PROBLEMS

1. (a) Find $(34, 55)$ using the Euclidean Algorithm.

   (b) Find $(2^2 3^3 5^5 7^7, 2^7 3^5 5^3 7^2)$.

   (c) Find $(2^2 7^3 19^5 23^7, 2^7 3^5 5^3 7^2)$.

2. Find the prime factorization of the following numbers:

   (a) 100

   (b) 222

   (c) 5040

   (d) 8000

   (e) 111111

   (f)* 20!

3. Let $a \in \mathbb{Z}$. Prove that:

   (a) $(a, 2a) = a$.

   (b)* $(a, a+1) = 1$.

   (c)* $(a, a+2) = 1$ or 2.

   (d)** $(8a+3, 5a+2) = 1$.

   (e)** $(3a+2, 5a+3) = 1$.

   (f)*** $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$, where $a > 1$ and $m, n \in \mathbb{Z}^+$.

4. Let $a, b \in \mathbb{Z}$ and $(a, b) = 1$. Prove that:

   (a)** $(a+b, a-b) = 1$ or 2.

   (b)** $(a+2b, 2a+b) = 1$ or 3.

   (c)** $(a^2+b^2, a+b) = 1$ or 2.

5. Prove that all of the powers in the prime-power factorization of an integer n are even if and only if n is a perfect square.

6. Which positive integers have exactly three positive divisors? Which have exactly four positive divisors?

7. Prove that if a and b are positive integers and $a^2 \mid b^2$, then $a \mid b$.

8. Prove that if a and b are positive integers and $a^3 \mid b^2$, then $a \mid b$.

9. Prove that if a and b are positive integers with $(a, b) = 1$, then $(a^n, b^n) = 1$ for all $n \in \mathbb{Z}^+$.

10. Prove that if a and b are positive integers with $(a, b) = 1$ and $ab = c^n$, then there are positive integers d and e such that $a = d^n$ and $b = e^n$.

11. Prove that the set of all numbers of the form $a + b\sqrt{-5}$, where a and b are integers, does not enjoy the property of unique factorization.

THEOREMS, EXAMPLES, AND HINTS

<u>THEOREM 1</u>: If a, b, k are integers, then $(a + kb, b) = (a, b)$.

<u>THEOREM 2</u> (Euclid's Lemma): If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. More generally, if a prime p divides a product $a_1 a_2 \dots a_n$, then it must divide at least one of the factors a_i.

<u>THEOREM 3</u>: If $a \geq 2$ is an integer, then there are unique distinct primes p_i and unique integers $e_i > 0$ such that

$$a = p_1^{e_1} \dots p_n^{e_n}.$$

<u>EXAMPLE 1</u>: Let $a \in \mathbb{Z}$. Prove that $(2a + 3, a + 2) = 1$.

<u>Proof</u>: By Theorem 1 we have

$$(2a+3, a+2) = (a+1+a+2, a+2) = (a+1, a+2) = (a+1, a+1+1) = (a+1, 1) = 1. \blacksquare$$

<u>EXAMPLE 2</u>: Let $a, b \in \mathbb{Z}$ and $(a, b) = 1$. Prove that $(a + 3b, a + b) = 1$ or 2.

<u>Proof</u>: By Theorem 1 we have

$$(a + 3b, a + b) = (a + b + 2b, a + b) = (2b, a + b).$$

It is easy to see that $(2b, a + b)$ equals $(b, a + b)$ or $2(b, a + b)$. From this and Theorem 1 it follows that

$$(2b, a + b) = (b, a + b) = (b, a) = 1$$

or

$$(2b, a + b) = 2(b, a + b) = 2(b, a) = 2. \blacksquare$$

<u>EXAMPLE 3</u>: Prove that if a and b are positive integers with $(a, b) = 1$, then $(a^2, b^2) = 1$ for all $n \in \mathbb{Z}^+$.

<u>Proof 1</u>: Assume to the contrary that $(a^2, b^2) = n > 1$. Then there is a prime p such that $p \mid a^2$ and $p \mid b^2$. From this by Euclid's Lemma it follows that $p \mid a$ and $p \mid b$, therefore $(a, b) \geq p$. This is a contradiction. $\blacksquare$

<u>Proof 2</u> (Hint): Just use Theorem 3.

<u>HINTS</u>: In problems 5, 7, 8, 10 use Theorem 3. In problem 11 it is enough to provide an example.