Chapter 2

Unique Factorization

2.1 Exercises

1. (a) $3^2 \cdot 5^4$, (b) 5625 is a square

2. (a) $2^6 \cdot 3^3$, (b) 1728 is a cube

3. Use Theorem 2.2 with $a = b$. Since $p \mid a \cdot a$, we have $p \mid a$ or $p \mid a$. This means that $p \mid a$.

4. Since $p^2 \mid ab$, it follows that p^2 occurs in the prime factorization of ab. Let p^i be the power of p in the factorization of a and let p^j be the power of p in the prime factorization of b. Then p^{i+j} is the power of p in the prime factorization of ab, so $i + j \geq 2$. Since $\gcd(a, b) = 1$, either $i = 0$ or $j = 0$. Therefore, either $i \geq 2$ or $j \geq 2$, which means that either $p^2 \mid a$ or $p^2 \mid b$.
Another solution: Since $p \mid ab$, either $p \mid a$ or $p \mid b$. Let's assume that $p \mid a$. Since $\gcd(a, b) = 1$, we have $\gcd(p^2, b) = 1$. By Proposition 1.13 (with $(a, b, c) = (p^2, b, a)$), we must have $p^2 \mid a$.

5. (a) Write $a = 2^{a_2}3^{a_3}\cdots$ and $b = 2^{b_2}3^{b_3}\cdots$. By Proposition 2.6, $na_p \leq nb_p$ for each p, so $a_p \leq b_p$ for each p. Use Proposition 2.6 again to get $a \mid b$.
(b) Write $a = 2^{a_2}3^{a_3}\cdots$ and $b = 2^{b_2}3^{b_3}\cdots$. Proposition 2.6 says that $ma_p \leq nb_p$ for each p. Since $m \geq n$, $a_p \leq b_p$ for each p. Use Proposition 2.6 again to get $a \mid b$.
(c) Let $a = 4, b = 2, m = 1, n = 2$.

6. (a) and (b) Write

$$a = 2^{a_2}3^{a_3}5^{a_5}\cdots \quad \text{and} \quad b = 2^{b_2}3^{b_3}5^{b_5}\cdots.$$

Then $a^n = 2^{na_2}3^{na_3}5^{na_5}\cdots$ and $b^n = 2^{nb_2}3^{nb_3}5^{nb_5}\cdots$. Let $d_p = \min(a_p, b_p)$. Then $nd_p = \min(na_p, nb_p)$. Proposition 2.7 says that

$$\gcd(a^n, b^n) = 2^{nd_2}3^{nd_3}5^{nd_5}\cdots = \left(2^{d_2}3^{d_3}5^{d_5}\cdots\right)^n = \gcd(a, b)^n.$$

7. Let $d = \gcd(a, c)$. Then $d \mid c$, so $d \mid a + b$. Since $d \mid a$, we have $d \mid b$.

8. Let $d = \gcd(a, b)$. By Proposition 1.3, $d \mid ax + by = 1$. Therefore, $d = 1$.

9. The answer is 3: If we have 4 consecutive integers, one of them is divisible by 4. An example of 3 consecutive squarefree integers is 1, 2, 3.

10. The answer is 8: If we have 9 consecutive odd integers, one of them is divisible by 9. This can be seen as follows: Let the consecutive odd integers be $n+2j$ for $0 \leq j \leq 8$. Write $n = 18q+r$ with $0 \leq r < 18$. Since n is odd and $18j$ is even, r must be odd. Write $r = 2k+1$ with $0 \leq k \leq 8$. If $0 \leq k \leq 4$, then

$$n + 2(4-k) = (18q + 2k + 1) + 2(4-k) = 18q + 9,$$

which is a multiple of 9. If $5 \leq k \leq 8$, then

$$n + 2(13-k) = (18q + 2k + 1) + 2(13-k) = 18q + 27,$$

which is a multiple of 9.
It is possible to have 8 consecutive odd squarefree integers: 29, 31, 33, 35, 37, 39, 41, 43. Note that we couldn't start at 11, because then the 8th number would be 25, which is not squarefree.

11. Let $n = 2^{n_2}3^{n_3}\cdots$. Then $r = n_2$ and $m = 3^{n_3}\cdots$.

12. (a) and (b) Let $d = \gcd(a^n, b)$, for some $n \geq 1$. If q is a prime dividing d, then $q \mid a$ and $q \mid b$, so $q \mid \gcd(a, b) = p$. Therefore, the only prime factor of d is p, so $d = p^j$ for some j. Since $p \mid a^2$ and $p \mid b$, we have $j \geq 1$. Suppose $j > n$. Then $p^j \mid a^n$ implies that $p^2 \mid a$ (look at the power of p in a). But $p^j \mid b$, and $j > n \geq 1$, so $p^2 \mid b$. Therefore, $p^2 \mid \gcd(a, b) = p$, which is a contradiction. Therefore, $1 \leq j \leq n$. Each of these is possible: Let $a = p$ and $b = p^j$ with $j \leq n$. Then $\gcd(a^n, b) = \gcd(p^n, p^j) = p^j$. To summarize, $\gcd(a^n, b) = p^j$ for some j with $1 \leq j \leq n$.

13. Since $\gcd(a, p^2) = p$, the power of p in the prime factorization of a is p^1. Since $\gcd(b, p^3) = p^2$, the power of p in the prime factorization of b is p^2. (a) The power of p in the prime factorization of ab is p^3, so $\gcd(ab, p^4) = p^3$. (b) Let $d = \gcd(a+b, p^4)$. Then d is a power of p. Since $p \mid a$ and $p \mid b$, we have $p \mid a+b$. Suppose $p^2 \mid a+b$. Since $p^2 \mid b$, we have $p^2 \mid (a+b)-b = a$, which is a contradiction. Therefore, $d = p$.

2.2 Projects

1. (a) If a and b are elements in $\mathcal{H}$, then $a = 1 + 4k_1, b = 1 + 4k_2$. Then

$$ab = (1 + 4k_1)(1 + 4k_2) = 1 + 4(k_1 + k_2) + 16k_1k_2 = 1 + 4k \in \mathcal{H}$$

Therefore, $\mathcal{H}$ is closed under multiplication.

Numbers of the form $3 + 4k$ are not closed under multiplication: $(3 + 4k_1)(3 + 3k_2) = 1 + 4m$ for some integer m.
(For example, $7 \cdot 11 = 77 = 1 + 4 \cdot 19$.)

(b) The first ten Hilbert numbers are $1, 5, 9, 13, 17, 21, 25, 29, 33, 37$.

(c) The first ten Hilbert primes are $5, 9, 13, 17, 21, 28, 33, 37, 41, 49$. The first Hilbert prime that is not a prime number is 9.

(d) Let $p = 3 + 4k_1$ and $q = 3 + 4k_2$ be prime numbers. Then $m = pq = 1 + 4k$ is a Hilbert number. As an integer, m can be factored in exactly one way as a product of primes, namely $m = pq$. If it were possible to factor m as the product of two Hilbert numbers, this would give rise to a factorization (in the integers) of m different from $m = pq$. Since this is impossible, m is a Hilbert prime.

(e) If p is a prime of the form $4k + 1$, then it can't have a non-trivial factorization so it's a Hilbert prime. Now assume that p is a Hilbert prime that is not a prime. Write $p = q_1 q_2 \dots q_n$, as the prime factorization of p. Then none of the q_i can be Hilbert numbers since p cannot factor as a product of Hilbert numbers. Furthermore, n must be even since the product of an odd number of integers of the form $4k + 3$ is not a Hilbert number. Using this, write $p = (q_1 q_2)(q_3 q_4) \dots (q_{n-1} q_n)$. Each pair of products is in $\mathcal{H}$. Therefore, if p is a Hilbert prime, $n = 2$.

(f) $441 = 9 \cdot 49 = 21 \cdot 21$.

(g) Answers will vary. Here are two possibilities.
$4389 = 21 \cdot 209 = 33 \cdot 133 = 57 \cdot 77$
$33649 = 77 \cdot 437 = 133 \cdot 253 = 161 \cdot 209$

(h) We begin the sieve by writing only the integers that are of the form $1 + 4k$. (We've only written these up to 93.)

1	5	9	13	17	21	25	29
33	37	41	45	49	53	57	61
65	69	73	77	81	85	89	93

Ignore 1, put a circle around 5 and then cross out every fifth number.

1	⑤	9	13	17	21	~~25~~	29
33	37	41	~~45~~	49	53	57	61
~~65~~	69	73	77	81	~~85~~	89	93

Now put a circle around 9 (the first number after 5 that has not been crossed out) and cross out every ninth number that's in our array.

1	⑤	⑨	13	17	21	~~25~~	29
33	37	41	~~45~~	49	53	57	61
~~65~~	69	73	77	~~81~~	85	89	93

Continue in this manner, circling the first number that is not crossed out and then crossing out multiples of that number. The final result for the first 32 integers of the form $1 + 4k$ is

1	⑤	⑨	⑬	⑰	㉑	~~㉕~~	㉙
㉝	㊲	㊶	~~㊺~~	㊾	㊸	㊼	㊿
~~(65)~~	(69)	(73)	(77)	~~(81)~~	~~(85)~~	(89)	(93)

2. (a) $[15, 21] = 105,\ [30, 40] = 120,\ [5, 47] = 235$

   (b) $\gcd(15, 60) = 15,\ \ [15, 60] = 60$

   (c) If $d = \gcd(a, b)$, there are integers k_1 and k_2 with

   $$a = k_1 d \text{ and } b = k_2 d.$$

   Since $a \mid [a, b]$ and $b \mid [a, b]$, there are integers k_3 and k_4 with

   $$[a, b] = k_3 a \text{ and } [a, b] = k_4 b.$$

   Therefore

   $$[a, b] = k_3 a = k_3(k_1 d) = (k_3 k_1)d = k \gcd(a, b).$$

   So, $(a, b) \mid [a, b]$.

   (d) Using the notation from (c), $\gcd(a, b) = [a, b]$ if and only if $k_1 k_3 = k_2 k_4 = 1$. Since each k_i is a positive integer, $k_1 = k_2 = k_3 = k_4 = 1$. This means that

   $$\gcd(a, b) = a,\ \ \gcd(a, b) = b,\ \ [a, b] = a,\ \ [a, b] = b,$$

   which forces $a = b$.

   (e) (i) $[p, q] = pq$, (ii) $[pq, p^2 r] = p^2 qr$, (iii) $[pq, 2q^2 r^3] = 2pq^2 r^3$

   (f) Let $a = 2^{a_2} 3^{a_3} \cdots$ and $b = 2^{b_2} 3^{b_3} \cdots$ be the prime factorizations of a and b. Let $c_p = \max(a_p, b_p)$ and let $[a, b] = n$. For n to be divisible by both a and b, each prime p that occurs in the factorization of n must occur to a power at least as big as a_p and b_p. This means that the smallest positive integer that that is divisible by both a and b (i.e. $[a, b]$) is

   $$2^{c_2} 3^{c_3} 5^{c_5} \cdots .$$

   (g) Let $a = 2^{a_2} 3^{a_3} \cdots$ and $b = 2^{b_2} 3^{b_3} \cdots$ be the prime factorizations of a and b. Let $d_p = \min(a_p, b_p)$ and $c_p = \max(a_p, b_p)$. We have already seen that

   $$\gcd(a, b) = 2^{d_2} 3^{d_3} 5^{d_5} \cdots \text{ and that } [a, b] = 2^{c_2} 3^{c_3} 5^{c_5} \cdots .$$

Therefore, the exponent of a prime p in $[a,b]\cdot\gcd(a,b)$ is $\min(a_p,b_p)+\max(a_p,b_p)=a_p+b_p$, which is the same as the exponent of p in ab. Since this is true for each prime, $[a,b]\cdot\gcd(a,b)=ab$.

(h) Since $\gcd(3,6,8)=1$ and $[3,6,8]=24$, their product is 24, which is not equal to $3\cdot 6\cdot 8$.

(i) Let

$$a=2^{a_2}3^{a_3}\cdots,\ b=2^{b_2}3^{b_3}\cdots \text{ and } c=2^{c_2}3^{c_3}\cdots.$$

Since $a\mid c,\ a_p\le c_p$ for all primes p and because $b\mid c,\ b_p\le c_p$ for all primes p. Therefore $\max(a_p,b_p)\le c_p$ for all primes p. Let $[a,b]=2^{m_2}3^{m_3}\cdots$, so $m_p=\max(a_p,b_p)$ for all p. Since $\max(a_p,b_p)\le c_p$, we see that $m_p\le c_p$ and therefore, $[a,b]\mid c$.

Here is an alternate proof.

The division algorithm says that

$$c=q[a,b]+r \quad \text{where } 0\le r<[a,b].$$

Also, $a\mid[a,b]$ and $a\mid c$, so $[a,b]=as_1$ and $c=as_2$ for integers s_1,s_2. So, $as_2=aqs_1+r$ and $a(q_2-qq_1)=r$. So, $a|r$. Similarly, $b|r$. Since $0\le r<[a,b]$, we must have $r=0$ from the definition of $[a,b]$. This means that $c=q[a,b]$, so $[a,b]\mid c$.

(j) We write the solutions as ordered pairs, (a,b).

$$(p^2,1),\ (1,p^2),\ (p^2,p^2),\ (p^2,p),\ (p,p^2).$$

(k) Let $a=p^{a_p}q^{a_q}$ and $b=p^{b_p}q^{b_q}$. If $[a,b]=p^2q$, then $\max(a_p,b_p)=2$ and $\max(a_q,b_q)=1$. If $a_p=2$, there are three choices for b_p. If $b_p=2$ there are only two more choices for a_p since we've already considered $a_p=b_p$. This gives five possible pairs. Similarly if $a_q=1$, there are two choices for b_q and if $b_q=1$ there is only one more choice for a_q. This gives a total of $5\cdot 3=15$ possibilities.

(l) If $a=2^{a_2}3^{a_3}\cdots$ and $b=2^{b_2}3^{b_3}\cdots$ and $[a,b]=n$, then $n_p=\max(a_p,b_p)$. If $n_p=a_p$, there are n_p+1 choices for a_p. If $n_p=b_p$, we have n_p more choices for a_p since the possibility that $a_p=b_p$ was already counted. This gives $2n_p+1$ choices for each prime p and the total number of solutions is

$$(2n_2+1)\,(2n_3+1)\,(2n_5+1)\cdots$$