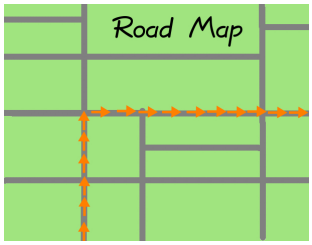
Module 1.6: Set Theory and Number Theory

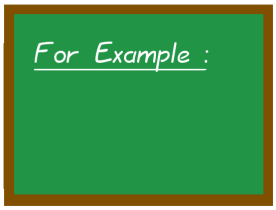


The problems in this module will expose you to topics where set theory overlaps with number theory. That's kind of cool, as it ties together the first topic in this book (set theory) with our last major topic (number theory). To introduce number theory, we're going to learn how to compute the set of multiples of an integer, the set of common multiples of two integers, the set of divisors of an integer, the set of common divisors of two integers, and testing an integer for primality, which are all routine tasks. We'll also learn some uncommon tasks, like detecting twin primes and "perfect" numbers.

We're also going to see something very important—we're going to see how knowing a mathematical theorem can result in a vastly improved computer program.

When the semester starts, I think that a lot of students in Discrete Mathematics classes (including some of the best) imagine that proving a theorem and writing a better computer program are two spectacularly unrelated tasks, with a lot of room in between them for several other categories of knowledge or activity. I wish to dispel this notion completely with a concrete example. That example will unfold slowly over the course of Page 193 to Page 199, the very heart of this module.

My goal is to show you a situation where knowing a theorem in mathematics can result in a vastly improved computer program. The course is just starting, so the example has to be easy, but rest assured that you will see other connections between Discrete Mathematics and computing as the course continues. Indeed, it is because of these connections that computing degrees at universities require a Discrete Mathematics course.



1-6-1

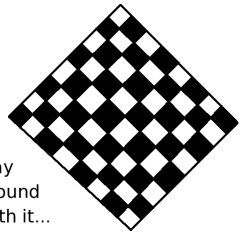
Having now established the relevance of number theory in discrete mathematics, we will begin by discussing sets of multiples and sets of divisors. When we say the *set of multiples* of 3 we mean the set

$$\text{multiples}(3) = \{3, 6, 9, 12, 15, \ldots\}$$

which, unless otherwise stated, is always in terms of the positive integers.

As you can see, this is an infinite set. We cannot possibly list all the members of this set. Instead, it is customary to give five examples of the pattern of an infinite set, and then put some dots. It is best if you write the first five examples, but for some infinite sets like $\{r \in \mathbb{R} \,|\, r > 5\}$ that would be impossible.

Just to be precise, when we say multiples(n) for any positive integer n, you take the set of integers $\{1, 2, 3, 4, 5, \ldots\}$ and multiply each of them by n, getting $\{n, 2n, 3n, 4n, 5n, \ldots\}$

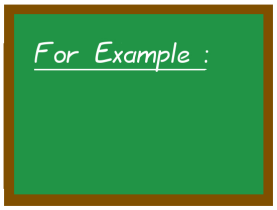


1-6-2

In similar notation to the previous box, write the roster of the following sets:

1. multiples(5)
2. multiples(2)

The solutions are found on Page 213.



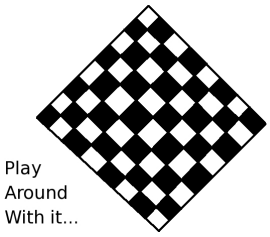
1-6-3

When we say the *common multiples* of 4 and 6 we mean the set

$$\text{multiples}(4) \cap \text{multiples}(6) = \{4, 8, 12, 16, 20, \ldots\} \cap \{6, 12, 18, 24, 30, \ldots\} = \{12, 24, 36, 48, 60, \ldots\}$$

This does require some degree of care and thought, because you are intersecting infinite sets. For example, 36, 48, and 60 were not among the first five elements of multiples(4) nor multiples(6).

Formally, the set of common multiples of x and y is the intersection of the multiples of x and the multiples of y.



1-6-4

With the definition of the previous box in mind...

- Write the first five common multiples of 2 and 5. (Hint, refer to the answers of the previous checkerboard box.)
- Write the first five common multiples of 6 and 8.
- Write the first five common multiples of 3 and 12.

The answers are to be found on Page 213.

Now that you've completed the previous question, you've probably noticed that every answer was the set of multiples of some number. Specifically...

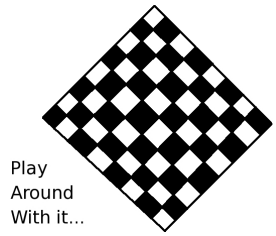
- $\text{multiples}(4) \cap \text{multiples}(6) = \{12, 24, 36, 48, 60, \ldots\} = \text{multiples}(12)$.
- $\text{multiples}(2) \cap \text{multiples}(5) = \{10, 20, 30, 40, 50, \ldots\} = \text{multiples}(10)$.
- $\text{multiples}(6) \cap \text{multiples}(8) = \{24, 48, 72, 96, 120, \ldots\} = \text{multiples}(24)$.
- $\text{multiples}(3) \cap \text{multiples}(12) = \{12, 24, 36, 48, 60, \ldots\} = \text{multiples}(12)$.

With that in mind, we can save ourselves a lot of writing! That is, of course, a very good thing.

We should instead define the *least common multiple* of x and y, abbreviated $\text{lcm}(x, y)$. Then we can write

- $\text{lcm}(4, 6) = 12$
- $\text{lcm}(2, 5) = 10$
- $\text{lcm}(6, 8) = 24$
- $\text{lcm}(3, 12) = 12$

It's worth mentioning that there are *much faster* ways of computing the *lcm* than writing out the sets of the multiples. Before this module is over, you will know what they are.

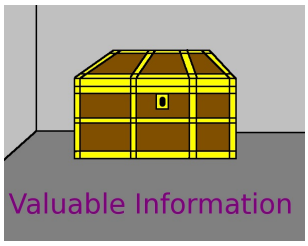


1-6-5

Let's say you're helping a younger relative with adding fractions. The first step is to find the lowest common denominator.

- When adding $1/4 + 1/6$, what is the lowest common denominator?
- When adding $1/2 + 1/5$, what is the lowest common denominator?
- When subtracting $1/6 - 1/8$, what is the lowest common denominator?
- When adding $1/3 + 1/12$, what is the lowest common denominator?

The answers are waiting for you on Page 214.

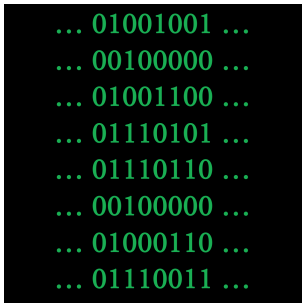


Unless you're asleep, you've surely noticed that the "lowest common denominator" when adding (or subtracting) fractions is actually the same thing as the "least common multiples" of the two given denominators.

However, in university-level mathematics, we always say "least common multiple" and not "lowest common denominator." That's because "least common multiple" reflects the existence of applications other than doing arithmetic with fractions.

Hopefully, at this point in your mathematical career, you've had the opportunity to solve a complicated math problem using a computer algebra package. While computer algebra packages tend to have almost all the same capabilities (a natural consequence of the fact that they are competing products) the "kingdom" of computer algebra packages is divided into two "phyla."

- One phylum is the real-number based, floating-point style, as taught in classes like *Numerical Analysis* or *Numerical Computing*. Those algorithms are fast, but subject to rounding error. MATLAB is the most famous member of this phylum.
- The other phylum is exact, integer-based, and slow, but totally immune to all rounding error. Those use exact rational arithmetic. Maple and Sage are the most famous members of this phylum.



In other words, instead of storing $1/3$ as $0.3333333\cdots$, or more precisely $0.0101010101\cdots$ in binary, it is stored as 1 and 3, or more precisely 00000001 and 00000011 in binary. Everything is represented as a fraction, if possible. As a computer program does lots of additions and subtracts of fractions, it must compute a lot of lowest common denominators (or we should say, least common multiples).

Moreover, in order to work efficiently, you have to use certain tricks. Doing a long sequence of fraction additions and subtractions will often result in a huge numerator and denominator. Exact rational arithmetic was thought of soon after the invention of the computer in the 1940s. However, only in the last thirty years has it become feasible. That's partly due to theoretical innovations, and partly because computers are a lot faster these days.

To give you an example of this, I asked Sage to generate a 10×16 random matrix filled with integers. The matrix it gave me was

$$\begin{pmatrix} 1 & 1 & -1 & 1 & 1 & -2 & -1 & 2 & 0 & 7 & -1 & -1 & 15 & 1 & 4 & 0 \\ 0 & -2 & -1 & 1 & 1 & 2 & 15 & 1 & -1 & -1 & 0 & 0 & -4 & -3 & -2 & -13 \\ 0 & 1 & 0 & 1 & -1 & 1 & 3 & -1 & 89 & 0 & 0 & 15 & -1 & -4 & 6 & 2 \\ -1 & 0 & 0 & 2 & 1 & 0 & 2 & -1 & 1 & 1 & -10 & 2 & 1 & -2 & 0 & 1 \\ 0 & -1 & 0 & -1 & 0 & 1 & 0 & -1 & 3 & -10 & 3 & 1 & 1 & -1 & 1 & -50 \\ 4 & 0 & 1 & -1 & -2 & 1 & 0 & 3 & 2 & 1 & -1 & 2 & 1 & 29 & 0 & 1 \\ 8627 & -1 & -1 & 0 & 5 & 6 & 2 & 0 & -3 & 1 & 1 & 1 & 0 & -1 & 0 & 0 \\ 221 & 8 & 4 & 0 & 0 & -3 & -18 & 2 & 1 & 1 & 0 & 1 & -1 & -4 & 26 & 3 \\ -6 & 1 & 5 & -1 & 0 & 5 & -1 & 3 & 2 & 0 & -1 & 1 & 1 & 22 & 1 & 2 \\ -2 & -3 & 1 & -1 & 1 & 1 & 1 & -2 & 0 & 0 & 5 & -1 & -4 & -1 & 1 & 1 \end{pmatrix}$$

Then I asked Sage for the RREF (reduced row echelon form). For those of you who have not had any coursework in matrices, rest assured that this is an extremely common thing for matrices. For example, you can use the RREF to compute solutions to systems of linear equations. The answer was

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{32691460}{32871315031} & \frac{41446686}{32871315031} & -\frac{4868771}{1060365001} & \frac{164658100}{32871315031} & \frac{121255432}{32871315031} & \frac{164296117}{65742630062} \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{63330681970}{32871315031} & -\frac{24842909760}{32871315031} & -\frac{3270525830}{1060365001} & -\frac{268941445110}{32871315031} & -\frac{4582040632}{32871315031} & \frac{273844909504}{32871315031} \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{29651252576}{32871315031} & \frac{31743752809}{32871315031} & -\frac{4745228921}{1060365001} & \frac{162500148193}{32871315031} & \frac{178300851651}{32871315031} & \frac{41404982079}{65742630062} \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{247671646032}{32871315031} & \frac{60292245291}{32871315031} & \frac{3205596200}{1060365001} & \frac{240276323286}{32871315031} & -\frac{28219389343}{32871315031} & -\frac{331721792881}{65742630062} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \frac{84953770533}{32871315031} & -\frac{37753045062}{32871315031} & \frac{5059456131}{1060365001} & -\frac{222625094673}{32871315031} & \frac{56423799871}{32871315031} & -\frac{697517490621}{65742630062} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -\frac{20700094778}{32871315031} & -\frac{17149125265}{32871315031} & \frac{2354138745}{1060365001} & -\frac{56712809991}{32871315031} & -\frac{195453742444}{32871315031} & \frac{160432683375}{32871315031} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \frac{22515991540}{32871315031} & -\frac{1366493246}{32871315031} & -\frac{2289189571}{1060365001} & -\frac{41278107036}{32871315031} & \frac{27425496996}{32871315031} & \frac{123323940109}{65742630062} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -\frac{24746588697}{32871315031} & \frac{11249997442}{32871315031} & \frac{5618177610}{1060365001} & \frac{220487073684}{32871315031} & \frac{37774045709}{32871315031} & -\frac{794671044061}{65742630062} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \frac{2221351304}{32871315031} & \frac{5082763453}{32871315031} & \frac{159501442}{1060365001} & \frac{849314290}{32871315031} & \frac{4914656373}{32871315031} & -\frac{12738811729}{32871315031} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \frac{9643756680}{32871315031} & -\frac{8147148291}{32871315031} & -\frac{378096991}{1060365001} & -\frac{21311550395}{32871315031} & -\frac{21855370409}{32871315031} & \frac{411026701741}{65742630062} \end{pmatrix}$$

As you can see, the answers—even for this tiny problem—had several ten-digit or larger numerators and denominators. Imagine how huge the numerators and denominators would be if I had a $10,000 \times 10,000$ matrix, which can occur easily in all sorts of engineering applications involving "the finite element method," a technique which has achieved great popularity for solving advanced civil and mechanical engineering problems.

If you'd like to see your own example of the above, then the Sage code for you to use is provided below. Of course, you will get a different random matrix than I will. However, the effect should be the same. Also, observe that the symbol which Sage uses for the integers is just $\mathbb{Z}$, formed by two consecutive capital Zs.

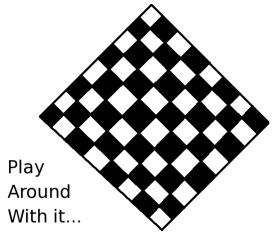
You might want to try changing the `10, 20` into `16, 32`, and see what happens. When I tried that, one of the entries of the final matrix was

$$\frac{12157504981221440351542 1949}{11467676316698020356831370}$$

```
A = random_matrix( ZZ, 10, 20 )
show(A)
show(A.rref())
```

By the way, since the previous box referred to random matrices, I thought I would mention that some theorems related to random matrices, including where they come up in Quantum Mechanics, are dependent on the truth or falsehood of the Riemann Hypothesis. (We talked about the Riemann Hypothesis on Page 242 of the module "Fermat's Last Theorem and Some Famous Unsolved Problems.")

Random matrices have many uses, from describing the growth of rounding error in computer algebra systems, to cryptanalysis.

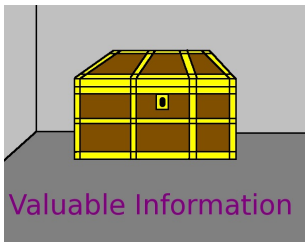


1-6-6

Since we saw that the intersections (of the sets of multiples of two positive integers) had structure and meaning, you might be curious as to what happens when we take a union of the sets of multiples of two positive integers. Referring to your work on the last several questions, write down the rosters of the following sets. Please write the first ten members of these sets, instead of the usual first five members.

1. What is multiples(4) $\cup$ multiples(6)?
2. What is multiples(6) $\cup$ multiples(8)?
3. What is multiples(2) $\cup$ multiples(5)?

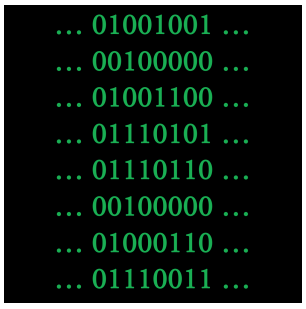
The answers will be given on Page 214.



For a particular number, it can be interesting to consider the *set of divisors* of that number. For example, suppose that I have ten eggs. I can divide them into 2 groups of 5 eggs, 5 groups of 2 eggs, 10 groups of 1 egg, and 1 group of 10 eggs. Therefore, we write divisors(10) = $\{1, 2, 5, 10\}$.

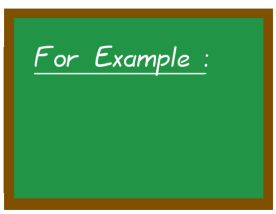
In general, the set of divisors of n is the set of all positive integers z with n/z equaling an integer.

Of course, all computer algebra programs (Maple, Mathematica, MATLAB, Magma, and Sage) have a command for computing the divisors of a given number.



Let's suppose that your team has been asked to program some mathematical software. For example, it could be part of an educational game, a calculator app on a cell phone, or some scientific application of Diophantine equations.

Your task is to figure out how to write a function to compute the set of divisors of a number. We will first do this "the obvious way," which works but which is very inefficient. Then we shall see a way to use a mathematical theorem to make our program vastly more efficient.

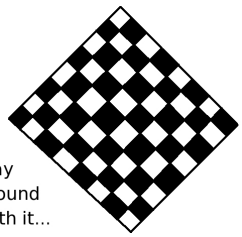


1-6-7

In order to figure out how to write a function to compute the set of divisors of a number, we should first explore how to do it by hand. One way is to count upward, and simply rule in, or rule out, each integer. For example, if I ask for the divisors of 12, then you could perform the following mental process:

Does 1 divide 12? Yes. Does 2 divide 12? Yes. Does 3 divide 12? Yes.
Does 4 divide 12? Yes. Does 5 divide 12? No. Does 6 divide 12? Yes.
Does 7 divide 12? No. Does 8 divide 12? No. Does 9 divide 12? No.
Does 10 divide 12? No. Does 11 divide 12? No. Does 12 divide 12? Yes.

Therefore, we write divisors(12) = $\{1, 2, 3, 4, 6, 12\}$.



1-6-8

Using the above method, compute for me now the divisors of 15.

The answer will be given on Page 214.

The Sage code for our straightforward, but slow, approach is given below this box. It produces the output `[1, 3, 5, 15]` as expected.

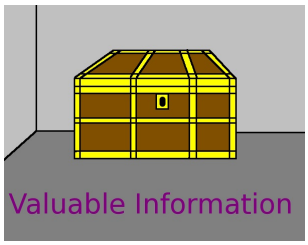
```
request = 15

# we start with the empty set
answer_set = [ ]

for x in range(1, request+1):
    # we will consider all values of x such that 1 <= x < request+1
    # due to a quirk in Python, it will include 1 but exclude request+1

    # the floor() function just means "round down"
    if ((request/x) == floor(request/x)):
        # this means that request/x is an integer
        # therefore, x is a divisor of request

        # this will insert x into answer_set
        answer_set.append(x)

print answer_set
```

What if I ask for the divisors of 60? Do you really have to count up to 60?! I suppose you could do it that way, if you have lots of free time, but that wouldn't be very much fun.

The answer is no—there is a faster way! We will use a mathematical theorem to guide us in writing a more efficient computer program. However, to see why we should care, consider the following.

When we were asked to find the divisors of 12 and 15, we needed 12 and 15 trial divisions, respectively. Actually, you don't really need the first division and the last division, because you already know what will happen if you divide a number by itself, or if you divide a number by one. While you'd only need 10 and 13 trial divisions for computing 12 and 15, what if you had to compute the divisors of a seven-digit number? How about a number with ten digits? In cryptography, we frequently use numbers that are 300-digits long.

You would experience inconvenient delays computing the set of divisors of even a 12-digit number using this straightforward method, let alone larger. We need a smarter method.

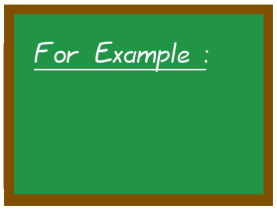


Here is the theorem that we're going to use to improve our program.

For any positive real numbers a, b, and c, if $ab = c$ then either $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$.

What this means is that when we search for the divisors of n, we can stop at $\sqrt{n}$. For example, if n is slightly less than one trillion, clearly $\sqrt{n}$ will be slightly less than one million. This means that we will check from 1 to 10^6 instead of 10^{12}. That means that our program will become literally *one million times faster*.

In summary, you first count upward until you exceed the square root of the original number. Then you find the "mirror images" of the discovered divisors. (The term "mirror image" is mathematical slang, and I'll explain it in a moment. The technical term is cofactor.)



1-6-9

Recall, we have been asked to find the set of divisors of 60.

We know that $64 > 60 > 49$ so that means $\sqrt{64} > \sqrt{60} > \sqrt{49}$ or more plainly, $8 > \sqrt{60} > 7$. I do not need to consider eight nor any higher number, though I must consider 7. Now I ask myself the following:

Does 1 divide 60? Yes. Does 2 divide 60? Yes. Does 3 divide 60? Yes.
Does 4 divide 60? Yes. Does 5 divide 60? Yes. Does 6 divide 60? Yes.
Does 7 divide 60? No.

At this point, I am halfway there. I have written down now

$$\text{divisors}(60) = \{1, 2, 3, 4, 5, 6,$$

and I shall compute the "mirror images" as follows: $60 \div 6 = 10$, $60 \div 5 = 12$, $60 \div 4 = 15$, $60 \div 3 = 20$, $60 \div 2 = 30$, and $60 \div 1 = 60$. I can complete the divisor set with these new numbers, giving me the complete set of the divisors.

$$\text{divisors}(60) = \left\{ 1, 2, 3, 4, 5, 6, \underbrace{10, 12, 15, 20, 30, 60}_{\text{mirror images}} \right\}$$

Looking at what we did in the previous box, you can see that it was much easier than doing 60 trial divisions.

To be specific, I had 7 trial divisions, where I found the factors $\{1, 2, 3, 4, 5, 6\}$. Then I had 6 more divisions to find the cofactors, which I called "mirror images." We only needed 13 divisions, not 60 divisions.

For Example :

1-6-10

Just to make sure that the trick is clear, let me show it to you again, but for 42 this time. Since $6 = \sqrt{36}$ and $7 = \sqrt{49}$, then $7 > \sqrt{42} > 6$, so I must include 6, but there is no need to include 7.

Does 1 divide 42? Yes. Does 2 divide 42? Yes. Does 3 divide 42? Yes.
Does 4 divide 42? No. Does 5 divide 42? No. Does 6 divide 42? Yes.

At this point, I am halfway there. I have written down now

$$\text{divisors}(42) = \{1, 2, 3, 6,$$

I shall compute the "mirror images" as follows: $42 \div 6 = 7$, $42 \div 3 = 14$, $42 \div 2 = 21$, and $42 \div 1 = 42$. I can complete the divisors set with these new numbers, giving me the complete set of the divisors:

$$\text{divisors}(42) = \left\{ 1, 2, 3, 6, \underbrace{7, 14, 21, 42}_{\text{mirror images}} \right\}$$

As you can see, I had six trial divisions, and I found the factors $\{1, 2, 3, 6\}$. Then there were four additional divisions to find the mirror images, called cofactors. There were 10 divisions instead of 42.

For Example :

1-6-11

At the risk of beating a dead horse, let's do it again for 169. If you think you've understood the algorithm, then you can just skip this example and continue on to the next box.

Because $\sqrt{169} = 13$, then I must include 13, but there is no need to include 14.

Does 1 divide 169? Yes. Does 2 divide 169? No. Does 3 divide 169? No.
Does 4 divide 169? No. Does 5 divide 169? No. Does 6 divide 169? No.
Does 7 divide 169? No. Does 8 divide 169? No. Does 9 divide 169? No.
Does 10 divide 169? No. Does 11 divide 169? No. Does 12 divide 169? No.
Does 13 divide 169? Yes.

At this point, I am halfway there. I have written down now

$$\text{divisors}(42) = \{1, 13,$$

We could compute the "mirror images" as follows: $169 \div 13 = 13$, and $169 \div 1 = 169$. However, the second one is obvious and the first one is just restating that $\sqrt{169} = 13$. Now the complete set of divisors is

$$\text{divisors}(169) = \{1, 13, 169\}$$

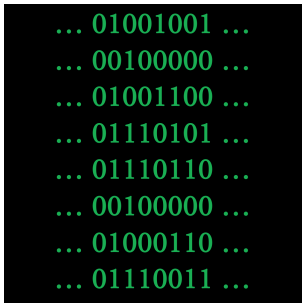
Note: we never list a member of a set more than once. If we did, then several formulas about the sizes of sets would stop working. Therefore, we don't write $\{1, 13, 13, 169\}$, but instead write 13 only once.

As you can see, I had 13 trial divisions, and I found the factors $\{1, 13\}$. Then there were two additional divisions to find the mirror images, called cofactors. There were 15 divisions instead of 169.

In reality, there's no need to perform a trial division to see if 1 goes into a number—of course it does! Also, we don't really need to perform the division by 1, because we know what the answer will be. We made a similar argument on Page 194. The fair comparison therefore is

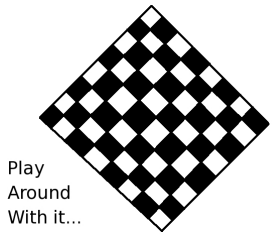
- For 60, we need 11 divisions instead of 58 divisions.
- For 42, we need 8 divisions instead of 40 divisions.
- For 169, we need 13 divisions instead of 167 divisions.

We will discuss this data in the next box.



Looking again at the data from the previous box, you can see that I have fulfilled my promise of showing a situation where knowing a mathematical theorem can help you write a vastly more efficient computer program. Of course, in this situation, the theorem was completely obvious, but later on there will be other (more complicated) examples.

Of course, if the number was approximately 10^{18}, then you'd perform only $\sqrt{10^{18}} = 10^9$ trial divisions. That means that your program would be 10^9 times faster than the original program, which would perform 10^{18} trial divisions. Knowing this theorem has made your program *one billion times faster*.



1-6-12

Let's practice this method by hand now, to make sure that you've understood it.

- Compute the set of divisors of 72. As a hint, we know that $9 = \sqrt{81}$ and $8 = \sqrt{64}$, thus $\sqrt{81} > \sqrt{72} > \sqrt{64}$ or more simply $9 > \sqrt{72} > 8$. Therefore, you must test 8 but there is no need to test 9.
- Compute the set of divisors of 36.
- Compute the set of divisors of 40.
- Compute the set of divisors of 90.

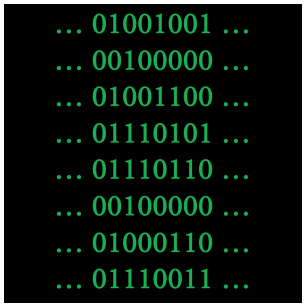
The answers will be on Page 214.

The code for the newer version will be given at the top of the next page. I ran the newer version and the older version on `cocalc.com`, a collaborative service that has a great interface for Sage.

For the number 12,345,678, I found out that our original program took 32.2 seconds on CoCalc.com, whereas our revised program took only 0.00931 seconds. Another way to say that is our original program requires 32,200 milliseconds, whereas our revised program requires 9.31 milliseconds. In summary, for this particular input, our program became $3458.64\cdots$ times faster because of this theorem.

For the number 123,456,789 the slower program actually timed out, but we can estimate that its running time would have been 322 seconds, whereas the faster program took 29.5 milliseconds. This means that we could estimate our program became $10,915.2\cdots$ times faster, for this particular input, because of this theorem.

```
request = 15

# the floor() function just means "round down"
stop = floor( sqrt( request ) )

# we start with the empty set
answer_set = [ ]

for x in range(1, stop+1):
    # we will consider all values of x such that 1 <= x < stop+1
    # due to a quirk in Python, it will include 1 but exclude stop+1

    if ((request/x) == floor(request/x)):
        # this means that request/x is an integer
        # therefore, x is a divisor of request

        # this will insert x into answer_set
        answer_set.append(x)

        if (x != (request/x) ):
            # request/x is also a divisor of request
            # so we should insert it into answer_set
            # but only when x =/= request/x
            # because we don't want two copies of the same number
            answer_set.append(request/x)

# if we leave the next line out, the numbers will be out of order
answer_set.sort()

print answer_set
```



Looking at the timings just given in the previous box, let's be honest now. If a user types a command, and the computer takes 32.2 seconds to give an answer, your program has a serious problem. Most users will assume that the program has locked up or crashed. A user will probably quit, restart, and try again. If they don't get a fast response after 2–5 tries, depending on their patience, then they will never use your program again, and they'll be looking at your competitor's products.

Response time is clearly an important matter!

It was a little bit unfair for me to state this theorem without giving you a proof of the theorem. In the next box, I'm going to prove our useful fact: for any positive real numbers a, b, and c, if $ab = c$ then either $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$. When I teach the semester long course in cryptography at UW Stout, MSCS-380/580: *Cryptography*, this is one of the first theorems that we prove.

There are many techniques available to help a mathematician write proofs. We're going to use what was called a *reductio ad absurdum* until the mid-twentieth century, and which is now called a *proof by contradiction*. We will temporarily assume the opposite of our claim, and show that this leads to some sort of absurdity or impossibility. This means that it is not possible for our claim to be false, and therefore our claim is true. By the way, sometimes the claim is called "the goal."

Claim: For any positive real numbers a, b, and c, if $ab = c$ then either $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$.

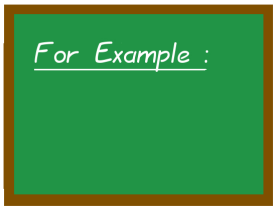
Proof: Suppose that a, b, and c are positive real numbers and that $ab = c$. Now we shall assume that both $a > \sqrt{c}$ and $b > \sqrt{c}$.

For any positive real numbers w, x, y, and z, if $w > x$ and $y > z$ then $wy > xz$. (It is easy to see that this statement will become false if we allow negative real numbers or zero.) Substitute $w = a$, $y = b$, $x = \sqrt{c}$, and $z = \sqrt{c}$.

Making those four substitutions, we obtain the following: if $a > \sqrt{c}$ and $b > \sqrt{c}$ then $ab > \sqrt{c}\sqrt{c}$.

Because, $\sqrt{c}\sqrt{c} = c$, so we can simplify: if $a > \sqrt{c}$ and $b > \sqrt{c}$ then $ab > c$. Yet, we said that $ab = c$. This is a contradiction! It is impossible for $ab > c$ and $ab = c$ to be true simultaneously.

(Because we have achieved a contradiction) our initial assumption must be false. It is not the case that both $a > \sqrt{c}$ and $b > \sqrt{c}$. Therefore, for any positive real numbers a, b and c, if $ab = c$ then either $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$. ■

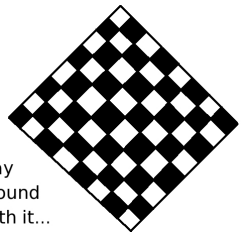


Thank you for sticking with me through that extensive discussion about computing the set of divisors of some positive integer. I'm sure that you must be tired by now, but the good news is that we only have one more major concept to define: *common divisors*. Suppose that someone asks you for the set of common divisors of 15 and 40. What do you do?

The "set of common divisors of 15 and 40" means

$$\text{divisors}(15) \cap \text{divisors}(40) = \{1, 3, 5, 15\} \cap \{1, 2, 4, 5, 8, 10, 20, 40\} = \{1, 5\}$$

1-6-13

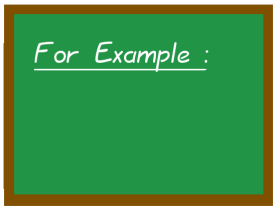


At this point, you have the sets of divisors for 10, 12, 15, 40, 36, 60, and 72, computed in the previous examples and checkerboard boxes. Do not recompute those, but using your previous work, compute the following sets:

- What is the set of common divisors of 36 and 40?
- What is the set of common divisors of 36 and 60?
- What is the set of common divisors of 72 and 60?
- What is the set of common divisors of 40 and 60?
- What is the set of common divisors of 36 and 42?
- What is the set of common divisors of 40 and 42?
- What is the set of common divisors of 42 and 72?

The answers are to be found on Page 215.

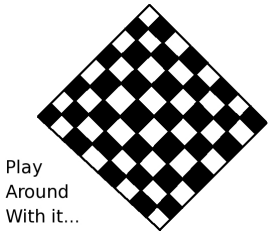
1-6-14



On Page 190, we saw that we could write the set of common multiples of x and y as the set of multiples of some other number. You might be wondering if it is possible to rewrite the set of common divisors of x and y as the set of divisors of some other number. The answer is yes! In the next box, you will rewrite your answers to the previous box, each being the set of divisors of some number. I'll do the first two for you.

- What is the set of common divisors of 36 and 40? $\{1, 2, 4\} = \text{divisors}(4)$.
- What is the set of common divisors of 36 and 60? $\{1, 2, 3, 4, 6, 12\} = \text{divisors}(12)$.

1-6-15



1-6-16

Remember, do not compute the answers to these questions from scratch! You did 95% of the work for this problem during the previous two checkerboards.

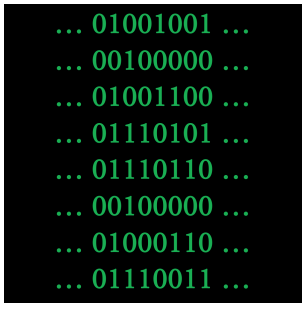
- What is the set of common divisors of 36 and 40? [Answer: $\{1, 2, 4\}$ = divisors(4).]
- What is the set of common divisors of 36 and 60? [Answer: $\{1, 2, 3, 4, 6, 12\}$ = divisors(12).]
- What is the set of common divisors of 72 and 60?
- What is the set of common divisors of 40 and 60?
- What is the set of common divisors of 36 and 42?
- What is the set of common divisors of 40 and 42?
- What is the set of common divisors of 42 and 72?

The answers can be found on Page 215.

Just as we saw for the *least common multiple*, we can save ourselves a lot of writing here. Efficiency in both mathematics and computer science is born of laziness, which is funny to me. It is funny because laziness is viewed as a *negative* attribute in high school, but laziness becomes a *positive* attribute in later life, after it is renamed "efficiency."

If we want to represent the set of common divisors, we can simply report the *greatest common divisor*, which is abbreviated *gcd*. For example, we would say that the $\gcd(36, 40) = 4$, while the $\gcd(36, 42) = 6$.

As with the lcm, there are much, much faster ways of computing the gcd than listing out the divisor set of each number. We will see one faster method on Page 208. Another such technique (that we will not be able to explore at this time) is the Extended Euclidean Algorithm (EEA)—it is very central in cryptography. You'll probably learn about the EEA later, before Discrete Mathematics has ended.



You might be wondering what the gcd is used for. It looks kind of useless, perhaps? As it turns out, the opposite is true. First, the gcd is the "mother of all operations" in exact rational arithmetic. It is crucial, because that's how you can algorithmically reduce fractions to lowest terms in one step.

For example, suppose that after some rational arithmetic, we get 72/120. An inefficient way to approach this might look like the following:

$$\frac{72}{120} = \frac{36}{60} = \frac{18}{30} = \frac{9}{15} = \frac{3}{5}$$

because you just expended eight divisions.

Instead, we can compute $\gcd(72, 120) = 24$, as well as $72 \div 24 = 3$ and $120 \div 24 = 5$. That way, we know 72/120 is really 3/5. We only needed two divisions after the gcd.

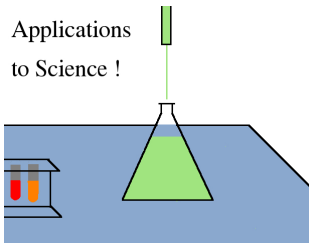
When coding up exact rational arithmetic, you need to reduce to lowest terms really, really often. Sometimes it is done after each and every addition, subtraction, multiplication, or division. If you don't do it so very often, then the numerators and the denominators will quickly balloon into huge numbers. Even with the frequent gcds, the numerators and denominators can still grow huge, as we saw on Page 192. Without frequent gcds it would be even worse.

There is a danger here of mistaking some phrases that sound very similar. Mathematically, we use the gcd and the lcm a lot—the greatest common divisor and the least common multiple. Also, "lowest common denominator" is the high-school term for "least common multiple."

For this reason, sometimes people say "least common divisor." That doesn't mean what you think it means. Consider

$$\text{divisors}(15) = \{1, 3, 5, 15\} \qquad \text{and} \qquad \text{divisors}(21) = \{1, 3, 7, 21\}$$

Clearly the common divisors are $\{1, 3\}$, so the least common divisor is 1. The least common divisor of any two positive integers is always 1.

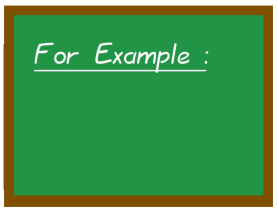


There is a technique for balancing complicated chemical equations with matrices. It comes out of the pure math used to solve multivariate linear systems of Diophantine equations—though the chemists might be surprised to hear this. It uses the gcd, a concept that you have now learned, and that is why I'm mentioning it now. Of course, you can only have an integer number of atoms, and that's the connection to Diophantine equations.

I wrote up this application to chemistry as a project for students, in Section 2.4 of my book *Sage for Undergraduates*, published by the American Mathematical Society in 2015. That section is only six pages, so if you've had a course that deals with matrices, then you can read it. By the way, that book is free in electronic form.

`http://www.gregorybard.com/books.html`

If you haven't had a course that deals with matrices, then don't worry about it. It is just one of many applications, and you will surely learn about matrices in some later course.

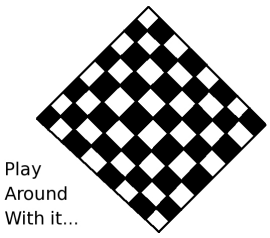


1-6-17

When I asked you to compute the "set of common divisors" for some pairs of integers, on Page 200 of this module, you found seven gcds for me, before you knew what the acronym gcd meant. While the following calculation looks pointless, it is really cool, trust me.

(This used to be a checkerboard problem, but I'm guessing that you must be rather tired now—so I'll do the work of the calculations for you.)

- What is $\frac{(36)(40)}{\gcd(36,40)} = \frac{(36)(40)}{4}$? [Answer: 360.]
- What is $\frac{(36)(60)}{\gcd(36,60)} = \frac{(36)(60)}{12}$? [Answer: 180.]
- What is $\frac{(72)(60)}{\gcd(72,60)} = \frac{(72)(60)}{12}$? [Answer: 360.]
- What is $\frac{(40)(60)}{\gcd(40,60)} = \frac{(40)(60)}{20}$? [Answer: 120.]
- What is $\frac{(36)(42)}{\gcd(36,42)} = \frac{(36)(42)}{6}$? [Answer: 252.]
- What is $\frac{(40)(42)}{\gcd(40,42)} = \frac{(40)(42)}{2}$? [Answer: 840.]
- What is $\frac{(42)(72)}{\gcd(42,72)} = \frac{(42)(72)}{6}$? [Answer: 504.]



1-6-18

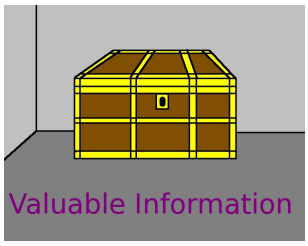
Now that I've done the calculations of the previous box for you, look at those answers. What is going on here? What is the pattern? What have we now discovered? In other words, can you complete the following equation, in general?

$$\frac{(x)(y)}{\gcd(x,y)} = ??$$

Take a moment to really think. Make a hypothesis and check it, perhaps with an example that I did not provide. If you are really flummoxed, then maybe you should look back at Page 190. The answers will be given on Page 216.

At first glance, it will look like the rest of this module is a review of 6th-grade arithmetic, but that is only an illusion. I'm going to show you some rapid computation techniques that number theorists use when working through examples. Indeed, you might have seen a few of these techniques before, but you almost surely have not seen *all* of these techniques before. (For example, an extremely rapid way of computing $\text{lcm}(144, 88) = 1584$.)

Indeed, some of you probably have never seen any of these techniques before. That's fine. Regardless of your circumstances, please take the rest of the module seriously.

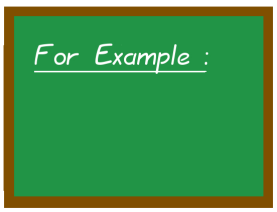


We will now look at ways to determine if a number is prime. One easy way to test if a number is prime or not is to compute its set of divisors. An integer $n > 1$ is prime if and only if $\text{divisors}(n) = \{1, n\}$.

An even easier way to test if an integer n is prime is to just check divisibility by all the primes less than $\sqrt{n}$. For example, $\sqrt{67}$ is just above 8, since $8^2 = 64$. That means I only have to check $\{2, 3, 5, 7\}$.

Furthermore, you can check divisibility by 2, 3, and 5 very easily.

- A number is divisible by 5 if and only if its last digit, when written in decimal, is 0 or 5.
- A number is divisible by 2 if and only if its last digit, when written in decimal, is even.
- A number is divisible by 3 if and only if the sum of its digits is divisible by 3.

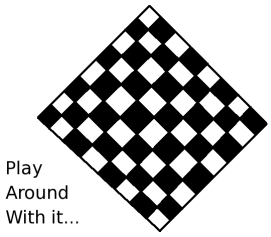


1-6-19

What if someone asks you if 167 is prime?

Even for a number like 167, primality is easy to check.

- The number 167 clearly is not divisible by 2, because 7 is not divisible by 2.
- We add $1 + 6 + 7 = 14$, and since 14 is not divisible by 3, 167 is not divisible by 3 either.
- The number 167 clearly is not divisible by 5, because the last digit is 7.
- Next, we check $167/7 = 23.8571\ldots$, so 167 is not divisible by 7.
- We also check $167/11 = 15.1818\ldots$, so 167 is not divisible by 11.
- There is no need to check 13, because $13^2 = 169 > 167$, so $\sqrt{167} < 13$. (This is because of the theorem that says "for any positive integers a, b, and c, if $ab = c$ then $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$.")

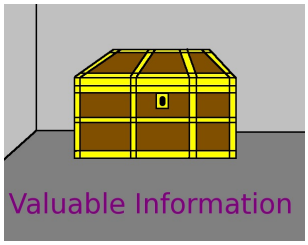


1-6-20

Using the technique of the previous box, tell me if the following integers are prime or composite.

- Is 105 prime?
- Is 101 prime?
- Is 61 prime?
- Is 69 prime?

The answers will be given on Page 216.

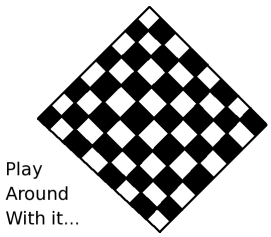


A *twin prime* is a prime p such that $p-2$ or $p+2$ is prime. We will talk more about twin primes on Page 253 of the module "Fermat's Last Theorem and Some Famous Unsolved Problems."

For example, numbers like 17 & 19, 29 & 31, as well as 41 & 43 are twin primes.

Let me mention two counterexamples. We would not say that 37 is a twin prime, because $35 = 5(7)$ is composite, and $39 = 3(13)$ is composite; similarly, we would not say that 47 is a twin prime, because $45 = (5)(9)$ is composite and $49 = 7(7)$ is composite.

By the way, the only time you will ever see all three of $p-2$, p, and $p+2$ being prime is $\{3, 5, 7\}$. This theorem is not too hard to prove, but we will not prove it at this time.

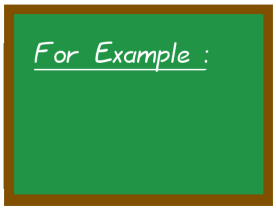


1-6-21

Are the following numbers twin primes? Hint: you did some of the work for this question while doing the question of the previous checkerboard box.

- Is 7 a twin prime?
- Is 15 a twin prime?
- Is 61 a twin prime?
- Is 67 a twin prime?
- Is 103 a twin prime?

The answers will be given on Page 216.



1-6-22

Keeping in mind those rapid mental tests for divisibility by 2, 3, and 5, we can do some phenomenally fast mental factoring of small numbers. The way that this is done is that you look at the number, and if you see any opportunities to "pull out" a 2, 3, or 5, then you do so immediately, followed by looking for new opportunities. Let's say you've been asked to factor 60.

- It ends in a "0" so it is divisible by 5, so we have $60 = 5(12)$.
- The 12 ends in a "2" so it is divisible by 2, which means we have $60 = 5(2)(6)$.
- Of course, we know that $6 = (3)(2)$, thus we have $60 = 5(2)(3)(2)$.

Once you have the number decomposed into a product of primes, it is customary to write the primes in increasing order. We get $60 = 2^2(3)5$.

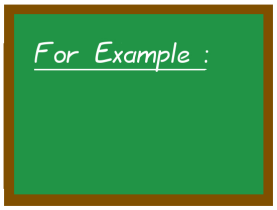
Of course, you should check the work of the previous box by multiplying it back out. Then you obtain:

$$2^2(3)5 = 4(3)(5) = 12(5) = 60$$

If you're working with friends, then they might take a very different route. They might start by dividing by 3. Once they have $60 = (3)(20)$ they might see that 20 ends in a "0," and pull out a 5. The path would be as follows:

$$60 = 3(20) = 3(5)(4) = 3(5)(2)(2) = 2^2(3)5$$

There are often many different paths, but the final answer is unique. Though you and friends might take different roads to the solution, the solution itself will always be the same.



1-6-23

Let's try factoring 72 using the above technique.

We might start by pulling out "2"s until the number isn't even:

$$72 = 2(36) = 2(2)(18) = 2(2)(2)(9) = 2(2)(2)(3)(3) = 2^3(3^2)$$

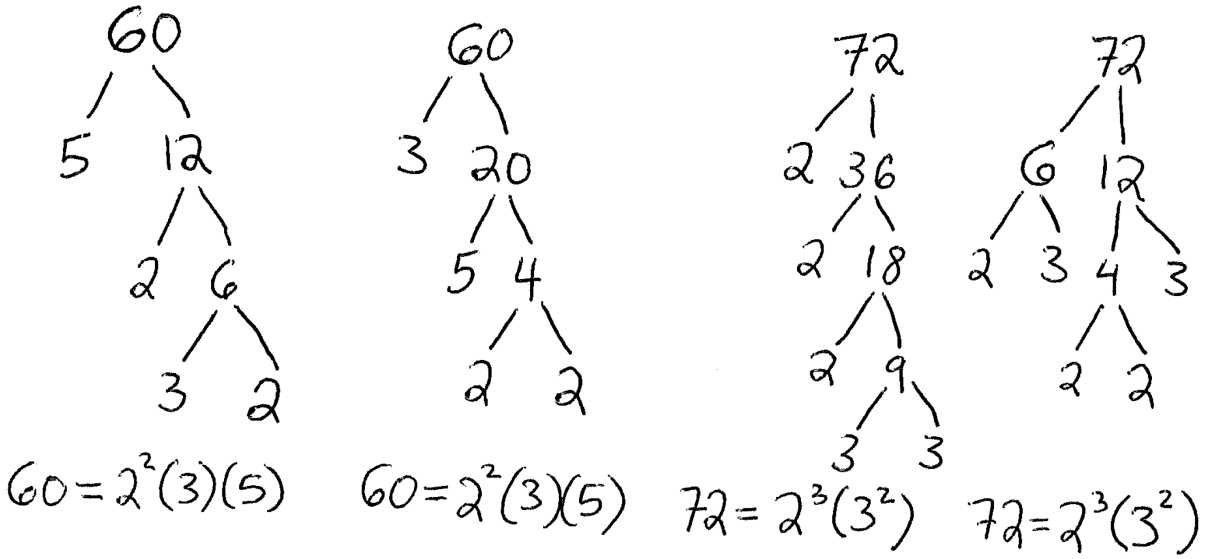
Alternatively, we might remember that $72 = 6(12)$, from our multiplication tables, so we could start there.

$$72 = 6(12) = (2)(3)(4)(3) = (2)(3)(2)(2)(3) = 2^3(3^2)$$

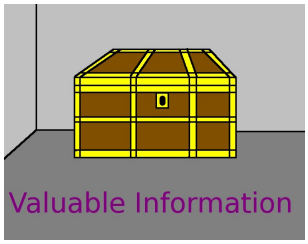
Of course, it is imperative to check the work by multiplying it back out.

$$2^3(3^2) = 8(9) = 72$$

There's a technique, called "drawing factor trees," that can help with doing this rapidly and painlessly. The trick is better illustrated with a drawing.



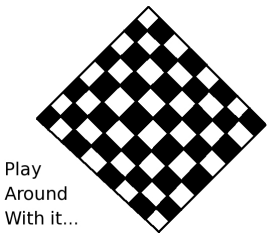
This method of writing out the process seems to help students do it faster.



We've actually hit an important theorem in mathematics! **Every integer greater than 1 can be written as a product of primes.** Moreover, the product of primes that you get is unique, up to the order in which you write them. This fact is sometimes called *the fundamental theorem of arithmetic*.

Since it is mathematical convention to write them in an increasing order, the factorization is unique in an absolute sense. That means that you and a friend might take different routes to solution, but you should get the same final answer.

Let's do a practice problem before continuing.



1-6-24

Factor the following numbers into a product of primes, written in an increasing order:

- 45
- 144
- 88
- 120
- 308

The answers will be given on Page 216

Unfortunately, many high school teachers tell their students that 1 is prime. That's not the convention in mathematics at all. One of the functions we use in number theory is the number of primes in the prime factorization, counting the multiplicities. For example, $30 = (2)(3)(5)$ has length 3, and $60 = 2^2(3)(5)$ has length 4, where as $720 = 2^4(3^2)(5)$ has length $4 + 2 + 1 = 7$.

Look how this would be wrecked if we considered 1 to be prime:

$$30 = (2)(3)(5) = (1)(2)(3)(5) = (1)(1)(2)(3)(5) = (1)(1)(1)(2)(3)(5) = (1)(1)(1)(1)(2)(3)(5)$$

Other things would break as well. The prime factorization of a number would no longer be unique, because you and your friend might use a different number of 1s. There is a theorem that if p is in the prime factorization of n, then $n/p < n$. This theorem, which is obviously true, moderately easy to prove, but very useful in proving more complicated theorems, would become false if we allowed $p = 1$ to be considered a prime.

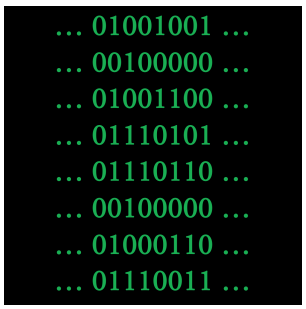
With all these techniques, perhaps you are thinking that factoring an integer is an easy task. The distinction here has to do with exactly which integers are to be factored. As it turns out, we should classify integers based the number of primes in the prime factorization, counting the multiplicities—which we called length in the previous box.

- If the factorization of z is of length two, we are guaranteed that there is a prime p dividing z such that $p \leq \sqrt{z}$.
- If the factorization of z is of length three, we are guaranteed that there is a prime p dividing z such that $p \leq \sqrt[3]{z}$.
- If the factorization of z is of length four, we are guaranteed that there is a prime p dividing z such that $p \leq \sqrt[4]{z}$.
- If the factorization of z is of length n, we are guaranteed that there is a prime p dividing z such that $p \leq \sqrt[n]{z}$.

The previous box stated that if the factorization of z is of length n, we are guaranteed that there is a prime p dividing z such that $p \leq \sqrt[n]{z}$.

I'd like to talk about the practical consequences of this theorem. For example, if you want to factor a number on the order of 10^{16} using trial division, and you know that $n > 3$, then you only need to search up to $\sqrt[4]{10^{16}} = 10^4$ to find the first prime factor. Then you pull that factor out, and work on the rest of the number, which is surely smaller than the original. In contrast, if $n = 2$, then you would have to search up to 10^8 to find the first prime factor. This means that your search space would be $10^8/10^4 = 10^{8-4} = 10^4 = 10,000$ times larger.

In general, z has to be fairly large before factoring becomes inconvenient—vaguely on the order of 10^{10} for a computer. It is harder to say when factoring becomes inconvenient for a human, because there are special tricks, including the Fermat Factorization Algorithm, invented by Pierre de Fermat (1607–1665). I am not sure if the majority of math professors know that trick, but you'll learn about it before this book is over.



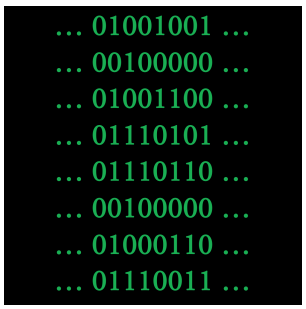
Of course, you're probably already aware that encryption is of primary importance on the internet. Without it, everyone would be able to read everyone else's emails, credit card numbers, and people could log into each other's accounts on websites. Without encryption, we would not have the internet as we know it, especially in terms of eCommerce.

By leaps and bounds, the most important cipher on the internet is *RSA*. It is so common place that some people mistakenly imagine that cryptography—the science of codes—is synonymous with studying only RSA. The letters RSA stand for the first letters of the last names of the inventors: Ron Rivest, Adi Shamir, and Leonard Adleman.

In order to understand RSA, you have to understand number theory. There's lots and lots of number theory connected to RSA. It will be our closing topic in this book.

It is often stated that the security of RSA rests on the hardness of factoring. Basically, because it is extremely infeasible to factor enormous numbers (around 400-digits long) of a special form (the product of two primes), the RSA cipher is secure when used properly.

However, if someone were to develop a new method of factoring, such as a quantum computer, then RSA would be broken.

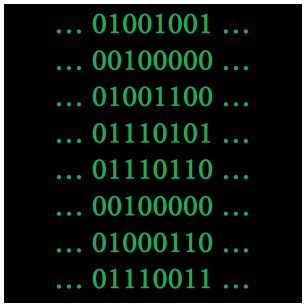


For the RSA cipher, because it depends on the hardness of factoring, the designers were clever and chose the worst possible case. There are primality tests that can test very large integers for primality very quickly. These use number theory techniques that you haven't been taught yet, but you can learn about them from any serious course in mathematical cryptography. That makes the $n = 1$ case easy to detect.

Accordingly, the worst case for factoring is $n = 2$. If we have a product of two distinct 100-digit primes, we will have a 200-digit number. The length of the prime factorization is just two. That means we would need to check all the primes up to 10^{100}, which is totally infeasible. Even checking up to 10^{16} would be very, very slow. In practice, cryptographers tend to use 300-digit and 400-digit numbers.

As you can see, all of this is a direct consequence of the fact that if the factorization of z is of length two, we are guaranteed that there is a prime p dividing z such that $p \leq \sqrt{z}$. In turn, that is a consequence of the fact that if the factorization of z is of length n, we are guaranteed that there is a prime p dividing z such that $p \leq \sqrt[n]{z}$. The former is just the latter restricted to $n = 2$.

We can actually prove this fact, for all positive integers n, so we will do that momentarily.



There are other factorization methods, such as the Pollard-rho method, the Elliptic-Curve Factorization method (see Page 240 of the module "Fermat's Last Theorem and Some Famous Unsolved Problems"), the Fermat Factorization method, the B-factorial method, and my favorite—the Quadratic Sieve. The best method is an enhancement of the Quadratic Sieve, called the Number-Field Sieve. Again, you can learn about these tools from any serious course in mathematical cryptography. However, even with these tools, it remains the case that factoring the product of two large unequal primes is a very, very hard task.

Let us now turn to the proof of the fact that if an integer z has n primes in its prime factorization, then there is at least one p dividing n such that $p \leq \sqrt[n]{z}$.

Claim: If an integer z has n primes in its prime factorization, then there is at least one p dividing n such that $p \leq \sqrt[n]{z}$.
Proof: Assume that there is an integer z with n primes $\{p_1, p_2, p_3, \ldots, p_n\}$ in its prime factorization, but that there is no prime p dividing n such that $p \leq \sqrt[n]{z}$.

Since there is no prime p dividing n such that $p \leq \sqrt[n]{z}$, observe

$$\begin{array}{ccc} p_1 & > & \sqrt[n]{z} \\ p_2 & > & \sqrt[n]{z} \\ p_3 & > & \sqrt[n]{z} \\ \vdots & \vdots & \vdots \\ p_n & > & \sqrt[n]{z} \end{array}$$

Multiplying all of these together, we obtain

$$p_1 p_2 p_3 \cdots p_n > (\sqrt[n]{z})^n$$

but $(\sqrt[n]{z})^n = z$ so we have instead

$$p_1 p_2 p_3 \cdots p_n > z$$

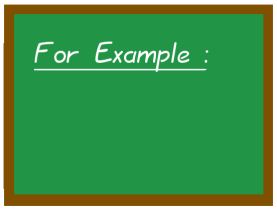
Of course

$$p_1 p_2 p_3 \cdots p_n = z$$

and plugging that into the previous inequality gives us $z > z$.

This is clearly false, giving us a contradiction! Therefore, our initial assumption must be false. It cannot be the case that there is an integer z with n primes $\{p_1, p_2, p_3, \ldots, p_n\}$ in its prime factorization, but with no prime p dividing n such that $p \leq \sqrt[n]{z}$.

In conclusion, if an integer z has n primes $\{p_1, p_2, p_3, \ldots, p_n\}$ in its prime factorization, then there is at least one p dividing n such that $p \leq \sqrt[n]{z}$. ■



1-6-25

We have (from the previous checkerboard) the factorizations $45 = 3^2(5)$ and $144 = 2^4(3^2)$. There is a technique for constructing the gcd and lcm rapidly. Moreover, they come out in factored form, automatically, when using this technique.

To make the lcm, we shall look prime by prime, and take the *larger* of the two exponents. For two, we see that it is absent from 45 (which means the zeroth power), and from 144, it is the fourth power. We write down 2^4. For three, we see that it is the second power in 45, and also the second power in 144. We write down 3^2. For five, we see that it is the first power in 45, and absent from 144 (which means the zeroth power), so we write down 5^1. We now have

$$\text{lcm}(45, 144) = (2^4)(3^2)(5^1) = 720$$

To make the gcd, we shall look prime by prime, and take the *smaller* of the two exponents. For two, we see that it is absent from 45 (which means the zeroth power), and from 144, it is the fourth power. We write down 2^0. For three, we see that it is the second power in 45, and also the second power in 144. We write down 3^2. For five, we see that it is the first power in 45, and absent from 144 (which means the zeroth power), so we write down 5^0. We now have

$$\text{gcd}(45, 144) = (2^0)(3^2)(5^0) = 9$$

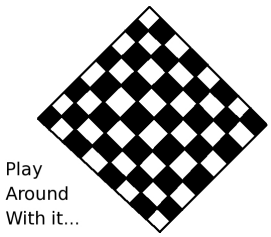
In order to check the gcd and the lcm computed in the previous box, we should make sure that the lcm (the least common multiple) which we claim is actually a common multiple of 45 and 144.

$$720 \div 144 = 5 \ \checkmark \qquad \text{and} \qquad 720 \div 45 = 16 \ \checkmark$$

Similarly, we should check that the gcd which we claim is actually a common divisor of 45 and 144.

$$45 \div 9 = 5 \ \checkmark \qquad \text{and} \qquad 144 \div 9 = 16 \ \checkmark$$

The word "cofactor," which we saw on Page 195 of this module, is also used here, to describe the 5 and the 16. So long as the two cofactors have a gcd equal to one, which means their set of common divisors is $\{1\}$, you have found the correct lcm and gcd.



1-6-26

Let's quickly practice the technique we just learned. You have already calculated the prime factorizations of 45, 88, 120, and 144, in the previous checkerboard box. Using those prime factorizations, compute the following:

- What is the $\text{gcd}(144, 88)$?
- What is the $\text{lcm}(144, 88)$?
- What is the $\text{gcd}(120, 144)$?
- What is the $\text{lcm}(120, 144)$?
- What is the $\text{gcd}(120, 45)$?
- What is the $\text{lcm}(120, 45)$?

The answers will be given on Page 217.

It should be noted that we're skipping over several theorems.

- Every positive integer can be written as a product of primes.
- The prime factorization of an integer is unique, up to ordering.
- The $\text{lcm}(p_1^{n_1}p_2^{n_2}p_3^{n_3}, p_1^{m_1}p_2^{m_2}p_3^{m_3}) = p_1^{e_1}p_2^{e_2}p_3^{e_3}$, where e_1 equal to the larger of n_1 and m_1, e_2 equal to the larger of n_2 and m_2, and e_3 equal to the larger of n_3 and m_3.
- The $\gcd(p_1^{n_1}p_2^{n_2}p_3^{n_3}, p_1^{m_1}p_2^{m_2}p_3^{m_3}) = p_1^{e_1}p_2^{e_2}p_3^{e_3}$, where e_1 equal to the smaller of n_1 and m_1, e_2 equal to the smaller of n_2 and m_2, and e_3 equal to the smaller of n_3 and m_3.
- For any two positive integers a and b, if the $\gcd(a,b) = g$, then the cofactors a/g and b/g have $\gcd(a/g, b/g) = 1$.
- For any two positive integers a and b, if the $\text{lcm}(a,b) = L$, then the cofactors L/a and L/b have $\gcd(L/a, L/b) = 1$.

It does not seem productive to prove these theorems at this time. Nonetheless, permit me to show you why the rapid gcd (and rapid lcm) techniques produce the correct answer.

Suppose we're working on computing the gcd of 120 and 144, but we don't yet know this min/max trick. We can factor however, and we get $120 = 2^3(3)(5)$ and $144 = 2^4(3^2)$.

I suppose I'd start by finding the possible values of G where G is a common divisor of 144 and 120. We'll make it the greatest common divisor as a second step. Maybe I think it should look like $G = 2^x3^y$, but I don't yet know what x and y are.

When I check my work, I need

$$\frac{120}{G} = \frac{2^3(3)(5)}{2^x3^y} \in \mathbb{Z} \qquad \text{and} \qquad \frac{144}{G} = \frac{2^4(3^2)}{2^x3^y} \in \mathbb{Z}$$

and it is pretty clear that if $x > 3$, then I will not be able to cancel all the 2s in the denominator for $120/G$—some will remain. This means $x \leq 3$. Similarly, it is pretty clear if $x > 4$, then I will not be able to cancel all the 2s in the denominator for $144/G$. In summary, I need $x \in \{0,1,2,3\}$ in order to make G a common divisor of 120 and 144.

Similarly, if $y > 1$, then I will not be able to cancel all the 3s in the denominator for $120/G$—some will remain. This means $y \leq 1$. For $144/G$, we can have $y \in \{0,1,2\}$, but if I want G to be a common divisor of 120 and 144, I need $y \in \{0,1\}$.

Now we come to 5. We account the 5 in the factorization of 120 as an exponent of 1, and the absence of a 5 in the factorization of 144 as an exponent of 0, because $5^0 = 1$. This means that I can't have a 5 in G at all. If G had a 5 in its factorization, then $144/G$ would not be an integer, because 144 is not divisible by 5. That's why I said $G = 2^x3^y$ and not $G = 2^x3^y5^z$.

To summarize the process so far, I need $x \in \{0,1,2,3\}$ and $y \in \{0,1\}$ to make G a common divisor of 120 and 144. Yet, I need the *greatest* common divisor, and so I should make $x = 3$ and $y = 1$, choosing the largest available choice for each.

Similarly, suppose we're working on computing the lcm of 120 and 144, but we don't yet know this min/max trick. Let's suppose I'll start by finding the possible values of L where L is a common multiple of 144 and 120. We'll make it the least common multiple as a second step. Maybe I think it should look like $L = 2^x 3^y 5$, but I don't yet know what x and y are.

When I check my work, I need

$$\frac{L}{120} = \frac{2^x 3^y 5}{2^3(3)(5)} \in \mathbb{Z} \qquad \text{and} \qquad \frac{L}{144} = \frac{2^x 3^y 5}{2^4(3^2)} \in \mathbb{Z}$$

and it is pretty clear that if $x < 3$, then I will not be able to cancel all the 2s in the denominator for $L/120$—some will remain. This means $x \geq 3$. Similarly, it is pretty clear if $x < 4$, then I will not be able to cancel all the 2s in the denominator for $L/144$. This means $x \geq 4$, in order to make L a common multiple of 120 and 144.

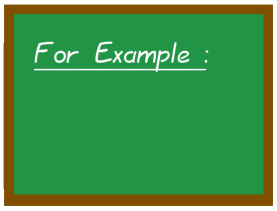
Similarly, if $y < 1$, then I will not be able to cancel all the 3s in the denominator for $L/120$—some will remain. This means $y \geq 1$. For $L/144$, I need $y \geq 2$, because if $y < 2$, then I cannot cancel all the 3s in the denominator of $L/144$. This means $y \geq 2$ in order to make L a common multiple of 120 and 144.

The question of what to do with the 5 now comes up. There needs to be a 5 in the factorization of L, otherwise $L/120$ will not be an integer. Should the factorization of L contain 5^1? 5^2? 5^3? Any positive power of 5 will be fine, because 120 has only one 5 in its prime factorization.

Since I need the *least* common multiple, I should make $x = 4$ and $y = 2$, choosing the smallest available choice for each. For that reason, I should also choose to raise the 5 to the first power, since higher powers would be wasteful.

Some of the techniques in this module were taught to me and my friends when we were in middle school. The purpose was not for computer science, but rather to help perform arithmetic without a calculator (with a paper and pencil). Doing arithmetic without a calculator was still considered a very important skill in the 1980s, even though calculators were already widely and cheaply available.

Let's study an example, given in the next box.



1-6-27

Consider adding $7/60 + 11/84$.

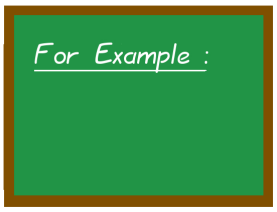
First, you would factor $60 = 5(12) = 5(4)(3) = 2^2(3)(5)$ and $84 = 4(21) = 2^2(3)(7)$. Second, you'd find the lcm of 60 and 84, which is $2^2(3)(5)(7) = 420$. Third, you'd find the cofactors $420/60 = 7$ and $420/84 = 5$. Fourth, in addition to checking the lcm, those cofactors help you put the fractions into the common denominator:

$$\frac{7(7)}{60(7)} + \frac{11(5)}{84(5)} = \frac{49}{420} + \frac{55}{420} = \frac{49+55}{420} = \frac{104}{420}$$

The fifth step was adding the numerators. Sixth, you factor $104 = 2(52) = 2^2(26) = 2^3(13)$. Seventh, you find the gcd of $104 = 2^3(13)$ and $420 = 2^2(3)(5)(7)$. That is $2^2 = 4$. Eighth, to check your gcd and to reduce $104/420$ to lowest terms, you compute the cofactors $104/4 = 26$ and $420/4 = 105$. The final answer is $104/420 = 26/105$.

In our hardest practice problems, we would frequently have 3-digit numerators and denominators, passing to 4-digit numbers on the way to a solution. This is great arithmetic drill, because you practice loads of math skills on the way to an answer.

Since you are no longer in middle school, I will not give you any practice problems with this technique.



1-6-28

Let's say that someone asks you to compute

$$\#\text{divisors}(1584) = \#\text{divisors}(2^4(3^2)11)$$

as well as

$$\#\text{divisors}(8100) = \#\text{divisors}(2^2(3^4)5^2)$$

meaning that we don't want the list of the divisors, but instead we merely want to know how many there are—the sizes of the sets.

Do you really have to compute the divisor sets of 1584 and 8100?! With our original technique, that would be phenomenally tedious, because we'd have to check from 1 to 1584 and from 1 to 8100. Using our more complicated technique, we must check up to 39 for 1584 because $39 < \sqrt{1584} < 40$ and we must check up to 90 because $90 = \sqrt{8100}$. That's not too horrible, but I'm sure you're very tired now, having read this long module, and you'd appreciate a shortcut. This is one of my favorite tricks in all of mathematics.

As it turns out

$$\begin{aligned} \#\text{divisors}(2^4(3^2)11) &= (4+1)(2+1)(1+1) = (5)(3)(2) = 30 \\ \#\text{divisors}(2^2(3^4)5^2) &= (2+1)(4+1)(2+1) = (3)(5)(3) = 45 \end{aligned}$$

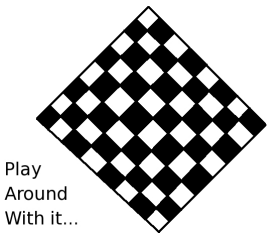
which we will verify by computer. (Just to be clear, you take all the exponents from the prime factorization, increase them by 1, and multiply them together—that's the number of divisors.) The Sage code for verification is given below.

```
print "For 1584..."
print divisors(1584)
print "Count = ", len(divisors(1584))
print
print "For 8100..."
print divisors(8100)
print "Count = ", len(divisors(8100))
```

The Sage code above gives the following output:

```
For 1584...
[1, 2, 3, 4, 6, 8, 9, 11, 12, 16, 18, 22, 24, 33, 36, 44, 48, 66, 72, 88,
99, 132, 144, 176, 198, 264, 396, 528, 792, 1584]
Count = 30

For 8100...
[1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 25, 27, 30, 36, 45, 50, 54, 60,
75, 81, 90, 100, 108, 135, 150, 162, 180, 225, 270, 300, 324, 405, 450, 540,
675, 810, 900, 1350, 1620, 2025, 2700, 4050, 8100]
Count = 45
```

As you can see, the technique appears to be correct (for these two cases). Of course, this is not a mathematical proof.



1-6-29

Tell me how many divisors the following numbers have.

- 10
- 60
- 100
- 360
- 3600

The answers will be given on Page 217.

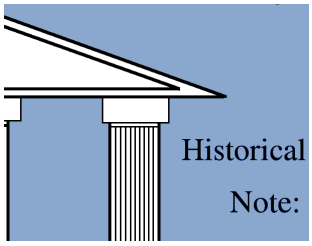
You probably are thinking that the previous question has no relationship to practical reality. Once again, that turns out to be false. It has to do with how civilizations organize their units. Let's put ourselves in the place of a caravan of merchants in the ancient period.

In the previous box, you computed that 100 has 9 divisors. They are

$$\text{divisors}(100) = \{1, 2, 4, 5, 10, 20, 25, 50, 100\}$$

which means that you can divide some pile of identical goods among 1, 2, 4, 5, 10, 20, 25, 50, or 100 trading partners evenly. Any other number of trading partners would make equal division impossible.

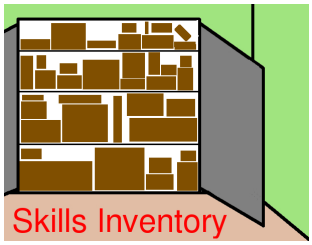
We will continue in the next box.



In contrast to our decimal system, the Babylonians liked to use 60, 360, and 3600 for their units. This is far more flexible, permitting many other sizes. Consider instead

$$\begin{aligned}
\text{divisors}(60) &= \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\} \\
\text{divisors}(360) &= \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, \\
&\quad 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360\} \\
\\
\text{divisors}(3600) &= \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, \\
&\quad 20, 24, 25, 30, 36, 40, 45, 48, 50, 60, 72, 75, \\
&\quad 80, 90, 100, 120, 144, 150, 180, 200, 225, 240, \\
&\quad 300, 360, 400, 450, 600, 720, 900, 1200, 1800, 3600\}
\end{aligned}$$

That is why, to this very day, we divide minutes into 60 seconds, a circle into 360 degrees, and an hour into 3600 seconds. Those units come directly from the Babylonians.



This module is now complete. Here is a list of some of the things that you learned during this module.

- Computing the set of multiples of a positive integer.
- Computing the set of common multiples of two integers.
- The meaning of the lcm of two integers.
- Computing the set of divisors of a positive integer.
- Computing the set of common divisors of two integers.
- The meaning of the gcd of two integers.
- The formula relating the gcd and lcm of a pair of integers.
- How to determine if a (somewhat small) number is prime.
- How to determine if a (somewhat small) number is a twin prime.
- How to factor numbers rapidly.
- How to compute the gcd and lcm of two numbers, from their prime factorizations.
- One of my favorite tricks, finding out how many divisors a number has, from its prime factorization.
- We had the vocabulary terms: common divisors, common multiples, gcd, greatest common divisor, lcm, least common multiple, set of divisors, set of multiples, the fundamental theorem of arithmetic, twin prime.

You were asked to calculate two sets of multiples on Page 189.

1. multiples(5) $= \{5, 10, 15, 20, 25, \ldots\}$
2. multiples(2) $= \{2, 4, 6, 8, 10, \ldots\}$

Here is the answer to the common multiples question from Page 190.

- The common multiples of 2 and 5 are $\{10, 20, 30, 40, 50, \ldots\}$.
- The common multiples of 6 and 8 are $\{24, 48, 72, 96, 120, \ldots\}$.
- The common multiples of 3 and 12 are $\{12, 24, 36, 48, 60, \ldots\}$.

Here are the answers to the question about adding fractions on Page 191.

- When adding $1/4 + 1/6$, what is the lowest common denominator? [Answer: 12.]
- When adding $1/2 + 1/5$, what is the lowest common denominator? [Answer: 10.]
- When subtracting $1/6 - 1/8$, what is the lowest common denominator? [Answer: 24.]
- When adding $1/3 + 1/12$, what is the lowest common denominator? [Answer: 12.]

On Page 193, I asked you to write the rosters of the unions of some sets of multiples. Here are the answers.

1. $\text{multiples}(4) \cup \text{multiples}(6) = \{4, 6, 8, 12, 16, 18, 20, 24, 28, 30, \ldots\}$
2. $\text{multiples}(6) \cup \text{multiples}(8) = \{6, 8, 12, 16, 18, 24, 30, 32, 36, 40, \ldots\}$
3. $\text{multiples}(2) \cup \text{multiples}(5) = \{2, 4, 5, 6, 8, 10, 12, 14, 15, 16, \ldots\}$

Note, there is clearly some structure here, but the structure appears to be different in each case. It certainly doesn't collapse neatly into a single item, like the intersections did.

On Page 194, you were asked to find the divisors of 15.
[Answer: $\text{divisors}(15) = \{1, 3, 5, 15\}$.]

Here are the sets of divisors that you were asked to compute on Page 197.

- The set of divisors of 72 is $\{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72\}$.
- The set of divisors of 36 is $\{1, 2, 3, 4, 6, 9, 12, 18, 36\}$.
- The set of divisors of 40 is $\{1, 2, 4, 5, 8, 10, 20, 40\}$.
- The set of divisors of 90 is $\{1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90\}$.

Here are the sets of common divisors, which you were asked to compute on Page 199.

- What is the set of common divisors of 36 and 40?

$$\text{divisors}(36) \cap \text{divisors}(40) = \{1, 2, 4\}$$

- What is the set of common divisors of 36 and 60?

$$\text{divisors}(36) \cap \text{divisors}(60) = \{1, 2, 3, 4, 6, 12\}$$

- What is the set of common divisors of 72 and 60?

$$\text{divisors}(72) \cap \text{divisors}(60) = \{1, 2, 3, 4, 6, 12\}$$

- What is the set of common divisors of 40 and 60?

$$\text{divisors}(40) \cap \text{divisors}(60) = \{1, 2, 4, 5, 10, 20\}$$

- What is the set of common divisors of 36 and 42?

$$\text{divisors}(36) \cap \text{divisors}(42) = \{1, 2, 3, 6\}$$

- What is the set of common divisors of 40 and 42?

$$\text{divisors}(40) \cap \text{divisors}(42) = \{1, 2\}$$

- What is the set of common divisors of 42 and 72?

$$\text{divisors}(42) \cap \text{divisors}(72) = \{1, 2, 3, 6\}$$

On Page 200 you were asked to rewrite your answers to the previous checkerboard box, writing each answer as the set of divisors of some other number. Here are the answers.

- What is the set of common divisors of 36 and 40? [Answer: $\{1, 2, 4\} = \text{divisors}(4)$.]
- What is the set of common divisors of 36 and 60?
  [Answer: $\{1, 2, 3, 4, 6, 12\} = \text{divisors}(12)$.]
- What is the set of common divisors of 72 and 60?
  [Answer: $\{1, 2, 3, 4, 6, 12\} = \text{divisors}(12)$.]
- What is the set of common divisors of 40 and 60?
  [Answer: $\{1, 2, 4, 5, 10, 20\} = \text{divisors}(20)$.]
- What is the set of common divisors of 36 and 42? [Answer: $\{1, 2, 3, 6\} = \text{divisors}(6)$.]
- What is the set of common divisors of 40 and 42? [Answer: $\{1, 2\} = \text{divisors}(2)$.]
- What is the set of common divisors of 42 and 72? [Answer: $\{1, 2, 3, 6\} = \text{divisors}(6)$.]

On Page 202, you were asked to complete the following equation, in general.

$$\frac{(x)(y)}{\gcd(x,y)} = ??$$

Answer: in general,

$$\frac{(x)(y)}{\gcd(x,y)} = \text{lcm}(x,y)$$

which is yet another reason why the gcd is "the mother of all operations" in exact rational arithmetic.

If we can code a good, fast, and efficient gcd function, then we get a good, fast, and efficient lcm function by applying the above formula. Using those fast gcd and lcm functions, we can perform exact rational addition, subtraction, multiplication and division.

On Page 203, you were asked to determine if four particular positive integers are prime or composite.

- Is 105 prime? [Answer: 105 is clearly divisible by 5, so it is composite.]
- Is 101 prime? [Answer: 101 is prime.]
- Is 61 prime? [Answer: 61 is prime.]
- Is 69 prime? [Answer: Since $6+9=15$, and 15 is divisible by 3, we know 69 is divisible by 3, and therefore 69 is composite.]

On Page 203, you were asked to determine whether or not five particular integers are twin primes.

- Is 7 a twin prime? [Answer: 7 is prime and 5 is prime, so yes.]
- Is 15 a twin prime? [Answer: $15 = 5(3)$ is composite, so no.]
- Is 61 a twin prime? [Answer: 61 is prime and 59 is prime, so yes.]
- Is 67 a twin prime? [Answer: 67 is prime but $65 = 5(13)$ and $69 = 3(23)$, so no.]
- Is 103 a twin prime? [Answer: 103 is prime and 101 is prime, so yes.]

Here are the solutions to the question from Page 205 where you were asked to factor some integers into a product of primes.

- $45 = 3^2(5)$
- $144 = 2^4(3^2)$
- $88 = 2^3(11)$
- $120 = 2^3(3)(5)$
- $308 = 2^2(7)11$

On Page 208, you were asked to compute some gcds and lcms based on the prime factorizations of the given numbers. Here are the answers..

- What is the $\gcd(144, 88)$? [Answer: $2^3 = 8$.]
- What is the $\text{lcm}(144, 88)$? [Answer: $2^4(3^2)11 = 1584$.]
- What is the $\gcd(120, 144)$? [Answer: $2^3(3) = 24$.]
- What is the $\text{lcm}(120, 144)$? [Answer: $2^4(3^2)(5) = 720$.]
- What is the $\gcd(120, 45)$? [Answer: $(3)(5) = 15$.]
- What is the $\text{lcm}(120, 45)$? [Answer: $2^3(3^2)(5) = 360$.]

On Page 212, I asked you to compute the number of divisors for 10, 60, 100, 360, and 3600.

- Because $10 = (2)(5)$, there are $(1+1)(1+1) = 2(2) = 4$ divisors.
- Because $60 = 2^2(3)(5)$, there are $(2+1)(1+1)(1+1) = 3(2)(2) = 12$ divisors.
- Because $100 = 2^2(5^2)$, there are $(2+1)(2+1) = 3(3) = 9$ divisors.
- Because $360 = 2^3(3^2)5$, there are $(3+1)(2+1)(1+1) = 4(3)(2) = 24$ divisors.
- Because $3600 = 2^4(3^2)5^2$, there are $(4+1)(2+1)(2+1) = 5(3)(3) = 45$ divisors.