MATH 135 Algebra, Solutions to Assignment 6

1: Find the prime factorization of each of the following integers.

(a) 30!

Solution: First, let us describe a method for finding the exponent of a prime p in the prime factorization of $n!$ for any positive integer n. Note that $n!$ is the product of the numbers $1, 2, 3, \cdots, n$. The multiples of p that occur in this list are $p, 2p, 3p, \cdots, \left\lfloor \frac{n}{p} \right\rfloor$, so there are $\left\lfloor \frac{n}{p} \right\rfloor$ multiples of p in the list. Similarly, there are $\left\lfloor \frac{n}{p^2} \right\rfloor$ multiples of p^2 in the list and $\left\lfloor \frac{n}{p^3} \right\rfloor$ multiples of p^3 and so on. Thus the exponent of the prime p in the prime factorization of $n!$ is equal to $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$.

Using the above rule, the exponent of 2 in 30! is $\lfloor \frac{30}{2} \rfloor + \lfloor \frac{30}{4} \rfloor + \lfloor \frac{30}{8} \rfloor + \lfloor \frac{30}{16} \rfloor = 15 + 7 + 3 + 1 = 26$, the exponent of 3 is $\lfloor \frac{30}{3} \rfloor + \lfloor \frac{30}{9} \rfloor + \lfloor \frac{30}{27} \rfloor = 10 + 3 + 1 = 14$, the exponent of 5 is $\lfloor \frac{30}{5} \rfloor + \lfloor \frac{30}{25} \rfloor = 6 + 1 = 7$, the exponent of 7 is $\lfloor \frac{30}{7} \rfloor = 4$, the exponent of 11 is $\lfloor \frac{30}{11} \rfloor = 2$, the exponent of 13 is $\lfloor \frac{30}{13} \rfloor = 3$, and the exponents of 17, 19, 23 and 29 are all equal to 1. Thus we have

$$30! = 2^{26} \cdot 3^{14} \cdot 5^7 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29\,.$$

(b) $\binom{30}{10}$

Solution: Using our rule from part (a) we find that

$$\begin{aligned} 10! &= 2^{5+2+1} \cdot 3^{3+1} \cdot 5^2 \cdot 7\ , \text{ and} \\ 20! &= 2^{10+5+2+1} \cdot 3^{6+2} \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \end{aligned}$$

and so

$$\begin{aligned} \binom{30}{10} = \frac{30!}{10!20!} &= \frac{2^{26} \cdot 3^{14} \cdot 5^7 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29}{(2^8 \cdot 3^4 \cdot 5^2 \cdot 7)(2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19)} \\ &= 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29\,. \end{aligned}$$

(c) $2^{36} - 1$

Solution: Recall that $a^2 - b^2 = (a-b)(a+b)$, $a^3 - b^3 = (a-b)(a^2+ab+b^2)$ and $a^3+b^3 = (a+b)(a^2-ab+b^2)$. Use these rules repeatedly to get

$$\begin{aligned} 2^{36} - 1 &= (2^{18} - 1)(2^{18} + 1) \\ &= (2^9 - 1)(2^9 + 1)(2^6 + 1)(2^{12} - 2^6 + 1) \\ &= (2^3 - 1)(2^6 + 2^3 + 1)(2^3 + 1)(2^6 - 2^3 + 1)(2^2 + 1)(2^4 - 2^2 + 1)(2^{12} - 2^6 + 1) \\ &= 7 \cdot 73 \cdot 9 \cdot 57 \cdot 5 \cdot 13 \cdot 4033 \\ &= 7 \cdot 73 \cdot 3^2 \cdot 3 \cdot 19 \cdot 5 \cdot 13 \cdot 4033\,. \end{aligned}$$

Note that 73 is prime, since $\lfloor \sqrt{73} \rfloor = 8$, and none of the primes 2, 3, 5, 7 is a factor of 73. To determine whether 4033 is prime, we test every prime p with $p \leq \lfloor \sqrt{4033} \rfloor = 63$ to see if it is a factor. Using the Sieve of Eratosthenes, we find that the primes we need to check are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61\,,$$

and when we test these we find that 37 is a factor, indeed $4033 = 37 \cdot 109$. Note that 109 is prime, since $\lfloor \sqrt{109} \rfloor = 10$ and none of the primes 2, 3, 5, 7 is a factor of 109. Thus we obtain the prime factorization

$$2^{36} - 1 = 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73 \cdot 109\,.$$

2: (a) Let $a = 8400$. Find the number of positive factors of a.

Solution: First let us find a formula for the number of positive factors of a given positive integer n in terms of its prime factorization. Suppose that a positive integer n has prime factorization $n = {p_1}^{k_1}{p_2}^{k_2}\cdots{p_l}^{k_l}$. The positive divisors of n are the integers of the form ${p_1}^{j_1}{p_2}^{j_2}\cdots{p_l}^{j_l}$ with $0 \le j_i \le k_i$ for each i. Since for each i there are (k_i+1) possible choices for j_i, the total number of positive factors of n is equal to

$$\prod_{i=1}^{l}(k_i+1) = (k_1+1)(k_2+1)\cdots(k_l+1)\,.$$

Note that the prime factorization of 8400 is $2^4 \cdot 3^1 \cdot 5^2 \cdot 7^1$, so by the above formula, it has $5\cdot 2\cdot 3\cdot 2 = 60$ positive factors.

(b) Find the number of positive integers whose prime factors are 2, 3 and 5 and which have exactly 100 positive divisors.

Solution: The positive integers with prime factors 2, 3 and 5 are of the form $2^k \cdot 3^l \cdot 5^m$ with $k, l, m \ge 1$. By the formula in part (a), this integer has $(k+1)(l+1)(m+1)$ positive divisors, so to have 100 positive divisors, we need to have $(k+1)(l+1)(m+1) = 100$. We list all possible ways to factor 100 into three integers which are greater than 1:

$2\cdot2\cdot25$	$4\cdot5\cdot5$	$5\cdot2\cdot10$	$10\cdot2\cdot5$	$25\cdot2\cdot2$
$2\cdot5\cdot10$		$5\cdot4\cdot5$	$10\cdot5\cdot2$	
$2\cdot10\cdot5$		$5\cdot5\cdot4$		
$2\cdot25\cdot2$		$5\cdot10\cdot2$		

Since there are 12 ways to factor 100 into three integers greater than 1, there are 12 such integers.

(c) Let $a = \prod_{k=1}^{6} k^k$. Find the number of factors (positive or negative) of a which are either perfect squares or perfect cubes (or both).

Solution: Let us find the prime factorization of a. We have

$$\begin{aligned} a &= \prod_{k=1}^{6} k^k = 1^1\cdot2^2\cdot3^3\cdot4^4\cdot5^5\cdot6^6 \\ &= 2^2\cdot3^3\cdot2^8\cdot5^5\cdot2^6\cdot3^6 \\ &= 2^{16}\cdot3^9\cdot5^5\,. \end{aligned}$$

The positive factors of a are of the form $2^i\cdot3^j\cdot5^k$ with $0\le i\le16$, $0\le j\le9$, and $0\le k\le5$. The factors of a which are perfect squares are of the form $2^i\cdot3^j\cdot5^k$ with $i = 0,2,4,\cdots,16$, $j = 0,2,4,6,8$, and $k = 0,2,4$. There are 9 choices for i, 5 for j, and 3 for k, so the number of square factors is equal to $9\cdot5\cdot3 = 135$. The factors of a which are perfect cubes are of the form $\pm2^i\cdot3^j\cdot5^k$ with $i = 0,3,6,9,12,15$, $j = 0,3,6,9$ and $k = 0,3$. There are 6 choices for i, 4 for j, and 2 for k, so there are $6\cdot4\cdot2 = 48$ positive cube factors and another 48 negative cube factors. Finally, note that some of the 48 positive cube factors are also squares, indeed the sixth powers are both cubes and squares. The sixth powers are of the form $2^i\cdot3^j\cdot5^k$ with $i = 0,6,12$, $j = 0,6$ and $k = 0$, so there are $3\cdot2\cdot1 = 6$ sixth powers. Thus the total number of factors (positive or negative) which are squares or cubes is $135+48+48-6 = 225$.

3: In parts (a) and (b), find the prime factorization of $\gcd(a,b)$ and of $\text{lcm}(a,b)$.

(a) $a = 2^4 \cdot 3^2 \cdot 5 \cdot 11$ and $b = 2^2 \cdot 5^3 \cdot 7 \cdot 11$

Solution: We have $\gcd(a,b) = 2^2 \cdot 5 \cdot 11$ and $\text{lcm}(a,b) = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$.

(b) $a = 25!$ and $b = (5500)^3(1001)^2$.

Solution: Using the formula that we found above in Problem 1(a) we have

$$\begin{aligned} a &= 2^{12+6+3+1} \cdot 3^{8+2} \cdot 5^{5+1} \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \\ &= 2^{22} \cdot 3^{10} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \end{aligned}$$

and we have

$$b = (2^2 \cdot 5^3 \cdot 11)^3 (7 \cdot 11 \cdot 13)^2 = 2^6 \cdot 5^9 \cdot 7^2 \cdot 11^5 \cdot 13^2$$

and so

$$\begin{aligned} \gcd(a,b) &= 2^6 \cdot 5^6 \cdot 7^2 \cdot 11^2 \cdot 13 \\ \text{lcm}(a,b) &= 2^{22} \cdot 3^{10} \cdot 5^9 \cdot 7^3 \cdot 11^5 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \end{aligned}$$

(c) Find the number of pairs of integers (a,b) with $0 \leq a \leq b$ such that $\gcd(a,b) = 60$ and $\text{lcm}(a,b) = 4200$.

Solution: To get $\gcd(a,b) = 60 = 2^2 \cdot 3 \cdot 5$ and $\text{lcm}(a,b) = 4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$, we must have $a = 2^{j_1} \cdot 3^{j_2} \cdot 5^{j_3} \cdot 7^{j_4}$ and $b = 2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \cdot 7^{k_4}$ with $\{j_1, k_1\} = \{2,3\}$, $\{j_2, k_2\} = \{1,1\}$, $\{j_3, k_3\} = \{1,2\}$ and $\{j_4, k_4\} = \{0,1\}$. There are two choices for the pair (j_1, k_1), namely $(j_1, k_i) = (2,3)$ or $(3,2)$, only one choice for (j_2, k_2), namely $(j_2, k_2) = (1,1)$, and two choices for each of the pairs (j_3, k_3) and (j_4, k_4). Thus there are $2 \cdot 1 \cdot 2 \cdot 2 = 8$ pairs of positive integers (a,b) with $\gcd(a,b) = 60$ and $\text{lcm}(a,b) = 4200$. Four of these pairs (a,b) will have $a < b$ and the other four (obtained by interchanging a and b) will have $a > b$. $\big($Incidentally, the four pairs are $(a,b) = (60, 4200), (120, 2100), (300, 840), (420, 600)\big)$.

4: (a) Show that for all positive integers a and b we have $a\big|b$ if and only if $a^2\big|b^2$.

Solution: Write $a = {p_1}^{j_1}{p_2}^{j_2}\cdots{p_n}^{j_n}$ and $b = {p_1}^{k_1}{p_2}^{k_2}\cdots{p_n}^{k_n}$ where the p_i are distinct primes. Then we have $a^2 = {p_1}^{2j_1}{p_2}^{2j_2}\cdots{p_n}^{2j_n}$ and $b^2 = {p_1}^{2k_1}{p_2}^{2k_2}\cdots{p_n}^{2k_n}$, and so

$$a\big|b \iff j_i \le k_i \text{ for all } i \iff 2j_i \le 2k_i \text{ for all i} \iff a^2\big|b^2\,.$$

(b) Show that for all positive integers a, b and c, if $c\big|ab$ then $c\big|\gcd(a,c)\gcd(b,c)$.

Solution: Write $a = {p_1}^{j_1}{p_2}^{j_2}\cdots{p_n}^{j_n}$, $b = {p_1}^{k_1}{p_2}^{k_2}\cdots{p_n}^{k_n}$ and $c = {p_1}^{m_1}{p_2}^{m_2}\cdots{p_n}^{m_n}$. Note that

$$\begin{aligned} ab &= {p_1}^{j_1+k_1}{p_2}^{j_2+k_2}\cdots{p_n}^{j_n+k_n} \\ \gcd(a,c) &= {p_1}^{\min\{j_1,m_1\}}{p_2}^{\min\{j_2,m_2\}}\cdots{p_n}^{\min\{j_n,m_n\}} \\ \gcd(b,c) &= {p_1}^{\min\{k_1,m_1\}}{p_2}^{\min\{k_2,m_2\}}\cdots{p_n}^{\min\{k_n,m_n\}} \\ \gcd(a,c)\gcd(b,c) &= {p_1}^{\min\{j_1,m_1\}+\min\{k_1,m_1\}}{p_2}^{\min\{j_2,m_2\}+\min\{k_2,m_2\}}\cdots{p_n}^{\min\{j_n,m_n\}+\min\{k_n,m_n\}}\,. \end{aligned}$$

Suppose that $c\big|ab$ so we have $m_i \le j_i + k_i$ for all i. Fix an index i. We consider three cases.

Case 1. If $m_i \le j_i$ then we have $m_i = \min\{j_i,m_i\} \le \min\{j_i,m_i\} + \min\{k_i,m_i\}$.

Case 2. If $m_i \le k_i$ then we have $m_i = \min\{k_i,m_i\} \le \min\{j_i,m_i\} + \min\{k_i,m_i\}$.

Case 3. If $m_i \ge j_i$ and $m_i \ge k_i$ then we have $m_i \le j_i + k_i = \min\{j_i,m_i\} + \min\{k_i,m_i\}$.

In all three cases we have $m_i \le \min\{j_i,m_i\} + \min\{k_i,m_i\}$. Thus $c\big|\gcd(a,c)\gcd(b,c)$ as required.

(c) Show that for all positive integers a and b we have $\gcd(a,b) = \gcd\big(a+b, \mathrm{lcm}(a,b)\big)$.

Solution: Let $d = \gcd(a,b)$, $m = \mathrm{lcm}(a,b)$, and $e = \gcd(a+b,m)$. We must show that $d = e$. Write $a = dk$ and $b = dl$ so we have $\gcd(k,l) = 1$ (by Proposition 2.27(ii)) and $m = dkl$ (by Theorem 2.59). By question 4(b) on assignment 4, we have

$$e = \gcd(a+b,m) = \gcd(d(k+l),dkl) = d\gcd(k+l,kl)\,,$$

so it suffices to show that $\gcd(k+l,kl) = 1$. Suppose, for a contradiction, that $\gcd(k+l,kl) \ne 1$. Let p be a common prime factor of $k+l$ and kl. Since p is prime and $p\big|kl$, we know that $p\big|k$ or $p\big|l$ by Theorem 2.53. If $p\big|k$ then since $p\big|(k+l)$ we also have $p\big|l$ by Proposition 2.11(ii). Similarly, if $p\big|l$ then since $p\big|(k+l)$ we also have $p\big|k$. In either case we see that p is a common prime factor of k and l, which contradicts the fact that $\gcd(k,l) = 1$.

5: A **Hilbert number** is a positive integer of the form $n = 1 + 4k$ for some integer $k \geq 0$. A **Hilbert prime** is a Hilbert number $n > 1$ whose only Hilbert number factors are 1 and n.

(a) List the first 20 Hilbert primes.

Solution: We can list the Hilbert primes using the same method used in the Sieve of Eratosthenes: list the Hilbert numbers $1, 5, 9, 13, \cdots$, cross off 1 (which is not a Hilbert prime), circle 5 (the first Hilbert prime), cross off the multiples of 5 (that is $25, 45, 65, 85, 105, \cdots$), circle 9 (the second Hilbert prime), cross off the multiples of 9 ($81, 117, \cdots$), and so on. The first 20 Hilbert primes are

$$5, 9, 13, 17, 21, 29, 33, 37, 41, 49, 53, 57, 61, 69, 73, 77, 89, 93, 97, 101$$

(b) Show that every Hilbert number greater than 1 is either a Hilbert prime or a product of Hilbert primes.

Solution: We simply copy the proof of Proposition 2.51. Suppose, for a contradiction, that the result is false. Let n be the smallest Hilbert number which is greater than 1 and is neither a Hilbert prime nor a product of Hilbert primes. Since n is not a Hilbert prime, it has a Hilbert number factor other than 1 and n, so it can be factored as $n = rs$ for some Hilbert numbers r and s with $1 < r, s < n$. By our choice of n, each of the Hilbert numbers r and s is either a Hilbert prime or a product of Hilbert primes. It follows that $n = rs$ is a product of Hilbert primes, giving the desired contradiction.

(c) Show that the factorization of a Hilbert number into Hilbert primes is not always unique.

Solution: Note that $9 \cdot 49 = 21 \cdot 21$.