Divisibility and Factorization

Lakshmy K V
email:kv_lakshmy@cb.amrita.edu
Phone: 9751529221

Number Theory is the branch of mathematics that studies the properties of the integers.

The first property we'll discuss is **divisibility**.

We know:

$$3 \cdot 5 = 15$$

We say that the number 15 is the **product** of the **factors** 3 and 5.

In particular, **3 is a factor of 15**. We write this as:

$$3 \mid 15$$

We say that "**3 divides 15**"

So, the notation

$$x \mid y$$

means that "x divides y."

But more specifically, it means there is another integer k so that

$$x \cdot k = y.$$

Remember: $3 \mid 15$, so what is k?

$$3 \cdot 5 = 15, \quad \text{so} \quad k = 5.$$

Divisiblity

Definition 1: Let $a, b \in \mathbf{Z}$. Then *a divides b*, denoted $a \mid b$, if there exists $c \in \mathbf{Z}$ such that $b = ac$. If $a \mid b$, then a is said to be a *divisor* or *factor* of b. The notation $a \nmid b$ means that a does not divide b.

Example 1:

(a) $3 \mid 6$ since there exists $c \in \mathbf{Z}$ such that $6 = 3c$. Here, $c = 2$. Hence 3 is a divisor of 6.

(b) $3 \nmid 5$ since there does not exist $c \in \mathbf{Z}$ such that $5 = 3c$. Note that c would have to be $\frac{5}{3}$ here and $\frac{5}{3} \notin \mathbf{Z}$. Hence 3 is not a divisor of 5.

(c) $3 \mid -6$ since there exists $c \in \mathbf{Z}$ such that $-6 = 3c$. Here, $c = -2$. Hence 3 is a divisor of -6. In fact, it is easily seen that $\pm 3 \mid \pm 6$.

(d) If $a \in \mathbf{Z}$, then $a \mid 0$ since there exists $c \in \mathbf{Z}$ such that $0 = ac$. Here, $c = 0$. In other words, any integer divides 0.

(e) If $a \in \mathbf{Z}$ and $0 \mid a$, then there exists $c \in \mathbf{Z}$ such that $a = 0c$ if and only if $a = 0$. In other words, the only integer having zero as a divisor is zero.

$x \mid y$ means $x \cdot k = y$ for some integer k.

True/False:

1. $4 \mid 20$ — TRUE, since $4 \cdot 5 = 20$
2. $3 \mid 46$ — FALSE, since $3 \cdot 15 = 45$ and $3 \cdot 16 = 48$
3. $17 \mid 17$ — TRUE, since $17 \cdot 1 = 17$
4. $12 \mid 6$ — FALSE, since $12 \cdot \frac{1}{2} = 6$ but $\frac{1}{2}$ is NOT an integer.
5. $5 \mid 137,560$ — TRUE, since ???

Some properties of divisibility

NOTE:

- In order for $x \mid y$, then it must be true that $x \leq y$.
- For any number x, $\quad 1 \mid x$.
- For any number x, $\quad x \mid x$.

We call 1 and x the **trivial divisors** of x, and usually ignore these when talking about divisors.

Some properties of divisibility

Suppose we know that x, y and z are three numbers so that

$$x \mid y \quad \text{and} \quad y \mid z.$$

Is it true that $x \mid z$??

Example:

$$4 \mid 12 \quad \text{and} \quad 12 \mid 24$$

Is it true that $4 \mid 24$?? YES! (Since $4 \cdot 6 = 24$).

Some properties of divisibility

Suppose we know that x is a number that divides both y and z:

$$x \mid y \quad \text{and} \quad x \mid z.$$

Is it true that $x \mid y + z$??

Example:

$$7 \mid 21 \quad \text{and} \quad 7 \mid 35$$

Is it true that $7 \mid 56$?? YES! (Since $7 \cdot 8 = 56$).

Proposition 1.1: Let $a, b, c \in \mathbf{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: Since $a \mid b$ and $b \mid c$, there exist $e, f \in \mathbf{Z}$ such that $b = ae$ and $c = bf$. Then

$$c = bf = (ae)f = a(ef)$$

and $a \mid c$. ■

Proposition 1.2: Let $a, b, c, m, n \in \mathbf{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid ma + nb$.

Proof: Since $c \mid a$ and $c \mid b$, there exist $e, f \in \mathbf{Z}$ such that $a = ce$ and $b = cf$. Then

$$ma + nb = mce + ncf = c(me + nf)$$

and $c \mid ma + nb$. ■

Theorem *For all $a, b, c \in \mathbb{Z}$, with $a \neq 0$*

- $a|a,\ 1|a;$
- $a|b \Longrightarrow a|-b;$
- $a|b$ *and* $a|c \Longrightarrow a|(b+c);$
- $a|b$ *and* $b|c \Longrightarrow a|c;$
- $a|b$ *and* $b|a \Longrightarrow a = \pm b.$

1. Prove or disprove each statement below.
   (a) $6 \mid 42$
   (b) $4 \mid 50$
   (c) $16 \mid 0$
   (d) $0 \mid 15$
   (e) $14 \mid 997157$
   (f) $17 \mid 998189$
2. Find integers a, b, and c such that $a \mid bc$ but $a \nmid b$ and $a \nmid c$.

4. If $a, b \in \mathbf{Z}$, find a necessary and sufficient condition that $a \mid b$ and $b \mid a$.
5. Prove or disprove the following statements.
   (a) If a, b, c, and d are integers such that $a \mid b$ and $c \mid d$, then $a + c \mid b + d$.
   (b) If a, b, c, and d are integers such that $a \mid b$ and $c \mid d$, then $ac \mid bd$.
   (c) If a, b, and c are integers such that $a \nmid b$ and $b \nmid c$, then $a \nmid c$.
6. *(a)* Let $a, b, c \in \mathbf{Z}$ with $c \neq 0$. Prove that $a \mid b$ if and only if $ac \mid bc$.
   (b) Provide a counterexample to show why the statement of part (a) does not hold if $c = 0$.

10. **(a)** Let $n \in \mathbf{Z}$. Prove that $3 \mid n^3 - n$.
(b) Let $n \in \mathbf{Z}$. Prove that $5 \mid n^5 - n$.
(c) Let $n \in \mathbf{Z}$. Is it true that $4 \mid n^4 - n$? Provide a proof or counterexample.

12. Prove that the square of any odd integer is expressible in the form $8n + 1$ with $n \in \mathbf{Z}$.

Find the number of positive integers not exceeding 500 that are divisible by 3.

Prime Numbers

Definition 5: Let $p \in \mathbf{Z}$ with $p > 1$. Then p is said to be *prime* if the only positive divisors of p are 1 and p. If $n \in \mathbf{Z}$, $n > 1$, and n is not prime, then n is said to be *composite*.

Lemma 1.5: Every integer greater than 1 has a prime divisor.

Proof: Assume, by way of contradiction, that some integer greater than 1, say n, has no prime divisor. By the well-ordering property, we may assume that n is the least such integer. Now $n \mid n$; since n has no prime divisor, n is not prime. So n is composite and consequently there exist $a, b \in \mathbf{Z}$ such that $n = ab$, $1 < a < n$, and $1 < b < n$. Since $1 < a < n$, we have that a has a prime divisor, say p, so that $p \mid a$. But $a \mid n$ so we have that $p \mid n$ by Proposition 1.1 from which n has a prime divisor, a contradiction. So every integer greater than 1 has a prime divisor. ■

Proposition 1.7: Let n be a composite number. Then n has a prime divisor p with $p \leq \sqrt{n}$.

Proof: Since n is a composite number, there exist $a, b \in \mathbf{Z}$ such that $n = ab$, $1 < a < n$, $1 < b < n$, and, without loss of generality, $a \leq b$. Now $a \leq \sqrt{n}$. (If $a > \sqrt{n}$, we have

$$n = ab > \sqrt{n}\sqrt{n} = n$$

which is impossible.) By Lemma 1.5, we have that a has a prime divisor, say p, so that $p \mid a$. But $a \mid n$, so we have that $p \mid n$ by Proposition 1.1. Furthermore, $p \leq a \leq \sqrt{n}$; p is the desired prime divisor of n. ■

Proposition 1.8: For any positive integer n, there are at least n consecutive composite positive integers.

Proof: Given the positive integer n, consider the n consecutive positive integers

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n+1$$

Let i be a positive integer such that $2 \leq i \leq n+1$. Since $i \mid (n+1)!$ and $i \mid i$, we have

$$i \mid (n+1)!+i, \qquad 2 \leq i \leq n+1$$

by Proposition 1.2. So each of the n consecutive positive integers above is composite. ■

18. ***(a)*** **Find 13 consecutive composite positive integers.**

21. Verify Goldbach's Conjecture (Conjecture 2) for the following even integers.
(a) 30
(b) 98

31. Prove or disprove the following conjecture.
Conjecture: If n is a positive integer, then $n^2 - n + 41$ is a prime number.

26. Prove or disprove the following statements.
(a) If p is a prime number, then $2^p - 1$ is a prime number.

We've talked about the **divisors** of an integer:

x **is a divisor of** y if there is an integer k so that

$$x \cdot k = y$$

Shorthand notation:

$$x \mid y.$$

We can list several divisors of any positive integer:

$$36 = 4 \cdot 9$$

$$36 = 6 \cdot 6$$

$$36 = 2 \cdot 18$$

$$36 = 2 \cdot 2 \cdot 3 \cdot 3$$

Which is better?

If we just want to find any two divisors, there may be many ways to do so.

We'd like to be able to find a list of divisors in such a way that the same list is always found.

Instead of looking for any divisors, let's agree to find all prime divisors of a number.

Example:

$$120 = 12 \cdot 10 = 3 \cdot 4 \cdot 2 \cdot 5 = 3 \cdot 2 \cdot 2 \cdot 2 \cdot 5$$

Or,

$$120 = 2 \cdot 60 = 2 \cdot 6 \cdot 10 = 2 \cdot 2 \cdot 3 \cdot 2 \cdot 5$$

We get the same **prime factors**, even though we didn't start with the same initial pair of divisors.

In fact, this will always be true !!

Theorem (The Fundamental Theorem of Arithmetic)

Every positive integer can be written in a unique way as the product of prime divisors.

So, suppose we take any (large) integer.

No matter how we start, we will always end up with the same list of prime divisors that multiply to that large number.

Example:

$$6765 = 5 \cdot 1353 = 5 \cdot 3 \cdot 451 = 3 \cdot 5 \cdot 11 \cdot 41$$

Example:

$$18,200 = 182 \cdot 100 = 2 \cdot 91 \cdot 10 \cdot 10 = 2 \cdot 7 \cdot 13 \cdot 2 \cdot 5 \cdot 2 \cdot 5$$

There's a better way to keep track of these...

$$18,200 = 2^3 \cdot 5^2 \cdot 7 \cdot 13$$

Let's always agree to write the **prime factorization** in order of lowest primes to highest primes.

We know how to find the divisors of any number.

If we're given two numbers, there will be divisors that are common to both numbers.

For example, 24 and 28 have common divisors of 2, 4.

4 is the largest number that is a divisor of both 24 and 28.

Definition

For any two integers x and y, the **greatest common divisor** is the largest number that is a divisor of both x and y.

Example: the greatest common divisor of 24 and 28 is 4.

Notation:

$$\gcd(24, 28) = 4$$

Finding the gcd is not always this easy, though.

But, we have steps to follow in order find it:

1. List the prime factors of each number.
2. Then list all prime factors that are common to each number.
3. The product of these common prime factors is the greatest common divisor.

Example: Find $\gcd(1540, 18200)$.

$$1540 = 154 \cdot 10 = 11 \cdot 14 \cdot 2 \cdot 5 = 11 \cdot 2 \cdot 7 \cdot 2 \cdot 5$$

$$1540 = 2^2 \cdot 5 \cdot 7 \cdot 11$$

$$18,200 = 2^3 \cdot 5^2 \cdot 7 \cdot 13$$

Common factors: $2 \cdot 2 \cdot 5 \cdot 7 = 140$

Therefore,

$$\gcd(1540, 18200) = 140.$$

Example: Find $\gcd(231, 260)$.

$$231 = 3 \cdot 7 \cdot 11$$

$$260 = 2^2 \cdot 5 \cdot 13$$

Common factors: none! (Not true: 1 is always a common factor)

Therefore,

$$\gcd(231, 260) = 1.$$

We say that 231 and 260 are **relatively prime**, since the greatest common divisor is 1.

Proposition 1.10: Let $a, b \in \mathbf{Z}$ with $(a, b) = d$. Then $(a/d, b/d) = 1$.

Proof: Let $(a/d, b/d) = d'$. Then $d' \mid a/d$ and $d' \mid b/d$ so there exist $e, f \in \mathbf{Z}$ such that $a/d = d'e$ and $b/d = d'f$. So $a = d'de$ and $b = d'df$; consequently, we have $d'd \mid a$ and $d'd \mid b$. This implies that $d'd$ is a common divisor of a and b and, since d is the greatest common divisor of a and b, we have $d' = 1$, from which comes the desired result. ■

Theorem 1.4: (The Division Algorithm) Let $a, b \in \mathbf{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbf{Z}$ such that

$$a = bq + r, \qquad 0 \leq r < b$$

(Note that q stands for *quotient* and r stands for *remainder*.)

Proof: Let $q = \left[\frac{a}{b}\right]$ and $r = a - b\left[\frac{a}{b}\right]$. Then $a = bq + r$ is easily checked. It remains to show that $0 \leq r < b$. By Lemma 1.3, we have that

$$\frac{a}{b} - 1 < \left[\frac{a}{b}\right] \leq \frac{a}{b}$$

Multiplying all terms of this inequality by $-b$, we obtain

$$b - a > -b\left[\frac{a}{b}\right] \geq -a$$

Reversing the inequality and adding a to all terms gives

$$0 \leq a - b\left[\frac{a}{b}\right] < b$$

which is precisely $0 \leq r < b$ as desired; so, q and r as defined above have the desired properties. It remains to show the uniqueness of q and r. Assume that

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b$$

and

$$a = bq_2 + r_2, \qquad 0 \leq r_2 < b$$

We must show that $q_1 = q_2$ and $r_1 = r_2$. We have

$$0 = a - a = bq_1 + r_1 - (bq_2 + r_2) = b(q_1 - q_2) + (r_1 - r_2)$$

which implies that

$$r_2 - r_1 = b(q_1 - q_2) \qquad \textbf{(1)}$$

Hence, $b \mid r_2 - r_1$. Now $0 \leq r_1 < b$ and $0 \leq r_2 < b$ imply $-b < r_2 - r_1 < b$; along with $b \mid r_2 - r_1$, we have $r_2 - r_1 = 0$ or $r_1 = r_2$. Now (1) becomes

$$0 = b(q_1 - q_2)$$

Since $b \neq 0$, we have that $q_1 - q_2 = 0$ or $q_1 = q_2$ as desired. ■

Lemma 1.12: If $a, b \in \mathbf{Z}$, $a \geq b > 0$, and $a = bq + r$ with $q, r \in \mathbf{Z}$, then $(a, b) = (b, r)$.

Proof: Let c be a common divisor of a and b. Then $c \mid a$ and $c \mid b$ imply $c \mid a - qb$ by Proposition 1.2, from which $c \mid r$; we then have that c is a common divisor of b and r. Now let c be a common divisor of b and r so that $c \mid b$ and $c \mid r$. Then $c \mid qb + r$ by Proposition 1.2, from which $c \mid a$; we then have that c is a common divisor of a and b. So the common divisors of a and b are the same as the common divisors of b and r from which $(a, b) = (b, r)$. ■

Theorem 1.13: (The Euclidean Algorithm) Let $a, b \in \mathbf{Z}$ with $a \geq b > 0$. By the division algorithm, there exist $q_1, r_1 \in \mathbf{Z}$ such that

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b$$

If $r_1 > 0$, there exist (by the division algorithm) $q_2, r_2 \in \mathbf{Z}$ such that

$$b = r_1q_2 + r_2, \qquad 0 \leq r_2 < r_1$$

If $r_2 > 0$, there exist (by the division algorithm) $q_3, r_3 \in \mathbf{Z}$ such that

$$r_1 = r_2q_3 + r_3, \qquad 0 \leq r_3 < r_2$$

Continue this process. Then $r_n = 0$ for some n. If $n > 1$, then $(a, b) = r_{n-1}$. If $n = 1$, then $(a, b) = b$.

Proof: Note that $r_1 > r_2 > r_3 > \ldots$. If $r_n \neq 0$ for all n, then $r_1, r_2, r_3, \ldots$ is an infinite, strictly decreasing sequence of positive integers, which is impossible. So $r_n = 0$ for some n. Now, if $n > 1$, repeated applications of Lemma 1.12 give

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{n-1}, r_n) = (r_{n-1}, 0) = r_{n-1}$$

as desired. If $n = 1$, the desired statement is obvious. ■

Example 14:

Find $(803, 154)$ by using the Euclidean algorithm.
The notation of Theorem 1.13 is used throughout. Here $a = 803$ and $b = 154$. By the division algorithm,

$$803 = 154 \cdot 5 + 33 \quad \textbf{(2)}$$

Since $r_1 = 33 > 0$ apply the division algorithm to $b = 154$ and $r_1 = 33$ to obtain

$$154 = 33 \cdot 4 + 22 \quad \textbf{(3)}$$

Since $r_2 = 22 > 0$, apply the division algorithm to $r_1 = 33$ and $r_2 = 22$ to obtain

$$33 = 22 \cdot 1 + 11 \quad \textbf{(4)}$$

Since $r_3 = 11 > 0$, we apply the division algorithm to $r_2 = 22$ and $r_3 = 11$ to obtain

$$22 = 11 \cdot 2 + 0$$

Since $r_4 = 0$, the Euclidean algorithm terminates and

$$(803, 154) = r_3 = 11$$

Proposition 1.11: Let $a, b \in \mathbf{Z}$ with a and b not both zero. Then

$$(a, b) = \min\{ma + nb : m, n \in \mathbf{Z}, ma + nb > 0\}$$

Proof: (of Proposition 1.11) Note that $\{ma + nb : m, n \in \mathbf{Z}, ma + nb > 0\} \neq \varnothing$ since, without loss of generality, $a \neq 0$ and then either $1a + 0b > 0$ or $-1a + 0b > 0$. So $\min\{ma + nb : m, n \in \mathbf{Z},\ ma + nb > 0\}$ exists by the well-ordering property; let

$$d = \min\{ma + nb : m, n \in \mathbf{Z}, ma + nb > 0\} = m'a + n'b$$

We first show that $d \mid a$ and $d \mid b$. By the division algorithm, there exist $q, r \in \mathbf{Z}$ such that

$$a = dq + r, \qquad 0 \leq r < d$$

Now

$$r = a - dq = a - (m'a + n'b)q = (1 - qm')a - qn'b$$

and we have that r is an integral linear combination of a and b. Since $0 \leq r < d$ and d is the minimum positive integral linear combination of a and b, we have $r = 0$, from which $a = dq + r$ implies that $a = dq$. So $d \mid a$. Similarly, $d \mid b$. It remains to show that d is the *greatest* common divisor of a and b. Let c be any common divisor of a and b so that $c \mid a$ and $c \mid b$. Then $c \mid m'a + n'b = d$ by Proposition 1.2, from which $c \leq d$. ■

Example 15:

Express $(803, 154)$ as an integral linear combination of 803 and 154. Essentially, work through the steps of Example 14 backward. We have

$$\begin{aligned}(803, 154) = 11 &= 33 - 22 \quad \text{[by (4)]} \\ &= 33 - (154 - 33 \cdot 4) \quad \text{[by (3)]} \\ &= 33 \cdot 5 - 154 \\ &= (803 - 154 \cdot 5)5 - 154 \quad \text{[by (2)]} \\ &= 803 \cdot 5 - 154 \cdot 26 \\ &= 5 \cdot 803 + (-26)154\end{aligned}$$

- Find the GCD(73,25) and express it as a combination of 73 and 25.

$$\begin{aligned} 73 &= 25 \cdot 2 + 23 \\ 25 &= 23 \cdot 1 + 2 \\ 23 &= 2 \cdot 11 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

We set up a box, using the sequence of quotients 2, 1, 11, and 2, as follows:

		2	1	11	2
0	1	$*$	$*$	$*$	$*$
1	0	$*$	$*$	$*$	$*$

Then the rule to fill in the remaining entries is as follows:

$$\text{New Entry} = (\text{Number at Top}) \cdot (\text{Number to the Left}) + (\text{Number Two Spaces to the Left}).$$

Thus the two leftmost $*$'s are

$$2 \cdot 1 + 0 = 2 \qquad \text{and} \qquad 2 \cdot 0 + 1 = 1,$$

so now our box looks like this:

		2	1	11	2
0	1	2	$*$	$*$	$*$
1	0	1	$*$	$*$	$*$

Then the next two leftmost $*$'s are

$$1 \cdot 2 + 1 = 3 \qquad \text{and} \qquad 1 \cdot 1 + 0 = 1,$$

and then the next two are

$$11 \cdot 3 + 2 = 35 \qquad \text{and} \qquad 11 \cdot 1 + 1 = 12,$$

and the final entries are

$$2 \cdot 35 + 3 = 73 \qquad \text{and} \qquad 2 \cdot 12 + 1 = 25.$$

The completed box is

		2	1	11	2
0	1	2	3	35	73
1	0	1	1	12	25

32. Find the greatest common divisors below.

(a) $(21, 28)$

(b) $(32, 56)$

(c) $(58, 63)$

(d) $(0, 113)$

(e) $(111, 129)$

(f) $(120, 165)$

33. Let $a \in \mathbf{Z}$ with $a > 0$. Find the greatest common divisors below.

(a) (a, a^n) where n is a positive integer

(b) $(a, a + 1)$

(c) $(a, a + 2)$

(d) $(3a + 5, 7a + 12)$

Stein's Algorithm

- Another algorithm for calculating the GCD of two values by Josef Stein in 1967 .
- It is optimised for use in computing, utilising fast bitwise shifts rather than the usually slower repeated subtraction, division or modulus operations.

Algorithm to find GCD using Stein's algorithm gcd(a, b)

1. If both a and b are 0, gcd is zero gcd(0, 0) = 0.
2. gcd(a, 0) = a and gcd(0, b) = b because everything divides 0.
3. If a and b are both even, gcd(a, b) = 2*gcd(a/2, b/2) because 2 is a common divisor. Multiplication with 2 can be done with bitwise shift operator.
4. If a is even and b is odd, gcd(a, b) = gcd(a/2, b). Similarly, if a is odd and b is even, then gcd(a, b) = gcd(a, b/2). It is because 2 is not a common divisor.
5. If both a and b are odd, then gcd(a, b) = gcd(|a-b|/2, b). Note that difference of two odd numbers is even
6. Repeat steps 3–5 until a = b, or until a = 0. In either case, the GCD is power(2, k) * b, where power(2, k) is 2 raise to the power of k and k is the number of common factors of 2 found in step 2.

Lemma 1.14: (Euclid) Let $a, b, p \in \mathbf{Z}$ with p prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: Assume that $p \nmid a$. Then $(a, p) = 1$. We must show that $p \mid b$. By Proposition 1.11, there exist $m, n \in \mathbf{Z}$ such that $ma + np = 1$. Also, $p \mid ab$ implies $ab = pc$ for some $c \in \mathbf{Z}$. Now multiplying both sides of $ma + np = 1$ by b, we have $mab + npb = b$; $ab = pc$ then implies that $mpc + npb = b$ or $p(mc + nb) = b$. So we have $p \mid b$ as desired. ■

Corollary 1.15: Let $a_1, a_2, \ldots, a_n, p \in \mathbf{Z}$ with p prime. If $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i.

Proof: We use induction on n. The statement for $n = 1$ is obvious. The statement for $n = 2$ is Lemma 1.14. Assume that $k \geq 2$ and that the desired statement is true for $n = k$ so that $p \mid a_1 a_2 \cdots a_k$ implies that $p \mid a_i$ for some i (with $1 \leq i \leq k$). We must show that $p \mid a_1 a_2 \cdots a_{k+1}$ implies that $p \mid a_i$ for some i (with $1 \leq i \leq k + 1$) so that the desired statement holds for $n = k + 1$. Now $p \mid a_1 a_2 \cdots a_{k+1}$ implies $p \mid (a_1 a_2 \cdots a_k) a_{k+1}$; Lemma 1.14 then implies $p \mid a_1 a_2 \cdots a_k$ or $p \mid a_{k+1}$. If $p \mid a_{k+1}$, then the desired statement holds for $n = k + 1$. If $p \nmid a_{k+1}$, then $p \mid a_1 a_2 \cdots a_k$, which implies that $p \mid a_i$ for some i (with $1 \leq i \leq k$) by the induction hypothesis, and the desired statement holds for $n = k + 1$, which completes the proof. ■

Definition 11: Let $a, b \in \mathbf{Z}$ with $a, b > 0$. The *least common multiple* of a and b, denoted $[a, b]$, is the least positive integer m such that $a \mid m$ and $b \mid m$.

Proposition 1.17: Let $a, b \in \mathbf{Z}$ with $a, b > 1$. Write $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ where $p_1, p_2, \ldots, p_n$ are distinct prime numbers and $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ are nonnegative integers (possibly zero). Then

$$(a, b) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \cdots p_n^{\min\{a_n, b_n\}}$$

and

$$[a, b] = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \cdots p_n^{\max\{a_n, b_n\}}$$

Lemma 1.18: Let $x, y \in \mathbf{R}$. Then $\max\{x, y\} + \min\{x, y\} = x + y$.

Proof: If $x < y$, then $\max\{x, y\} = y$ and $\min\{x, y\} = x$, and the desired result follows. The cases are similar for $x = y$ and $x > y$. ■

The relationship between the greatest common divisor and the least common multiple of two positive integers is now given by the following theorem.

Theorem 1.19: Let $a, b \in \mathbf{Z}$ with $a, b > 0$. Then $(a, b)[a, b] = ab$.

Proof: If $a, b > 1$, write $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ as in Proposition 1.17. Then

$$\begin{aligned}
(a, b)[a, b] &= \{p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \cdots p_n^{\min\{a_n,b_n\}}\}\{p_1^{\max\{a_1,b_1\}} p_2^{\max\{a_2,b_2\}} \cdots p_n^{\max\{a_n,b_n\}}\} \\
&= p_1^{\min\{a_1,b_1\}+\max\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}+\max\{a_2,b_2\}} \cdots p_n^{\min\{a_n,b_n\}+\max\{a_n,b_n\}} \\
&= p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_n^{a_n+b_n} \quad \text{(by Lemma 1.18)} \\
&= p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} \\
&= ab
\end{aligned}$$

as desired. The cases $a = 1$ and $b > 1$, $a > 1$ and $b = 1$, and $a = b = 1$ are easily checked and are left as exercises. ■

61. Find the greatest common divisor and the least common multiple of each pair of integers below.

(a) $2^2 \cdot 3^3 \cdot 5 \cdot 7,\ 2^2 \cdot 3^2 \cdot 5 \cdot 7^2$

(b) $2^2 \cdot 5^2 \cdot 7^3 \cdot 11^2,\ 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17$

(c) $2^2 \cdot 5^7 \cdot 11^{13},\ 3^2 \cdot 7^5 \cdot 13^{11}$

(d) $3 \cdot 17 \cdot 19^2 \cdot 23,\ 5 \cdot 7^2 \cdot 11 \cdot 19 \cdot 29$

62. Find five integers that are relatively prime (when taken together) but such that no two of the integers are relatively prime when taken separately.

63. Find each of the least common multiples below by using the Euclidean algorithm and Theorem 1.19.

(a) $[221, 323]$

(b) $[257, 419]$

(c) $[313, 1252]$

(d) $[1911, 9702]$

76. *(a)* Let $n \in \mathbf{Z}$ with $n > 1$, and let p be a prime number. If $p \mid n!$, prove that the exponent of p in the prime factorization of $n!$ is $[n/p] + [n/p^2] + [n/p^3] + \cdots$. (Note that this sum is finite, since $[n/p^m] = 0$ if $p^m > n$.)

(b) Use part (a) above to find the prime factorization of 20!.

(c) Find the number of zeros with which the decimal representation of 100! terminates.

Thank You