Math 446 - Homework # 1

In the following problems, x, y, z, m, n are integers.

1. *Prove that if $x|y$ and $y|z$, then $x|z$.*

   Solution: Since $x|y$ we have that $xs = y$ for some integer s. Since $y|z$ we have that $yt = z$ for some integer t. Therefore, $x(st) = (xs)t = yt = z$. Hence $x|z$.

2. *Prove that if $x|y$ and $m|n$, then $xm|yn$.*

   Solution: Since $x|y$ we have that $xs = y$ for some integer s. Since $m|n$ we have that $mt = n$ for some integer t. Hence $xm(st) = (xs)(mt) = yn$. Therefore $xm|yn$.

3. *Prove that if $xy|z$, then $x|z$.*

   Solution: Since $xy|z$ we have that $(xy)k = z$ for some integer k. Hence $x(yk) = z$. Thus, $x|z$.

4. *Prove that $xz|yz$ if and only if $x|y$.*

   Solution: Suppose that $xz|yz$. Then $(xz)k = yz$ for some integer k. Hence $xk = y$. Thus $x|y$.

   Now suppose that $x|y$. Then there exists an integer n with $xn = y$. Multiplying by z gives us that $(xz)n = yz$. Hence $xz|yz$.

5. *Prove that if $x|(y+z)$ and $x|y$, then $x|z$.*

   Solution: Since $x|(y+z)$ there exists an integer s with $xs = y + z$. Since $x|y$ there exists an integer t with $xt = y$. Therefore,

   $$z = xs - y = xs - xt = x(s - t).$$

   Hence $x|z$.

6. *Prove that if $x|y$ and $x|z$, then $x|(my + nz)$.*

   Solution: Since $x|y$ we have that $xs = y$ for some integer s. Since $x|z$ we have that $xt = z$ for some integer t. Therefore

   $$my + nz = m(xs) + n(xt) = x(ms + nt).$$

   Hence $x|(my + nz)$.

7. Let $n > 1$ be an integer.

   (a) n is composite if and only if there exist positive integers a and b such that $n = ab$ and $1 < a < n$ and $1 < b < n$.

   Solution: Let $n > 1$ be an integer. Suppose that n is composite. Then since n is not prime, there exists a positive integer a that divides n where $1 < a < n$. By the definition of division, this means that there exists another positive integer b with $n = ab$. Note that $b = n/a$. Since $1 < a < n$ we have that $1 > 1/a > 1/n$. Thus $n > n/a > 1$. That is, $1 < b < n$. This gives us that $n = ab$ where $1 < a < n$ and $1 < b < n$.

   Conversely suppose that $n = ab$ where $1 < a < n$ and $1 < b < n$. Then n has a positive divisor a that is not equal to 1 or n. Hence n is not prime. That is, n is composite.

   (b) n is composite if and only if there exist positive integers a and b such that $n = ab$ and $1 < a$ and $1 < b$.

   Solution: Suppose n is composite. Then from the first part of this exercise, there exists positive integers a and b with $1 < a < n$ and $1 < b < n$. So $1 < a$ and $1 < b$.

   Suppose now that there exists positive integers a and b with $n = ab$ and $1 < a$ and $1 < b$. Since $1 < a$ we have that $1/a < 1$. Therefore, $n/a < n$. Since $b = n/a$ this gives us that $b < n$. Therefore, b is a divisor of n with $1 < b < n$. Thus n cannot be prime since we have a positive divisor that is not equal to 1 or n. So n is composite.

8. *Prove that* 4 *does not divide* $n^2 + 2$ *for any integer* n.

   Solution: We prove this by contradiction. Suppose that 4 divides $n^2 + 2$ for some integer n. Then there exists an integer m with $4m = n^2 + 2$.

   Suppose that n is even. Then $n = 2k$ for some integer k. Hence $4m = 4k^2 + 2$. Thus $2m = 2k^2 + 1$. This is a contradiction since we can't have an even integer equal to an odd integer.

   Suppose that n is odd. Then $n = 2j + 1$ for some integer j. Hence $4m = (2j+1)^2 + 2 = 4j^2 + 4j + 3 = 2(2j^2 + 2j + 1) + 1$. Again we have an even integer equal to an odd integer, which can't happen.

   Hence there cannot exist an integer n where 4 divides $n^2 + 2$.

9. *Prove that any prime of the form $3k+1$ is of the form $6s+1$.*

   Solution: Let p be a prime of the form $3k+1$ where k is a positive integer.

   Suppose that k is even. Then $k = 2s$ for some integer s. Hence $p = 3k+1 = 6s+1$, which is what we want to show.

   Suppose that k is odd. Then $k = 2t+1$ for some integer t. Hence $p = 3k+1 = 3(2t+1)+1 = 6t+4 = 2(3t+2)$ is even. Since p is prime and p is even, we must have that $p = 2$ (since 2 is the only even prime). But then $2 = 2(3t+2)$. This implies that $3t+2 = 1$. But then $t = -1/3$ which isn't an integer. This contradicts the fact that t is an integer. Hence this case, where k is odd, cannot occur.

   In summary, if p is a prime of the form $3k+1$ then k must be even and p is of the form $6s+1$.

10. *Show that n^4+4 is composite for all $n > 1$.*

    Solution: Before we begin the proof, note that if $n = 1$ then $n^4+4 = 5$ which is prime, that is, not composite. This is why we must have $n > 1$.

    We break the proof into two cases.

    Suppose that $n > 1$ is even. Then $n = 2k$ for some integer $k \geq 1$. Hence
    $$n^4 + 4 = 16k^4 + 4 = 4(4k^4 + 1).$$
    Note that $4k^4 + 1 \geq 4(1)^4 + 1 = 5$. Hence we have factored n^4+4 into a product xy with $x > 1$ and $y > 1$. Thus, by exercise 7b, n^4+4 is composite.

    Suppose that n is odd. Then $n = 2j+1$ for some integer $j \geq 1$. Hence
    $$\begin{aligned} n^4 + 4 &= 16j^4 + 32j^3 + 24j^2 + 8j + 5 \\ &= (4j^2+1)(4j^2+8j+5). \end{aligned}$$
    Note that the first factor above satisfies $4j^2+1 \geq 4(1)^2+1 = 5$. The second factor satisfies $4j^2+8j+5 \geq 4(1)^2+8(1)+5 = 17$. Hence we have factored n^4+4 into a product xy with $x > 1$ and $y > 1$. Thus, by exercise 7b, n^4+4 is composite.

11. Let $n > 1$ be an integer. If $2^n - 1$ is a prime, then n is prime. [An integer of the form $2^p - 1$, where p is prime is called a Mersenne prime.]

Solution: We prove the contrapositive: Let $n > 1$. If n is composite, then $2^n - 1$ is composite.

Suppose that $n > 1$ is composite. Then $n = ab$ where $a > 1$ and $b > 1$ by exercise 7. Note that

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^{2a} + 2^a + 1).$$

Note that the first factor from the equation above satisfies $2^a - 1 \geq 2^2 - 1 = 3$. And the second factor satisfies

$$2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^{2a} + 2^a + 1 \geq 2^a + 1 \geq 2^2 + 1 = 5.$$

Therefore, we have factored $2^n - 1$ into a product xy where $x > 1$ and $y > 1$. By exercise 7, we have that $2^n - 1$ is composite.

12. *Let d and n be integers, both not zero. If $d|n$ and $d|n + 1$, then $d = 1$ or $d = -1$.*

    Solution: Since $d|n$ we have that $n = dk$ for some integer k. Since $d|(n + 1)$ we have that $n + 1 = dm$ for some integer m. By subtracting these two equations we get

    $$1 = (n + 1) - n = dm - dk = d(m - k).$$

    Hence $d|1$. Therefore, $d = 1$ or $d = -1$.