Errata for *Elementary Number Theory*

page	line	reads	should read
ix	6	$ax + b$	$ax + by$
2	-6	suceed	succeed
3	8	composite	*composite*
5	5,6	;	,
7	1	many primes	many positive primes
8	-9	M_{11213}	$M_?$ (look it up on the internet)
8	-1	Problem 6.21 ...	replace with text below
9	-0		see Problems 6.23 and 6.24 below
17	10	$500 = 41 \cdot 12 + 8$	$500 = 41 \cdot 12 + 8,$
18	12	ϕ	φ
21	-8	**Theorem**	**Theorem.**
23	5	$a_j \vert (n_i, n_j) \vert$	$a_j((n_i, n_j))$
23	18	$2a_2$	$2a_1$
23	-4	Prove	Prove that when $n > 1$
25	2	arithmetic	*arithmetic*
25	-5	$m > 0$	$m > 1$
25	-2	$(f \vert)$	(f)
27	8,16,-10	$f\ ($	$f($
28	4	$(-1)^{(p-1/2)}$	$(-1)^{(p-1)/2}$
28	8	whichever	which
28	14	Example 9, and	Example 9 and
28	16	Theorem 17, and	Theorem 17 and
29	1	Lemma 13.2	Lemma 12.2
29	11	!	! .
30	-5	$z \in \mathbb{Z}$	$z \in \mathbb{Z}.$
32	-10	$\bar{g}(x^p - x)$	$\bar{g}\ \ (x^p - x)$
33	15	S_k^n	S_k^{p-1}
33	-6		(add) In how many ways?

page	line	reads	should read
33	-0		see Problem 15.15 below
36	12	r_{i+1}	r_i
39	15	$g^{\mathrm{ind}}g^{(a)}$	$g^{\mathrm{ind}_g(a)}$
39	-9	$\mathrm{ind}_g(a+b)$	$\mathrm{ind}_g(ab)$
41	-1	$g_1, \ldots, g$	$g_1, \ldots, g_r$
43	7	$\mathbb{Z}_{n_i}$	$\mathbb{Z}_{n_1}$
47	1	$\mathbb{Z}_{2_\alpha}$	$\mathbb{Z}_{2^\alpha}$
48	6	only at 0,	only at 1, the identity,
49	-9	$(1+m_\alpha p)^p$	$(1+m_\alpha p^\alpha)^p$
49	-10,-1	ϕ (three times)	φ (three times)
51	-8	ϕ (twice)	φ (twice)
52	-2	$h_1^{\varphi(p_1\alpha_1)}$	$h_1^{\varphi(p_1^{\alpha_1})}$
52	-1	$h_1^{\phi(p_1\alpha_1)}$	$h_1^{\varphi(p_1^{\alpha_1})}$
53	2	ϕ	φ
53	-9	β_{-1}	β_{00}
53	-9	$\mathbb{Z}_2^{\alpha-2}$	$\mathbb{Z}_{2^{\alpha-2}}$
54	7	$\nu(n)/\|\phi(n)$	$\nu(n)\|\phi(n)$
63	10	$\ldots(p)$	$\ldots(p)$.
65	2	$\frac{p-1}{2}$	$\frac{p-1}{2}$
66	-7	For example,	(new paragraph) For example,
74	-10	$p2 \equiv (3)$	$p \equiv 2\ (3)$
76	-5	Corollary 4.2	Corollary 26.2
80	8	$4u^2-2u^2$	$4u^2-2y^2$
81	11	integers 501, 503, and	integers 503 and
81	-0		see Problems 27.15 and 27.16 below
82	3	$(x-y\sqrt{m})(x^2+y\sqrt{m}$	$(x-y\sqrt{m})(x+y\sqrt{m})$
86	-7	$\bar{\omega}+\bar{\omega}=-1$	$\omega+\bar{\omega}=-1$
9	5	$m \not\equiv 1\ (4)$	$m \equiv 1\ (4)$
96	-7	Lemma 32.1	Lemma 31.1
97	7	group U of units	group of units
99	-2	infinitely α	infinitely many α
104	-10	$\|N(\beta-\tau)\|$	$\|N(\beta-\alpha\tau)\|$

page	line	reads	should read
107	-9	$= \pm 4 \cdot 5$	$= \pm 5$
107	-8	$(\frac{3}{5})$	$\left(\frac{3}{5}\right)$
112	14	$\mathbf{B}(m)\mu.$	$\mathbf{B}(m).$
112	15	$\pi \vert N(\pi) \vert n \vert ab = \alpha\bar{\alpha}\beta\bar{\beta}$	$\pi \vert N(\pi) \Rightarrow \pi \vert n \Rightarrow \pi \vert ab \Rightarrow \pi \vert \alpha\bar{\alpha}\beta\bar{\beta}$
114	2	$\tau =$	$\tau' =$
114	-4	$\cdots \pi_k^{\alpha_k}$	$\cdots \pi_k^{\gamma_k}$
121	-2	unequivalent	inequivalent
126	-13	$\sum_{i=j}^n$	$\sum_{i=1}^n$
127	-1	$\alpha\alpha =$	$\alpha\alpha' =$
129	-11	$(N(\alpha^*)^{-1}\alpha^*) =$	$(N(\alpha^*)^{-1}\alpha^*)\alpha =$
130	4	D (twice)	$\mathbf{D}$ (twice)
131	-9	any γ which left divides α and β.	if any γ which left divides α and β also divides δ.
133	-8	π	p
138	-0		see Problem 41.52 below
140	-1	$(u + v^2)$	$(u + v)^2$
142	5	we were done	we are done
148	5	one of the six	one of the eight
156	2	noncummutative	noncommutative
175	3	$\mathbb{N}(x)$	$N(x)$
175	4	$\Phi(\mathbf{n})$	$\Phi(n)$
175	8,9	$\mathbb{R}$ (four times)	R (four times)
175	9	(x)	$[x]$
178		Improper unit, 108, 134, 168	Improper unit, 94, 108, 134, 168

6.21* (page 8). Suppose $(m, n) = 1$ so that the fraction m/n is written in "lowest terms." When does

$$\frac{m}{n} = x^2 + y^2$$

have a solution in rational numbers x and y?

6.23 (page 9). Show that there are infinitely many *negative* primes of the form $4n+1$.

6.24 (page 9). Prove: for every n

$$\begin{array}{lll} 3 \not| n & \text{implies} & 3 | n^2 - 1 \\ 5 \not| n & \text{implies} & 5 | n^4 - 1 \\ 7 \not| n & \text{implies} & 7 | n^6 - 1 \end{array}$$

Generalize if you can.

15.15* (page 33). Generalize Thue's Theorem (14.4): Suppose n is not a perfect square, $A > 0$ and $z \in \mathbb{Z}$. Then the congruence

$$xz \equiv y \ (n)$$

has a solution $< x, y >$ for which $|x| < A\sqrt{n}$, $|y| < \sqrt{n}/A$, and x and y are not both 0.

27.15* (page 81). Improve Lemma 26.3 by showing that it remains true when $|k| \leq |m|$ is replaced by $|k| \leq 2\sqrt{|m|}$.

27.16* (page 81). Prove that

$$x^2 + 41y^2 = p$$

has a solution for the odd prime p if and only if $\left(\frac{-41}{p}\right) = 1$ and characterize those primes another way.

41.52* (page 138). Show $A(41)$ is a unique factorization domain. (Hint: see Problem 27.16.)