due Jan 31 | Homework Set 3 (section 1.2 & 1.3) | Name: _____

1. If a divides c and b divides c, must ab divide c? Why or why not. What if $\gcd(a, b) = 1$?

If a divides c and b divides c, then ab does not have to divide c. For example, let $c = 12$, $a = 4$, and $b = 6$. Here 4 and 6 both divide 12, but $4 \cdot 6 = 24$ does not. Note $\gcd(4,6) = 2$.

However, if the $\gcd(a,b) = 1$, the statement is true.

Let a, b, and c be integers such that both a and b divide c and $\gcd(a,b) = 1$. By Theorem 1.3 (or the GCD=1 Theorem), there exist integers u and v such that $1 = au + bv$. By the definition of divides, there exist integers r and t such that $c = ar$ and $c = bt$. Combining these we get that

$$\begin{aligned} c = c \cdot 1 &= c(au + bv) = c(au) + c(bv) = (bt)(au) + (ar)(bv) = b(t(au)) + a(r(bv)) \\ &= b((ta)u) + a((rb)v) = b((at)u) + a((br)v) = b(a(tu)) + a(b(rv)) \\ &= (ba)(tu) + (ab)(rv) = (ab)(tu) + (ab)(rv) = (ab)(tu + rv). \end{aligned}$$

Thus, by definition, ab divides c.

2. Let a, b, c, and d be integers. If $\gcd(a, b) = c$ and b divides ad, prove that b also divides cd.

Let a, b, c, and d be integers such that $c = \gcd(a,b)$ and b divides ad. By definition, there exists an integer t such that $ad = bt$. By Theorem 1.3, there exist integers u and v such that $c = au + bv$. Combining these, we get that

$$\begin{aligned} cd = (au + bv)d &= (au)d + (bv)d = a(ud) + b(vd) = a(du) + b(vd) \\ &= (ad)u + b(vd) = (bt)u + b(vd) = b(tu) + b(vd) = b(tu + vd). \end{aligned}$$

Hence, by definition, b divides cd.

3. Prove that $\sqrt{10}$ is irrational.

Suppose $\sqrt{10}$ is rational. By definition, there exist integers a and b such that $\gcd(a,b) = 1$ and $\sqrt{10} = a/b$. Thus, $10 = (a/b)^2 = a^2/b^2$, which is equivalent to $a^2 = 10b^2$. Since $10 = 2 \cdot 5$, we get that 2 and 5 divide a^2. By Corollary 1.9, 2 divides a. By definition, there exists an integer k such that $a = 2k$. Thus, $a^2 = (2k)^2 = 4k^2$. Since $a^2 = 10b^2$, $2k^2 = 5b^2$. Then 2 divides $5b^2$, and by Theorem 1.5, 2 divides b^2. Corollary 1.9 yields that 2 divides b. Hence, we've shown that 2 divides both a and b. By Corollary 1.4, 2 divides $\gcd(a,b)$. But $\gcd(a,b) = 1$, so we reach a contradiction.

Thus, $\sqrt{10}$ must be irrational.

4. Let a and b be integers, and let n and m be positive integers such that $n \leq m$. If p is prime and $\gcd(a,b) = p$, prove that p^n divides $\gcd(a^n, b^m)$. Prove or disprove that $\gcd(a^n, b^m) = p^n$.

Let a and b be integers. Let n and m be positive integers such that $n \leq m$. Let p be prime such that $\gcd(a,b) = p$. By definition, there exist integers k and t where $a = pk$ and $b = pt$. By Theorem 1.3 there are integers u and v such that

$$\gcd(a^n, b^m) = a^n u + b^m v = (pk)^n u + (pt)^m v = (p^n k^n)u + (p^m t^m)v$$
$$= p^n(k^n u) + p^m(t^m v) = p^n(k^n u) + p^n(p^{m-n}(t^m v)) = p^n\left[k^n u + p^{m-n}(t^m v)\right].$$

By definition, p^n divides $\gcd(a^n, b^m)$.

However, there is no guarantee that $p^n = \gcd(a^n, b^m)$. For example, let $a = 45$ and $b = 21$ with $n = 4$ and $m = 5$. Then $\gcd(a,b) = \gcd(45,21) = 3$. But $\gcd(a^n, b^m) = \gcd(a^4, b^5) = \gcd(45^4, 21^5) = 3^5 \neq 3^n$.

5. While these are both computational questions, be sure to write your conclusion in a complete sentence(s).
   a. Express 8,069,490 as a product of primes.

Written as a product of primes, we have

$$8{,}069{,}490 = 2 \cdot 3^3 \cdot 5 \cdot 11^2 \cdot 13 \cdot 19.$$

   b. Find the greatest common divisor of 304 and 5985, using the Euclidean Algorithm. Use your answer to write the gcd(304,5985) as a linear combination of 304 and 5985.

Let $a = 5985$ and $b = 304$.
Apply the Euclidean Algorithm:

$$5985 = 304(19) + 209$$
$$304 = 209(1) + 95$$
$$209 = 95(2) + 19$$
$$95 = 19(5) + 0.$$

Thus, the $\gcd(304, 5985) = 19$.
Now, using backward substitution, we will find a u and v which satisfy: $19 = 5985u + 304v$.

$$19 = 209 - 95(2)$$
$$= 209 - [304 - 209(1)](2)$$
$$= 209 \cdot 3 + 304(-2)$$
$$= [5985 - 304(19)] \cdot 3 + 304(-2)$$
$$= 5985 \cdot 3 + 304(-59)$$

Thus, $u = 3$ and $v = -59$ to give us the linear combination:

$$\gcd(304, 5985) = 19 = 5985 \cdot 3 - 304 \cdot 59.$$