## Section 4: Prime Numbers

Another concept you have likely studied in the past is that of a *prime number*. There are no surprises with this definition.

> **Definition**
>
> An integer $n > 1$ is called *prime* if its only positive divisors are 1 and $n$. Otherwise it is called *composite*.

The earliest mathematicians known to have classified integers into prime and composite were the Pythagoreans, at approximately the same time period as the lifetime of the prophet Daniel (550 to 520 B.C.). Of course, historians do not know for certain that there were not others who studied prime numbers in earlier times.

### Exploring the Definition

Consider the integer 5. First, $5 > 1$, so 5 is eligible to be called prime or composite (–5 would not be eligible to be called prime or composite according to our definition). We then determine the positive divisors of 5: $1 \mid 5$, $2 \nmid 5$, $3 \nmid 5$, $4 \nmid 5$, $5 \mid 5$. Since the only positive divisors of 5 are 1 and 5, 5 is prime.

Now consider the integer 24. Since $24 = 4 \cdot 6$, $4 \mid 24$ and $6 \mid 24$. Therefore 24 is composite.

When checking an integer $n$ to see if it has divisors other than 1 and $n$, we do not actually have to check all the integers 2 through $n - 1$; we only need check the integers 2 through $\lfloor \sqrt{n} \rfloor$ (see footnote[6]). Why? Look at the previous example, where $24 = 4 \cdot 6$, for a hint; the smaller of the two factors, namely 4, is less than $\sqrt{24}$. In fact, suppose that $x \mid n$, where $x \neq 1$ and $x \neq n$. Then $n = x \cdot y$ for some integer $y$, and we must also have $y \neq 1$ and $y \neq n$. Suppose both of $x$ and $y$ were larger than $\sqrt{n}$. Then

$$n = xy > \sqrt{n} \cdot \sqrt{n} = n,$$

which is a contradiction; we cannot have $n > n$, that is, there is no number that is greater than itself. The supposition that led to the contradiction, namely that both $x$ and $y$ are larger than $\sqrt{n}$, must therefore be false, and we conclude that at least one of them must be not larger than $\sqrt{n}$. Consequently, if we have checked all the integers from 2 through $\lfloor \sqrt{n} \rfloor$ and found no divisors of $n$, then $n$ must be prime.

Now let's check 31 for primality. Since $\sqrt{31} = 5.57$, we need only check to see if 2, 3, 4, or 5 divide 31. In fact, there's one more possibility we can eliminate! We can also skip checking for divisibility by the composite number $4 = 2 \cdot 2$. Why? Because if $4 \mid n$, so does 2. If $4 \mid n$, there is an integer $a$ such that $n = 4 \cdot a$. But then $n = 2 \cdot 2a$, and $2 \mid n$ by definition. If $2 \nmid n$, then neither will 4, so 4 does not need to be checked. The same is true for any composite number. Our list to check is now 2, 3, and 5.

$2 \nmid 31$ since $2 \nmid 1$

$3 \nmid 31$ since $3 + 1 = 4$ and $3 \nmid 4$

$5 \nmid 31$ since $5 \nmid 1$

Therefore 31 is prime![7] This is called the *method of trial division*.

---

[6] the "floor function": $\lfloor k \rfloor$ is the largest integer less than or equal to $k$.

[7] it is not necessary to use the divisibility tests; the methods of section 1.2 suffice.