This may not be a complete list of the solutions. Problems with sufficient solutions in the back of the text were not included.

Problem 3.94: *Let a and b be nonzero integers. Prove that there is a natural number m such that*

(i) $a|m$ *and* $b|m$, *and*
(ii) *if c is an integer such that* $a|c$ *and* $b|c$, *then* $m|c$.

Proof. Let $S = \{n \in \mathbb{N} : a|n \text{ and } b|n\}$. Since $ab \in S$, $S \neq \emptyset$. Thus, by the Least-Natural-Number-Principle, there is a smallest element of S. Let m be this smallest element. Now suppose $a|c$ and $b|c$. Then $c \in S$ and so $c \geq m$. So by the division algorithm for integers, there exist integers p, r such that $0 \leq r < m$ such that $c = mq + r$. Since $a|m$ and $b|m$, then $a|r$ and $b|r$. If $c \neq 0$, then r is an element of S smaller than m. Thus, $r = 0$ and $m|c$. ■

Problem 3.96: *If $a, b \in \mathbb{N}$, then prove that* $\gcd(a, b) \times \text{lcm}(a, b) = ab$.

Proof. Let $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$. Since $d|a$ and $d|b$, there exist integers p and q such that $a = dp$ and $b = dq$. Moreover, $\gcd(p, q) = 1$ – otherwise, if $\gcd(p, q) = d' > 1$, then dd' is a common divisor of a and b which is larger than d. Since $a|m$, there exists an integer r such that $m = ar$, and so $m = dpr$. Since $b|m$ and $b = dq$, $dq|dpr$. Then $q|pr$, and since $\gcd(p, q) = 1$, $q|r$ by Corollary 3.13. Thus, we have dpq divides $m = dpr$. Now $a|dpq$ and $b|dpq$ implies that $m|dpq$ because dpq is a common multiple of a and b and m is the least common multiple of a and b. Therefore,

$$m = dpq = \frac{(dp)(dq)}{d} = \frac{ab}{d}.$$

■

Problem 3.98: *Prove Corollary 3.11: If a, b, and c are integers such that a and b are relatively prime and $a|bc$, then $a|c$.*

Proof. Let $a, b, c \in \mathbb{Z}$ such that $\gcd(a, b) = 1$ and $a|bc$. By Theorem 3.10, there are integers m and n such that $1 = ma + nb$. Then $c = mac + nbc$. Since $a|bc$, there exists some integer q such that $bc = aq$. Thus, $c = mac + naq = a(cm + nq)$ and a divides c. ■

Problem 3.100: *Prove Corollary 3.13: Let a and b be integers, and let p be a prime number. If p divides ab, then p divides a or p divides b.*

Proof. Suppose p does not divide a. Then by Theorem 3.12, a and p are relatively prime. So by Corollary 3.11, $p|b$. ∎

Problem 3.103: *Let a and b be integers not both zero, and let d be a natural number such that d divides a and d divides b. Prove that* $\gcd(a,b) = d$ *if and only if* $\gcd(a/d, b/d) = 1$.

Proof. Let a and b be integers not both zero, and let d be a natural number such that d divides a and d divides b.

($\Rightarrow$) Suppose $\gcd(a,b) = d$. Then by Theorem 3.10, there exist integers m and n such that $ma+nb = d$. Then $m\frac{a}{d}+n\frac{b}{d} = 1$. Therefore, by Theorem 3.10, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

($\Leftarrow$) Suppose $\gcd(a/d, b/d) = 1$. Then by Theorem 3.10, there exist integers m and n such that $m\frac{a}{d} + n\frac{b}{d} = 1$. Thus $ma + nb = d$. Now suppose for the sake of contradiction that c is a common divisor of a and b such that $c > d$. Then $m\frac{a}{c} + n\frac{b}{c} = \frac{d}{c}$, which is a contradiction, because the left hand side is an integer while the right hand side is not. Therefore d is the greatest common divisor of a and b. ∎

Problem 3.104: *A fraction a/b is said to be in lowest terms provided* $\gcd(a,b) = 1$. *Two fractions a/b and c/d are said to be equivalent provided $ad = bc$. Prove that every fraction is equivalent to a fraction in lowest terms.*

Proof. Let $a, b \in \mathbb{Z}$. Let $d = \gcd(a,b)$. By Problem 103, $\gcd(a/d, b/d) = 1$. Note that $\frac{a/d}{b/d}$ is equivalent to a/b because $(a/d)b = (b/d)a$. Therefore a/b is equivalent to the fraction $\frac{a/d}{b/d}$, which is in lowest terms. ∎

Problem 3.105: *Find a fraction that is equivalent to 1739/4042 that is written in lowest terms.*

We use the Euclidean algorithm to find $\gcd(1739, 4042)$.

$$
\begin{aligned}
4042 &= 2(1739) + 564 \\
1739 &= 3(564) + 47 \\
564 &= 12(47) + 0
\end{aligned}
$$

and so $\gcd(1739, 4042) = 47$ and

$$\frac{1739}{4042} = \frac{1739/47}{4042/47} = \frac{37}{86}.$$

Problem 3.110: *Let $p, q \in \mathbb{Z}$ such that 3 divides $p^2 + q^2$. Prove that 3 divides p and 3 divides q.*

Proof. Let $n \in \mathbb{N}$. Then there exist integers k and $0 \leq r \leq 2$ such that $n = 3k + r$. Then $n^2 + 1 = 3(3k^2 + 2kr) + r^2 + 1$, where $0 \leq r \leq 2$. Hence, $n^2 + 1$ is not divisible by 3, since $r^2 + 1$ is not divisible by 3 for $r \in \{0, 1, 2\}$. This then implies that $n^2 + 4$ is not divisible by 3. So for any natural number n, neither $n^2 + 1$ nor $n^2 + 4$ is divisible by 3.

Now let $p = 3j + r$ for some $j, r \in \mathbb{Z}$ with $0 \leq r \leq 2$. Then $p^2 + q^2 = 3(3j^2 + 2jr) + q^2 + r^2$ and since $3|(p^2 + q^2)$, we must have $3|(q^2 + r^2)$. Since 3 does not divide either $q^2 + 1$ or $q^2 + 4$ (corresponding to the cases $r = 1$ and $r = 2$, respectively), $r = 0$. Therefore, 3 divides both p and q. ■

Problem 3.116: *Prove that the diophantine equation $6x + 15y = 83$ does not have a solution.*

Proof. Since $3 = \gcd(6, 15)$ and 3 does not divide 83, by Theorem 3.16(a), $6x + 3y = 83$ does not have a solution. ■