## SECTION 3.5 Primes and Greatest Common Divisors

*The prime numbers are the building blocks for the natural numbers in terms of multiplication, just as the elements (like carbon, oxygen, or uranium) are the building blocks of all matter. Just as we can put two hydrogen atoms and one oxygen atom together to form water, every composite natural number is uniquely constructed by multiplying together prime numbers. Analyzing numbers in terms of their prime factorizations allows us to solve many problems, such as finding greatest common divisors. Prime numbers have fascinated people for millennia, and many easy-to-state questions about them remain unanswered. Students interested in pursuing these topics more should definitely consider taking a course in number theory.*

**1.** In each case we can just use trial division up to the sqnare root of the number being tested.

**a)** Since $21 = 3 \cdot 7$, we know that 21 is not prime.

**b)** Since $2 \not| 29$, $3 \not| 29$, and $5 \not| 29$, we know that 29 is prime. We needed to check for prime divisors only up to $\sqrt{29}$, which is less than 6.

**c)** Since $2 \not| 71$, $3 \not| 71$, $5 \not| 71$, and $7 \not| 71$, we know that 71 is prime.

**d)** Since $2 \not| 97$, $3 \not| 97$, $5 \not| 97$, and $7 \not| 97$, we know that 97 is prime.

**e)** Since $111 = 3 \cdot 37$, we know that 111 is not prime.

**f)** Since $143 = 11 \cdot 13$, we know that 143 is not prime.

**3.** In each case we can use trial division, starting with the smallest prime and increasing to the next prime once we find that a given prime no longer is a divisor of what is left. A calculator comes in handy. Alternatively, one could use a factor tree.

**a)** We note that 2 is a factor of 88, and the quotient upon division by 2 is 44. We divide by 2 again, and then again, leaving a quotient of 11. Since 11 is prime, we are done, and we have found the prime factorization: $88 = 2^3 \cdot 11$.

**b)** $126 = 2 \cdot 63 = 2 \cdot 3 \cdot 21 = 2 \cdot 3 \cdot 3 \cdot 7 = 2 \cdot 3^2 \cdot 7$

**c)** $729 = 3 \cdot 243 = 3 \cdot 3 \cdot 81 = 3 \cdot 3 \cdot 3 \cdot 27 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 9 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 3^6$

**d)** $1001 = 7 \cdot 143 = 7 \cdot 11 \cdot 13$

**e)** $1111 = 11 \cdot 101$ (we know that 101 is prime because we have already tried all prime factors less than $\sqrt{101}$)

f) $909090 = 2\cdot 454545 = 2\cdot 3\cdot 151515 = 2\cdot 3\cdot 3\cdot 50505 = 2\cdot 3\cdot 3\cdot 3\cdot 16835 = 2\cdot 3\cdot 3\cdot 3\cdot 5\cdot 3367 = 2\cdot 3\cdot 3\cdot 3\cdot 5\cdot 7\cdot 481 = 2\cdot 3\cdot 3\cdot 3\cdot 5\cdot 7\cdot 13\cdot 37 = 2\cdot 3^3\cdot 5\cdot 7\cdot 13\cdot 37$

**5.** $10! = 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10 = 2\cdot 3\cdot 2^2\cdot 5\cdot (2\cdot 3)\cdot 7\cdot 2^3\cdot 3^2\cdot (2\cdot 5) = 2^8\cdot 3^4\cdot 5^2\cdot 7$

**7.** We give a proof by contradiction. Suppose that in fact $\log_2 3$ is the rational number $p/q$, where $p$ and $q$ are integers. Since $\log_2 3 > 0$, we can assume that $p$ and $q$ are positive. Translating the equation $\log_2 3 = p/q$ into its exponential equivalent, we obtain $3 = 2^{p/q}$. Raising both sides to the $q^{\text{th}}$ power yields $3^q = 2^p$. Now this is a violation of the Fundamental Theorem of Arithmetic, since it gives two different prime factorizations of the same number. Hence our assumption (that $\log_2 3$ is rational) must be wrong, and we conclude that $\log_2 3$ is irrational.

**9.** This is simply an existence statement. To prove that it is true, we need only exhibit the primes. Indeed, 3, 5, and 7 satisfy the conditions. (Actually, this is the only example, and a harder problem is to prove that there are no others.)

**11.** The prime factors of 30 are 2, 3, and 5. Thus we are looking for positive integers less than 30 that have none of these as prime factors. Since the smallest prime number other than these is 7, and $7^2$ is already greater than 30, in fact only primes (and the number 1) will satisfy this condition. Therefore the answer is 1, 7, 11, 13, 17, 19, 23, and 29.

**13.** a) Since $\gcd(11,15) = 1$, $\gcd(11,19) = 1$, and $\gcd(15,19) = 1$, these three numbers are pairwise relatively prime.

b) Since $\gcd(15,21) = 3 > 1$, these three numbers are not pairwise relatively prime.

c) Since $\gcd(12,17) = 1$, $\gcd(12,31) = 1$, $\gcd(12,37) = 1$, $\gcd(17,31) = 1$, $\gcd(17,37) = 1$, and $\gcd(31, 37) = 1$, these four numbers are pairwise relatively prime. (Indeed, the last three are primes, and the prime factors of the first are 2 and 3.)

d) Again, since no two of 7, 8, 9, and 11 have a common factor greater than 1, this set is pairwise relatively prime.

**15.** The identity shown in the hint is valid, as can be readily seen by multiplying out the right-hand side (all the terms cancel—telescope—except for $2^{ab}$ and $-1$). We will prove the assertion by proving its contrapositive. Suppose that $n$ is *not* prime. Then by definition $n = ab$ for some integers $a$ and $b$ each greater than 1. Since $a > 1$, $2^a - 1$, the first factor in the suggested identity, is greater than 1. Clearly the second factor is greater than 1. Thus $2^n - 1 = 2^{ab} - 1$ is the product of two integers each greater than 1, so it is not prime.

**17.** We compute $\phi(n)$ here by enumerating the set of positive integers less than $n$ that are relatively prime to $n$.

a) $\phi(4) = |\{1,3\}| = 2$ b) $\phi(10) = |\{1,3,7,9\}| = 4$

c) $\phi(13) = |\{1,2,3,4,5,6,7,8,9,10,11,12\}| = 12$

**19.** All the positive integers less than or equal to $p^k$ (and there are clearly $p^k$ of them) are less than $p^k$ and relatively prime to $p^k$ unless they are a multiple of $p$. Since the fraction $1/p$ of them are multiples of $p$, we have $\phi(p^k) = p^k\,(1 - 1/p) = p^k - p^{k-1}$.

**21.** To find the greatest common divisor of two numbers whose prime factorizations are given, we just need to take the smaller exponent for each prime.

a) The first number has no prime factors of 2, so the gcd has no 2's. Since the first number has seven factors of 3, but the second number has only five, the gcd has five factors of 3. Similarly the gcd has a factor of $5^3$. So the gcd is $3^5\cdot 5^3$.

b) These numbers have no common prime factors, so the gcd is $1$. c) $23^{17}$ d) $41 \cdot 43 \cdot 53$

e) These numbers have no common prime factors, so the gcd is $1$.

f) The gcd of any positive integer and $0$ is that integer, so the answer is $1111$.

**23.** To find the least common multiple of two numbers whose prime factorizations are given, we just need to take the larger exponent for each prime.

a) The first number has no prime factors of $2$ but the second number has $11$ of them, so the lcm has $11$ factors of $2$. Since the first number has seven factors of $3$ and the second number has five, the lcm has seven factors of $3$. Similarly the lcm has a factor of $5^9$ and a factor of $7^3$. So the lcm is $2^{11} \cdot 3^7 \cdot 5^9 \cdot 7^3$.

b) These numbers have no common prime factors, so the lcm is their product, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$.

c) $23^{31}$ d) $41 \cdot 43 \cdot 53$ e) $2^{12} \cdot 3^{13} \cdot 5^{17} \cdot 7^{21}$, as in part (b)

f) It makes no sense to ask for a positive multiple of $0$, so this question has no answer. Least common multiples are defined only for positive integers.

**25.** First we find the prime factorizations: $92928 = 2^8 \cdot 3 \cdot 11^2$ and $123552 = 2^5 \cdot 3^3 \cdot 11 \cdot 13$. Therefore $\gcd(92928, 123552) = 2^5 \cdot 3 \cdot 11 = 1056$ and $\text{lcm}(92928, 123552) = 2^8 \cdot 3^3 \cdot 11^2 \cdot 13 = 10872576$. The requested products are $(2^5 \cdot 3 \cdot 11) \cdot (2^8 \cdot 3^3 \cdot 11^2 \cdot 13)$ and $(2^8 \cdot 3 \cdot 11^2) \cdot (2^5 \cdot 3^3 \cdot 11 \cdot 13)$, both of which are $2^{13} \cdot 3^4 \cdot 11^3 \cdot 13 = 11{,}481{,}440{,}256$.

**27.** The important observation to make here is that the smaller of any two numbers plus the larger of the two numbers is always equal to the sum of the two numbers. Since the exponent of the prime $p$ in $\gcd(a,b)$ is the smaller of the exponents of $p$ in $a$ and in $b$, and since the exponent of the prime $p$ in $\text{lcm}(a,b)$ is the larger of the exponents of $p$ in $a$ and in $b$, the exponent of $p$ in $\gcd(a,b)\text{lcm}(a,b)$ is the sum of the smaller and the larger of these two values. Therefore by the observation, it equals the sum of the two values themselves, which is clearly equal to the exponent of $p$ in $ab$. Since this is true for every prime $p$, we conclude that $\gcd(a,b)\text{lcm}(a,b)$ and $ab$ have the same prime factorizations and are therefore equal.

**29.** Obviously there are no definitive answers to these problems, but we present below a reasonable and satisfying rule for forming the sequence in each case.

a) There are 1's in the prime locations and 0's elsewhere. In other words, the $n^{\text{th}}$ term of the sequence is $1$ if $n$ is a prime number and $0$ otherwise.

b) The suspicious 2's occurring every other term and the appearance of the 11 and 13 lead us to discover that the $n^{\text{th}}$ term is the smallest prime factor of $n$ (and is $1$ when $n = 1$).

c) The $n^{\text{th}}$ term is the number of positive divisors of $n$. For example, the twelfth term is $6$, since $12$ has the positive divisors $1$, $2$, $3$, $4$, $6$, and $12$. A tip-off to get us going in the right direction is that there are 2's in the prime locations.

d) Perhaps the composer of the problem had something else in mind, but one rule here is that the $n^{\text{th}}$ term is $0$ if and only if $n$ has a repeated prime factor; the 1's occur at locations for which $n$ is "square-free" (has no factor, other than $1$, that is a perfect square). For example, $12$ has the square $2^2$, so the twelfth term is $0$.

e) We note that all the terms (after the first one) are primes. This leads us to guess that the $n^{\text{th}}$ term is the largest prime less than or equal to $n$ (and is $1$ when $n = 1$).

f) Each term comes from the one before it by multiplying by a certain number. The multipliers are $2$, $3$, $5$, $7$, $11$, $13$, $17$, $19$, and $23$—the primes. So the rule seems to be that we obtain the next term from the $n^{\text{th}}$ term by multiplying by the $n^{\text{th}}$ prime number (and we start at 1). In other words, the $n^{\text{th}}$ term is the product of the smallest $n-1$ prime numbers.

**31.** Consider the product $n(n+1)(n+2)$ for some integer $n$. Since every second integer is even (divisible by 2), this product is divisible by 2. Since every third integer is divisible by 3, this product is divisible by 3. Therefore this product has both 2 and 3 in its prime factorization and is therefore divisible by $2 \cdot 3 = 6$.

**33.** It is hard to know how to get started on this problem. To some extent, mathematics is an experimental science, so it would probably be a good idea to compute $n^2 - 79n + 1601$ for several positive integer values of $n$ to get a feel for what is happening. Using a computer, or at least a calculator, would be helpful. If we plug in $n = 1, 2, 3, 4,$ and $5$, then we get the values 1523, 1447, 1373, 1301, and 1231, all of which are prime. This may lead us to believe that the proposition is true, but it gives us no clue as to how to prove it. Indeed, it seems as if it would be very hard to prove that this expression *always* produces a prime number, since being prime means the absence of nontrivial factors, and nothing in the expression seems to be very helpful in proving such a negative assertion. (The fact that we cannot factor it algebraically is irrelevant—in fact, if it factored algebraically, then it would essentially *never* be prime.) Perhaps we should try some more integers. If we do so, we find a lot more prime numbers, but we are still skeptical. Well, perhaps there is some way to arrange that this expression will have a factor. How about 1601? Well, yes! If we let $n = 1601$, then all three terms will have 1601 as a common factor, so that 1601 is a factor of the entire expression. In fact, $1601^2 - 79 \cdot 1601 + 1601 = 1601 \cdot 1523$. So we have found a counterexample after all, and the proposition is false. Note that this was not a problem in which we could proceed in a calm, calculated way from problem to solution. Mathematics is often like that—lots of false leads and approaches that get us nowhere, and then suddenly a burst of insight that solves the problem. (The smallest $n$ for which this expression is not prime is $n = 80$; this gives the value $1681 = 41 \cdot 41$.)

**35.** Recall that the proof that there are infinitely many primes starts by assuming that there are only finitely many primes $p_1, p_2, \ldots, p_n$, and forming the number $p_1p_2\cdots p_n + 1$. This number is either prime or has a prime factor different from each of the primes $p_1, p_2, \ldots, p_n$; this shows that there are infinitely many primes. So, let us suppose that there are only finitely many primes of the form $4k+3$, namely $q_1, q_2, \ldots, q_n$, where $q_1 = 3$, $q_2 = 7$, and so on.

What number can we form that is not divisible by any of these primes, but that must be divisible by a prime of the form $4k + 3$? We might consider the number $4q_1q_2\cdots q_n + 3$. Unfortunately, this number is not prime, as it is is divisible by 3 (because $q_1 = 3$). Instead we consider the number $Q = 4q_1q_2\cdots q_n - 1$. Note that $Q$ is of the form $4k + 3$ (where $k = q_1q_2\cdots q_n - 1$). If $Q$ is prime, then we have found a prime of the desired form different from all those listed. If $Q$ is not prime, then $Q$ has at least one prime factor not in the list $q_1, q_2, \ldots, q_n$, because the remainder when $Q$ is divided by $q_j$ is $q_j - 1$, and $q_j - 1 \neq 0$. Therefore $q_j \not| Q$ for $j = 1, 2, \ldots, n$. Because all odd primes are either of the form $4k+1$ or of the form $4k+3$, and the product of primes of the form $4k+1$ is also of this form (because $(4k+1)(4m+1) = 4(4km+k+m)+1$), there must be a factor of $Q$ of the form $4k+3$ different from the primes we listed. This complete the proof.

**37.** We need to show that this function is one-to-one and onto. In other words, if we are given a positive integer $x$, we must show that there is exactly one positive rational number $m/n$ (written in lowest terms) such that $K(m/n) = x$. To do this, we factor $x$ into its prime factorization and then read off the $m$ and $n$ such that $K(m/n) = x$. The primes that occur to even powers are the primes that occur in the prime factorization of $m$, with the exponents being half the corresponding exponents in $x$; and the primes that occur to odd powers are the primes that occur in the prime factorization of $n$, with the exponents being half of one more than the exponents in $x$. Since this uniquely determines $m$ and $n$, there is one and only one fraction, in lowest terms, that maps to $x$ under $K$.