Do the following exercises from the text:
Section 2.5: 1(b), (c), 3, 5, 6

1. Find the canonical representation of each of the following nu;mbers.

(b) $3718 = 2 \cdot 11 \cdot 13^2$ **(c)** $3234 = 2 \cdot 3 \cdot 7^2 \cdot 11$

3. $(3718,\ 3234) = 2^1 \cdot 3^0 \cdot 7^0 \cdot 11^1 \cdot 13^0 = 22$

$[3718,\ 3234] = 2^1 \cdot 3^1 \cdot 7^2 \cdot 11^1 \cdot 13^2 = 546,546$

5. $\tau(3718) = 2 \cdot 2 \cdot 3 = 12$, $\sigma(3718) = \frac{2^2-1}{2-1} \cdot \frac{11^2-1}{11-1} \cdot \frac{13^3-1}{13-1} = 3 \cdot 12 \cdot 183 = 6588$

6. Find the sum of the squares of the positive divisors of 4725.

► **Solution.** The sum of the divisors of $4725 = 3^3 \cdot 5^2 \cdot 7$ is

$$\sigma(4725) = (1 + 3 + 3^2 + 3^3)(1 + 5 + 5^2)(1 + 7).$$

Similarly, the sum of the squares of the divisors is given by

$$\begin{aligned} \sigma^*(4725) &= (1 + 3^2 + 3^4 + 3^6)(1 + 2^2 + 5^4)(1 + 7^2) \\ &= \frac{(3^2)^4 - 1}{3^2 - 1} \cdot \frac{(5^2)^3 - 1}{5^2 - 1} \cdot \frac{(7^2)^2 - 1}{7^2 - 1} \\ &= 26,691,000. \end{aligned}$$

◄

Section 3.2: 3, 6

3. Try to prove that there are infintely many primes of the form $4k + 1$ by imitating the proof of Theorem 3.3. Why does the proof break down?

► **Solution.** Suppose there are only finitely many primes of the form $4k + 1$, say p_1, p_2, …, p_r. Consider the number $m = 4p_1p_2 \cdots p_r + 1$, which is of the form $4k + 1$. Since $m > p_i$ for $i = 1, 2, \ldots, 4$ and $p_1, p_2, \ldots, p_r$ are the only primes of this form, then m must be composite. Therefore, by the Fundamental Theorem of Arithmetic, m must have prime divisors. At this point, the argument of the proof of Theorem 3.3 breaks down since we cannot argue as we did there that m must (in this case) have a prime divisor of the form $4k + 1$. The problem is that the product of two numbers of the form $4k + 3$ is a number of the form $4k + 1$. Thus, all of the prime factors of m could be of the form $4k + 3$, which would not give a new prime of the form $4k + 1$. ◄

6. If $p \geq q \geq 5$ and p and q are bot primes. show that $24 \mid (p^2 - q^2)$.

► **Solution.** If p and q are both primes with $p \geq q \geq 5$, then $(2,\, p) = (3,\, p) = (2,\, q) = (3,\, q) = 1$. Thus, $(6,\, p) = (6,\, q) = 1$. Therefore, we can write $p = 6a \pm 1$ and $q = 6b \pm 1$ with a and b integers and then,

$$\begin{aligned} p^2 - q^2 &= (6a \pm 1)^2 - (6b \pm 1)^2 \\ &= 36(a^2 - b^2) \pm 12(a - b) \\ &= 12(a - b)[3(a + b) \pm 1]. \end{aligned}$$

If a and b are both even or both odd then $a - b$ is even and it follows that $24 \mid (p^2 - q^2)$. If one of a and b is even and the other is odd, then $a + b$ is odd so that $3(a + b) \pm 1$ is even and again $24 \mid (p^2 - q^2)$. ◄

Section 3.4: 8

8. Let $q = 2^{n-1} \cdot p$ where $p = 2^n - 1$ is a Mersenne prime. List all of the divisors of q and show directly that q is a perfect number.

► **Solution.** The divisors of q are 2^k for $0 \leq k \leq n - 1$ and $2^k p$ for $0 \leq k \leq n - 1$. Thus,

$$\begin{aligned} \sigma(q) &= (1 + 2 + \cdots + 2^{n-1}) + (1 + 2 + \cdots + 2^{n-1})p \\ &= \frac{2^n - 1}{2 - 1} + \frac{2^n - 1}{2 - 1}p \\ &= (2^n - 1)(1 + p) \\ &= 2^n(2^n - 1) = 2q. \end{aligned}$$

Therefore, q is a perfect number. ◄

Problems not from the text:

1. Prove that any integer of the form $3n + 2$ has a prime factor of the same form.

► **Solution.** All primes except for 3 must have remainder 1 or 2 when divided by 3. Thus they will have the form $3k + 2$ or $3k + 1$. The product of integers of the form $3k + 1$ will also have the form $3k + 1$. Thus, if all the prime divisors of an integer m have the form $3k + 1$, then so does m. Therefore, since the given integer has the form $3n + 2$, it is not possible to have all of the prime divisors of the form $3k + 1$, so at least 1 will have to have the form $3k + 2$. ◄

2. If $p \geq 5$ is a prime number, show that $p^2 + 2$ is composite.

[*Hint:* p must have one of the two forms $6k + 1$ or $6k + 5$. (Verify this if you use it.)]

► **Solution.** Since $p \geq 5$ and p is prime, then $(2,\, p) = (3,\, p) = 1$ so $(6,\, p) = 1$ and we can write $p = 6k \pm 1$. Then

$$p^2 + 2 = (6k \pm 1)^2 + 2 = (36k^2 \pm 12k + 1) + 2 = 3(12k^2 \pm 4k + 1).$$

Hence $3 \mid (p^2 + 2)$ so $p^2 + 2$ is composite. ◄

3. (a) Given that p is a prime and $p \mid a$, prove that $p^n \mid a^n$.

   ► **Solution.** If $p \mid a$ then $a = pc$ for some integer c. Then $a^n = p^n c^n$ so $p^n \mid a^n$. ◄

   (b) If $(a,\, b) = p$ where p is prime, what are the possible values of $(a^2,\, b^2)$, $(a^2,\, b)$, and $(a^3,\, b^3)$?

   ► **Solution.** Since $(a,\, b) = p$ then $a = pc$, $b = pd$ where $(c,\, d) = 1$. Then $(c^2,\, d^2) = 1$ so $a^2 = p^2c^2$ and $b^2 = p^2d^2$ so $p^2 = (a^2,\, b^2)$. $(a^2,\, b) = p$ if $p^2 \nmid b$ or p^2 if $p^2 \mid b$, $(a^3,\, b^3) = p^3$. ◄