Errata for An Experimental Introduction to Number Theory

Benjamin Hutz

Department of Mathematics and Statistics, Saint Louis University

Email address: benjamin.hutz@slu.edu
The trial division algorithm (Algorithm 0.1) is missing divisors.

**Algorithm 0.1 Trial Division**

**Input:** a positive integer \( n \geq 1 \)

**Output:** a list of divisors

**Algorithm:**

1. Repeat until \( d > \sqrt{n} \).
   a. If \( d \) divides \( n \), add \( d \) and \( \frac{n}{d} \) to the list of divisors.
   b. Increase \( d \) by one.

2. Return the list of divisors

- Equation in middle of page 25. \( \pi(100) = 25 \) so that \( \frac{\pi(100)}{100} = 0.25 \). Also needs to be corrected in the subsequent table.
- Exercise 3.4a needs to have a relatively prime numerator.
  
  \((3.4)\) Compute the following Jacobi symbols \( \left( \frac{a}{n} \right) \). Determine whether \( a \) is quadratic residue or non-residue modulo \( n \).
  
  a. \( \left( \frac{11}{77} \right) \)
  
  b. \( \left( \frac{17}{37} \right) \)

- page 66. Statement of Theorem 3.7 should read: If \( p > 2 \) is a prime and \( a \) is an integer not divisible by \( p \), then...

- In proof of the Law of Quadratic Reciprocity:
  
  a. Bottom of page 71, the equation should read
     \[
     x_1^2 + x_2^2 - x_3^2 + \cdots + x_p^2 \equiv 1 - 2x_1x_2 \pmod{q}.
     \]
  
  b. There are a couple extra closing parenthesis in the sequence of equations (13)
  
  c. The equations on the top of page 73 are missing a couple places where \( (-1)^e \) should have been a Legendre Symbol \( \left( \frac{-1}{q} \right)^e \).

- page 75. Theorem 3.22: parts (c), (d), and (e) also require \( m \) and \( n \) to be odd.

- page 79. First line of proof of Theorem 3.37. It should read: \( a = g^k \) and \( x = g^y \) for some integers \( k \) and \( y \).

- page 80. the 3rd line should read: \( \varphi(n) = 6 \)

- page 82. Fifth line of proof of Lemma 3.42. It should read: \( r | xy \).

- page 83. end of proof of Lemma 3.44, \( g + p \) should be \( g + n \).

- page 88. Exercise 3.20: parts (c), (d), and (e) also require \( m \) and \( n \) to be odd.
• page 89. Exploration 3.29. (a),(b) should be $n = 2^k$ and $n$ an odd prime power.
• page 112. Theorem 5.10: The first equation in the proof should start $\sum_{d\mid p^e} \varphi(d)$
• page 194. First displayed equation should read $14 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3$.
• page 195. Second line of displayed equation is missing $c_i$ in the middle term $= c_0 + \sum_{i=1}^d c_i x^i + \sum_{i=1}^d ic_i x^{i-1} y + \sum_{i=1}^d c_i h(x, y) y^2$
• page 259. The resultant is 48