HW1 Solutions

1.49 Let $p_1, p_2, p_3, \ldots$ be the list of the primes in ascending order: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and so forth. Define $f_k = p_1 p_2 \cdots p_k + 1$ for $k \geq 1$. Find the smallest k for which f_k is not a prime.
Solution. f_1, f_2, f_3, f_4, and f_5 are prime, but

$$f_6 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509.$$

1.50 Prove that if d and d' are nonzero integers, each of which divides the other, then $d' = \pm d$.
Solution. Assume that $d = ad'$ and $d' = bd$. Then

$$d = ad' = abd,$$

so that canceling d gives $1 = ab$. As a and b are nonzero integers, $|a| \geq 1$ and $|b| \geq 1$. But $1 = |ab| = |a|\,|b|$ gives $|a| = 1 = |b|$. Hence, $a = 1 = b$ or $a = -1 = b$.

1.54 **(i)** Prove that if n is ***squarefree*** (i.e., $n > 1$ and n is not divisible by the square of any prime), then $\sqrt{n}$ is irrational.
Solution. We rewrite the proof of Proposition 1.14. Suppose, on the contrary, that $\sqrt{n}$ is rational, where n is squarefree; that is, $\sqrt{n} = a/b$. We may assume that a/b is in lowest terms; that is, $(a, b) = 1$. Squaring, $a^2 = nb^2$. Let p be a prime divisor of n, so that $n = pq$. Since n is squarefree, $(p, q) = 1$. By Euclid's lemma, $p \mid a$, so that $a = pm$, hence $p^2m^2 = a^2 = pqb^2$, and $pm^2 = qb^2$. By Euclid's lemma, $p \mid b$, contradicting $(a, b) = 1$.

(ii) Prove that $\sqrt[3]{2}$ is irrational.
Solution. Assume that $\sqrt[3]{4} = a/b$, where $(a, b) = 1$. Then $4b^3 = a^3$, so that a is even; say, $a = 2m$. Hence $4b^3 = 8m^3$; canceling, $b^3 = 2m^3$, forcing b to be even. This contradicts $(a, b) = 1$.

1.55 **(i)** Find $d = \gcd(12327, 2409)$, find integers s and t with $d = 12327s + 2409t$, and put the fraction 2409/12327 in lowest terms.

Solution. One uses the Euclidean algorithm to get: $(12327, 2409) = 3$ and $3 = 12327 \cdot 299 - 2409 \cdot 1530$; the fraction $2409/12327 = 803/4109$ is in lowest terms.

(ii) Find $d = \gcd(7563, 526)$, and express d as a linear combination of 7563 and 526.

Solution. The Euclidean algorithm gives

$$(7563, 526) = 1 \text{ and } 1 = 532 - 526 - 37 - 7563.$$

(iii) Find $d = \gcd(73122, 7404621)$ and express d as a linear combination of 73122 and 7404621.

Solution. Here are the equations of the Euclidean algorithm:

$$\begin{aligned}
7404621 &= 101 \cdot 73122 + 19299 \\
73122 &= 3 \cdot 19299 + 15225 \\
19299 &= 1 \cdot 15225 + 4074 \\
15225 &= 3 \cdot 4074 + 3003 \\
4074 &= 1 \cdot 3003 + 1071 \\
3003 &= 2 \cdot 1071 + 861 \\
1071 &= 1 \cdot 861 + 210 \\
861 &= 4 \cdot 210 + 21 \\
210 &= 10 \cdot 21.
\end{aligned}$$

We conclude that the gcd is 21. Following the algorithm in the text, we find that

$$21 = 34531 \cdot 73122 - 341 \cdot 7404621.$$

1.60 If a and b are relatively prime and if each divides an integer n, prove that their product ab also divides n.

Solution. Assume that $(a, b) = 1$ and $n = ak = b\ell$. By Corollary 1.40, $b \mid ak$ implies $b \mid k$. Thus, $k = bk'$ and so $n = ak = abk'$.

1.60 If a and b are relatively prime and if each divides an integer n, prove that their product ab also divides n.

Solution. Assume that $(a, b) = 1$ and $n = ak = b\ell$. By Corollary 1.40, $b \mid ak$ implies $b \mid k$. Thus, $k = bk'$ and so $n = ak = abk'$.

1.60 If a and b are relatively prime and if each divides an integer n, prove that their product ab also divides n.

Solution. Assume that $(a, b) = 1$ and $n = ak = b\ell$. By Corollary 1.40, $b \mid ak$ implies $b \mid k$. Thus, $k = bk'$ and so $n = ak = abk'$.

1.64 If F_n denotes the nth term of the Fibonacci sequence 0, 1, 1, 2, 3, 5, 8, . . ., prove, for all $n \geq 1$, that F_{n+1} and F_n are relatively prime.

Solution. The hint refers to the fact, which is the key step in antanairesis, that $(a, b) = (a - b, b)$ whenever $a > b$. The proof is by induction on $n \geq 1$. The base step $n = 1$ is true, for $(F_2, F_1) = (1, 1) = 1$. For the inductive step, use antanairesis and the defining recurrence,

$$\begin{aligned}(F_{n+2}, F_{n+1}) &= (F_{n+1} - F_n, F_{n+1}) \\ &= (F_n, F_{n+1}) = 1.\end{aligned}$$

Here is a proof that is a variation of the same idea. Let $n \geq 1$ be the smallest integer for which F_{n+1} and F_n have gcd $d > 1$. We note that $n > 1$ because $(F_2, F_1) = (1, 1) = 1$, and so $n - 1 \geq 1$. But if d is a common divisor of F_{n+1} and F_n, then d divides $F_{n-1} = F_{n+1} - F_n$, so that $(F_n, F_{n-1}) \neq 1$. This contradicts n being the smallest index for which $(F_{n+1}, F_n) \neq 1$.

1.67 **(i)** Consider a complex number $z = q + ip$, where $q > p$ are positive integers. Prove that

$$(q^2 - p^2, 2qp, q^2 + p^2)$$

is a Pythagorean triple by showing that $|z^2| = |z|^2$.

Solution. If $z = q + ip$, then $|z^2| = |z|^2$, by part (i). Now $z^2 = (q^2 - p^2) + i2qp$, so that $|z^2| = (q^2 - p^2)^2 + (2qp)^2$. On the other hand, $|z|^2 = (q^2 + p^2)^2$. Thus, if we define $a = q^2 - p^2$, $b = 2qp$, and $c = q^2 + p^2$, then $a^2 + b^2 = c^2$ and (a, b, c) is a Pythagorean triple.

(ii) Show that the Pythagorean triple (9, 12, 15) (which is not primitive) is not of the type given in part (i).

Solution. Suppose there are q and p for (9, 12, 15). Then $2qp = 12$ and $qp = 6$. Since $q > p$ are positive integers, the only possibilities are $q = 6$ and $p = 1$ or $q = 3$ and $p = 2$. The first possibility gives the Pythagorean triple (12, 35, 37) while the second gives the Pythagorean triple (5, 12, 13).

(iii) Using a calculator which can find square roots but which can display only 8 digits, show that

$$(19597501, 28397460, 34503301)$$

is a Pythagorean triple by finding q and p.

Solution. If q and p exist, then we have

$$q^2 + p^2 = 34503301$$
$$q^2 - p^2 = 19597501.$$

Therefore, $2p^2 = 14905800$ and $p^2 = 7452900$. Hence, $p = 2730$. Finally, $2qp = 28397460$, and so $q = 5201$. Since we were able to find q and p, the original trio does form a Pythagorean triple.