Problem 1

Recall that if $d = (a, b)$ with $a = de$ and $b = df$, then $(e, f) = 1$. That is, if we factor out the GCD from two numbers, the remaining numbers are relatively prime. Show that it is necessary to divide *both* numbers by the GCD. That is, find numbers a and b with $d = (a, b)$, and $a = de$, such that $(e, b) \neq 1$.

Let $a = 4$ and $b = 6$.

$$d = (a, b) = (4, 6) = 2$$

$$a = de \Rightarrow 2 = 4e \Rightarrow e = 2$$

$$(e, b) = (2, 6) = 2 \neq 1$$

Thus, both numbers must be divided by the GCD of a and b.

Problem 2

Which positive integers have exactly three distinct positive divisors? Four?

For any given $a \in \mathbb{N}$, a has at least two factors: 1 and a. If we want additional factors, then there must exist a prime factor f such that $1 < f < a$. Since f is a factor, $f|a \Rightarrow a = fk$ for some $k \in \mathbb{N}, k > 1$.

For a to have only 3 factors, k must be one of $1, f$, or a. $f \cdot a$ is obviously too big and $f \cdot 1 = f$ which is less than a, so k must be f. Thus, for a number to have exactly 3 factors, it must be in the form f^2 where f is a prime integer.

For a to have only 4 factors, k must not be $1, f$, or a. Thus, there are two cases, k is prime or k is not prime. If k is prime, then the factors of a are $1, f, k$, and a. So a will be in the form fk where f and k are prime integers. If k is not prime, then it must be a product of some number of primes. However, if k is a product of primes that are not already factors of a, then a will have more than 4 factors. So, k must be factors of a prime which divides a. The only such prime is f, so k is a power of f. We see that, in order to have 4 factors, k must be f^2, as the factors of a will then be $1, f, f^2$, and a. Thus, a must in the form f^3 where f is a prime integer. So, for a to have exactly

4 factors, it must be either in the form fk or f^3 where f and k are prime integers.

Problem 3

Prove that if $(a, b) = 1$ then $(a, b^n) = 1$ for any positive integer n. Then go on to show that $(a^m, b^n) = 1$ for any positive integers m and n.

We will use strong induction to prove this.
Base Case: Let $n = 1$. $(a, b^1) = (a, b) = 1$ since given. Thus, our base case is true.
Inductive Hypothesis: Assume that for a k and all $j \in \mathbb{N}$ such that $1 \leq k \leq j$, $(a, b^k) = 1$.
We need to show that $(a, b^{k+1}) = 1$.

$$(a, b^{k+1})$$

$$= (a, b^k \cdot b)$$

By the inductive hypothesis, $(a, b^k) = 1$. So

$$= (a, b)$$

By the inductive hypothesis once more, $(a, b) = 1$. Thus, $(a, b^{k+1}) = 1$. Thus, by induction, we have shown that $(a, b^n) = 1$ for $n \in \mathbb{N}$. By letting b^n be some arbitrary integer c, we can repeat the same induction to prove $(a^m, c) = 1$ for all positive integers m. We can then substitute c for b^n to show that $(a^m, b^n) = 1$ for all positive integers m and n.

Problem 4

Prove the converse to #3. That is, if there are positive integers m and n such that $(a^m, b^n) = 1$ then a and b are relatively prime.

Let us instead prove the contrapositive. Let $d = (a, b)$ and $d > 1$. $d|a$ and $d|b$. Following this, we can say $d|(a \cdot a^{m-1}) \Rightarrow d|a^m$ and $d|(b \cdot b^{n-1}) \Rightarrow d|b^n$. Since d is a common divisor, $(a^m, b^n) \geq d \neq 1$. Since we have proven the contrapositive, the original statement is true: for any $m, n \in \mathbb{Z}$, if $(a^m, b^n) = 1$ then $(a, b) = 1$.

Problem 5

Prove this corollary: $(a^n, b^n) = (a, b)^n$ (even when a and b are not relatively prime).

Let $d = (a, b)$. Then, there exists a $e, f \in \mathbb{Z}$ such that $a = de$ and $b = df$ and $(e, f) = 1$.

$$\begin{gathered}(a^n, b^n) \\ = ((de)^n, (df)^n) \\ = (d^n e^n, d^n f^n)\end{gathered}$$

Since $(e, f) = 1$ and following our proof from problem 3, we can say that $(d^n e^n, d^n f^n) = d^n \cdot (e^n, f^n) = d^n \cdot 1 = d^n$. Since $(a, b) = d$, $(a, b)^n = d^n$. Since $d^n = d^n$, we have shown that $(a^n, b^n) = (a, b)^n$.

Problem 6: (Extra Credit)

Given that $(a, b) = 1$, what can you determine (with proof, of course!) about $(a^2 + b^2, a + b)$?

We can rewrite $(a^2 + b^2, a + b)$:

$$\begin{gathered}(a^2 + b^2, a + b) \\ = ((a + b)^2 - 2ab, a + b) \\ = ((a + b)^2 - 2ab + (a + b)((-1)(a + b)), a + b) \\ = (-2ab, a + b) \\ = (2ab, a + b)\end{gathered}$$

Since $(a, b) = 1$, $(a, a + b) = 1$, and thus, $(ab, a + b) = 1$. Since, $(ab, a + b) = 1$, the only other possible factor that can divide both $2ab$ and $a + b$ is 2. When we test, we see that if $a + b$ is even, it will be divisible by 2 and $(a^2 + b^2, a + b) = 2$. If $a + b$ is odd, then $(a^2 + b^2, a + b) = 1$.