hey, if I flip over the second triangle and put it on top of the first triangle, I get a rectangle." But it's easy to count the number of points with integer coordinates in a rectangle, and doing so completes the proof of quadratic reciprocity.

Page 177, Line 2

The last vertex of the triangle $T'(p,q)$ has its coordinates reversed. It should be $(\frac{p}{2}, \frac{q}{2})$, not $(\frac{q}{2}, \frac{p}{2})$. So this line should read:

"...in the triangle $T'(p,q)$ whose vertices are $(0,0)$, $(0,\frac{q}{2})$, and $(\frac{p}{2},\frac{q}{2})$."

Page 180, New Exercise

There's a very short clever proof of quadratic reciprocity, using only Euler's formula and the Chinese remainder theorem, due to G. Rousseau, On the quadratic reciprocity law, *J. Austral. Math. Soc. Ser. A* **51** (1991), 423–425. The proof is described completely in the accepted answer to the MathOverflow post `http://mathoverflow.net/questions/1420/`. This would make a good (worked) exercise.

Page 198, New Exercise for Chapter 25

25.8. Exercise 2.4 asked you to find values of c that belong to two or three different primitive Pythagorean triples. Using the tools that we developed in this chapter, prove that for every N there is a value of c that belongs to at least N different primitive Pythagorean triples.

Page 204, Exercise 26.4

The polynomial should be

$$F(x) = x^2 - x + 41,$$

not $F(x) = x^2 - x - 41$.

Page 211, Line 1

"If a and p are relatively prime" should say "If p is prime and a and p are relatively prime". (Although by this point in the book, most readers will probably realize that the letter p is prime unless we say otherwise!)

Page 223, Exercise 28.18

The mathematician's name is (Solomon W.) Golomb, not Golumb.

Page 228, text

Both "discrete logarithm" and "Discrete Logarithm Problem" should be added to the index.

Page 229 and elsewhere
The preferred spelling is "Elgamal", not "ElGamal".

Page 232, Lines 6–8
The books says that "If x, y, and z have a common factor, we can factor it out and cancel it, so we may as well assume that they are relatively prime." It's actually a little subtler, since z only appears squared. So replace with the following:

If x, y, and z have a common factor, say g, then g^4 divides $x^4 + y^4$, so g^4 divides z^2, so g^2 divides z. Then dividing by g^4 gives a smaller solution in integers, namely $(x/g)^4 + (y/g)^4 = (z/g^2)^2$. So we may as well assume that x, y, and z have no nontrivial common factors.

Page 240, Lines -11 and -7
The inequalities in these displayed equations should be $3 \le s < u$ and $3 \le q < s$, respectively.

Page 255, Figure 33.1
Pigeon 5 should be 0.02776, not 0.02778.

Page 255, Line -3
The value of m is allowed to be 0, so the string of inequalities should read $0 \le m < n \le Y$.

Page 270, Line 3
There's an extraneous minus sign in this displayed equation. It should read

$$600 = i \cdot (1+i)^6 \cdot 3 \cdot (2+i)^2 \cdot (2-i)^2.$$

Page 283, Line 18, Second Displayed Equation
With the conventions we're using, the factors are in the reverse order. So this display should read

$$237 + 504i = (15 - 17i)(-10 + 23i) + (-4 - 11i).$$

Page 300, Line 4
"$X^2 - p$ has no roots" should be "$X^2 - p$ has no rational roots".

Page 303, Line 12
"If α is an algebraic number, that is, if α is a root of a polynomial..." should be "If α is an irrational algebraic number, that is, if α is an irrational root of a polynomial...," since obviously if α is rational, then there is a rational number close to α, namely α itself. On the other hand, note that Liouville's Inequality (Theorem 37.2), as we have stated it, is true even if α is rational.

Page 307, Lines 9–10
This inequality is not quite right. It should read

$$|r_4 - \beta| < 2 \cdot 10^{-20} = 2/b_4^5.$$

Page 317–318
Due to the way that the binomial coefficient is defined on Page 314, the discussion on Pages 317–318 describes the computation of $\binom{n}{n-k}$, not $\binom{n}{k}$. In lieu of rewriting this material, one can discuss the symmetry property before Theorem 38.2, being sure to that $0! = 1$ to handle the case the $k = 0$.

Page 376, Line −8
The formula for $R(p)$ is $R(p) = 4(D_1 - D_3)$. So for a prime p that is congruent to 1 modulo 4, the divisors 1 and p of p are 1 modulo 4, so we have $D_1 = 2$ and $D_3 = 0$. Hence $R(p) = 8$, and as indicated, the 8 is accounted for by first writing $p = A^2 + B^2$, and then switching A and B and/or changing the signs of one or both of A and B.

Page 397+, Index
The index still includes entries for the Foxtrot cartoons that were removed from the 4th edition (at the insistence of the publisher).

Suggested Additional Chapter
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.

Suggested Additional Chapter
Possibly include a short chapter on Hadamard matrices. These are n-by-n matrices A with all entries ± 1 whose columns are pairwise orthogonal. Equivalently, such that $|\det A| = n^{n/2}$ takes the largest possible value among matrices whose entries all have absolute value 1. Not hard to show that if $n \geq 3$, then must have $4 \mid n$. There's a construction for infinitely many n that uses Legendre symbols, so a nice application of the multiplicativity of the Legendre symbol. It is not known whether Hadarmard matrices exist for all n, although experimental evidence suggests that they do. (Note: It is not necessary to know about determinants to define a Hadamard matrix. A Hadamard matrix may be defined to be a list of n vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^n$ whose entries are all ± 1 and with the property that $\mathbf{v}_i \cdot \mathbf{v}_j = 0$ for all $i \neq j$.)