D. Drucker 9/10/09 version

ERRATA/COMMENTS FOR

Underwood Dudley, *Elementary Number Theory*, Second Edition, 1978

p. 2, footnote: pp. 226ff $\rightarrow$ pp. 227ff
p. 5, line 7: but first we need. $\rightarrow$ but first we need [Delete the period.]
p. 5, line 5 of proof of **Theorem 2**: greater than b $\rightarrow$ greater than or equal to b
p. 5, line 7 of proof of **Theorem 2**: be. $\rightarrow$ be smaller.
p. 6, 1st sentence: Not true. If $a < 0$ and $b > 0$, then $a - b$, $a - 2b$, ..., are all negative and less than a. Thus we need to include $a + b$, $a + 2b$, etc.
p. 6, first two sentences after **Exercise 8**: Replace 69 with 70 (3 times) and add "by Exercise 6" at the end of the second sentence. OR: Change the second sentence to read "From $69 = 3 \cdot 21 + 6$ we get $(69, 21) = (21, 6)$ and from $21 = 3 \cdot 6 + 3$ we get $(6, 3) = 3$."
p. 19, Problem 14: 2^{n-1} $\rightarrow$ $2^n - 1$
p. 22, line 1: odd number of horses and cowboys (plural) $\rightarrow$ odd number of horses (plural)
p. 29, line 4: $m(l_1 - q_2)$ $\rightarrow$ $m(q_1 - q_2)$
p. 30, line 12: $3 \cdot 4 \equiv 2 \cdot 8$ $\rightarrow$ $3 \cdot 4 \equiv 3 \cdot 8$
p. 31, last line: by $\rightarrow$ be
p. 56, line 1: $1/3 + 1/6 = 15/6$ $\rightarrow$ $1/3 + 1/6 = 12/6$ [This is the end of an equation from p. 55.]
p. 62, Problem 12: is $\rightarrow$ are [We need both p and $2p + 1$ to be prime.]
p. 99, first displayed equation: Change the second exponent from $(q - 1)$ to $(q - 1)/2$.
p. 99, equation (6): $\left[\dfrac{28}{35}\right]$ $\rightarrow$ $\left[\dfrac{28}{11}\right]$
p. 126, Problem 15: Does every rational $\rightarrow$ Does every nonegative rational
p. 137, lines -7, -6: and look at $b^2 = m^2 - n^2$ modulo 4. Remember that $x^2 \equiv -1$ agree $\rightarrow$ and we agree
p. 144, line 4 of proof: for some integer k, $k \geq 1$. $\rightarrow$ for some integer k, $1 \leq k < p$.
p. 144, line 7 of proof: for some k_1, with $k_1 < k$. $\rightarrow$ for some k_1, with $1 \leq k_1 < k$.
p. 144, middle of page: The proof shows there is an integer u such that $u^2 \equiv -1 \pmod{p}$; i.e., $u^2 + 1 = kp$ for some k, $k \geq 1$. Choose u so that $|u| < p/2$. Then $kp = u^2 + 1 < p^2/4 + 1 < p^2$, so $k < p$. [We will use this fact later.]
p. 145, last two sentences of proof of **Lemma 4**: Change to: Thus $k \mid p$, but since p is prime and $1 \leq k < p$, we must have $k = 1$. It follows that $x^2 + y^2 = p$ and the lemma is proved.
p. 147, line 20: for which $g(k)$ is known. $\rightarrow$ for which $g(k)$ is not known.
p. 152, line 2: $mp = x^2 + v^2 + 1^2 + 0^2$ $\rightarrow$ $mp = x^2 + y^2 + 1^2 + 0^2$.
p. 157, line 9: For $n = -1$ $\rightarrow$ For $N = -1$
p. 225, line -9: Ivan Niven and H. S. Zukerman $\rightarrow$ Ivan Niven and H. S. Zuckerman
p. 231, answer to last part of Section 3, Problem 3: $x = 1$, $y = 6$ and $x = 3$, $y = 1$ $\rightarrow$ $x = 6$, $y = 1$ and $x = 1$, $y = 3$
p. 232, answer to Section 6, Problem 7: 101 $\rightarrow$ 31
p. 233, answer to Section 9, Problem 15: 5, 8, and 12 $\rightarrow$ 5, 8, 10, and 12
p. 234, answer to Section 16, Problem 3: 625 $\rightarrow$ 629
p. 244, answer to Miscellaneous Problem 29: $(1 - x^2)$ $\rightarrow$ $(1 - x)^2$