SECTION 3.5 Primes and Greatest Common Divisors

2. The numbers 19, 101, 107, and 113 are prime, as we can verify by trial division. The numbers $27 = 3^3$ and $93 = 3 \cdot 31$ are not prime.

4. We obtain the answers by trial division. The factorizations are $39 = 3 \cdot 13$, $81 = 3^4$, $101 = 101$ (prime), $143 = 11 \cdot 13$, $289 = 17^2$, and $899 = 29 \cdot 31$.

6. A 0 appears at the end of a number for every factor of 10 ($= 2 \cdot 5$) the number has. Now 100! certainly has more factors of 2 than it has factors of 5, so the number of factors of 10 it has is the same as the number of factors of 5. Each of the twenty numbers 5, 10, 15, ..., 100 contributes a factor of 5 to 100!, and in addition the four numbers 25, 50, 75, and 100 contribute one more factor of 5. Therefore there are 24 factors of 5 in 100!, so 100! ends in exactly 24 0's.

8. We follow the hint. There are n numbers in the sequence $(n+1)!+2$, $(n+1)!+3$, $(n+1)!+4$, ..., $(n+1)!+(n+1)$. The first of these is composite because it is divisible by 2; the second is composite because it is divisible by 3; the third is composite because it is divisible by 4; ...; the last is composite because it is divisible by $n+1$. This gives us the desired n consecutive composite integers.

10. We must find, by inspection with mental arithmetic, the greatest common divisors of the numbers from 1 to 11 with 12, and list those whose gcd is 1. These are 1, 5, 7, and 11. There are so few since 12 had many factors—in particular, both 2 and 3.

12. Since these numbers are small, the easiest approach is to find the prime factorization of each number and look for any common prime factors.

a) Since $21 = 3 \cdot 7$, $34 = 2 \cdot 17$, and $55 = 5 \cdot 11$, these are pairwise relatively prime.

b) Since $85 = 5 \cdot 17$, these are not pairwise relatively prime.

c) Since $25 = 5^2$, 41 is prime, $49 = 7^2$, and $64 = 2^6$, these are pairwise relatively prime.

d) Since 17, 19, and 23 are prime and $18 = 2 \cdot 3^2$, these are pairwise relatively prime.

14. a) Since $6 = 1 + 2 + 3$, and these three summands are the only proper divisors of 6, we conclude that 6 is perfect. Similarly $28 = 1 + 2 + 4 + 7 + 14$.

b) We need to find all the proper divisors of $2^{p-1}(2^p - 1)$. Certainly all the numbers $1, 2, 4, 8, \ldots, 2^{p-1}$ are proper divisors, and their sum is $2^p - 1$ (this is a geometric series). Also each of these divisors times $2^p - 1$ is also a divisor, and all but the last is proper. Again adding up this geometric series we find a sum of $(2^p - 1)(2^{p-1} - 1)$. There are no other other proper divisors. Therefore the sum of all the divisors is $(2^p - 1) + (2^p - 1)(2^{p-1} - 1) = (2^p - 1)(1 + 2^{p-1} - 1) = (2^p - 1)2^{p-1}$, which is our original number. Therefore this number is perfect.

16. We need to find a factor if there is one, or else check all possible prime divisors up to the square root of the given number to verify that there is no nontrivial divisor.

a) $2^7 - 1 = 127$. Division by 2, 3, 5, 7, and 11 shows that these are not factors. Since $\sqrt{127} < 13$, we are done; 127 is prime.

b) $2^9 - 1 = 511 = 7 \cdot 73$, so this number is not prime.

c) $2^{11} - 1 = 2047 = 23 \cdot 89$, so this number is not prime.

d) $2^{13} - 1 = 8191$. Division by 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, and 89 (phew!) shows that these are not factors. Since $\sqrt{8191} < 97$, we are done; 8191 is prime.

18. Certainly if n is prime, then all the integers from 1 to $n - 1$ are less than or equal to n and relatively prime to n, but no others are, so $\phi(n) = n - 1$. Conversely, suppose that n is not prime. If $n = 1$, then we have $\phi(1) = 1 \neq 1 - 1$. If $n > 1$, then $n = ab$ with $1 < a < n$ and $1 < b < n$. Note that neither a nor b is relatively prime to n. Therefore the number of positive integers less than or equal to n and relatively prime to n is at most $n - 3$ (since a, b, and n are not in this collection), so $\phi(n) \neq n - 1$.

20. We form the greatest common divisors by finding the minimum exponent for each prime factor.

a) $2^2 \cdot 3^3 \cdot 5^2$ **b)** $2 \cdot 3 \cdot 11$ **c)** 17 **d)** 1 **e)** 5 **f)** $2 \cdot 3 \cdot 5 \cdot 7$

22. We form the least common multiples by finding the maximum exponent for each prime factor.

a) $2^5 \cdot 3^3 \cdot 5^5$ **b)** $2^{11} \cdot 3^9 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17^{14}$ **c)** 17^{17} **d)** $2^2 \cdot 5^3 \cdot 7 \cdot 13$

e) undefined (0 is not a positive integer) **f)** $2 \cdot 3 \cdot 5 \cdot 7$

24. We have $1000 = 2^3 \cdot 5^3$ and $625 = 5^4$, so $\gcd(1000, 625) = 5^3 = 125$, and $\operatorname{lcm}(1000, 625) = 2^3 \cdot 5^4 = 5000$. As expected, $125 \cdot 5000 = 625000 = 1000 \cdot 625$.

26. By Exercise 27 we know that the product of the greatest common divisor and the least common multiple of two numbers is the product of the two numbers. Therefore the answer is $(2^7 \cdot 3^8 \cdot 5^2 \cdot 7^{11})/(2^3 \cdot 3^4 \cdot 5) = 2^4 \cdot 3^4 \cdot 5 \cdot 7^{11}$.

28. The number of (positive) factors that a positive integer n has can be determined from the prime factorization of n. If we write this prime factorization as $n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, then there are $(e_1+1)(e_2+1)\cdots(e_r+1)$ different factors. This follows from the ideas in Chapter 5. Specifically, in choosing a factor we can choose 0, 1, 2, ..., e_1 of the p_1 factors, a total of e_1+1 choices; for each of these there are e_2+1 choices as to how many p_2 factors to include, and so on. If we don't want to go through the analysis using the ideas given below, we could simply compute the number of factors for each n, starting at 1 (perhaps using a computer program), and thereby obtain the answers by "brute force."

a) If an integer is to have exactly three different factors (we assume "positive factors" is intended here), then n must be the square of a prime number; that is the only way to make $(e_1+1)(e_2+1)\cdots(e_r+1)=3$. The smallest prime number is 2. So the smallest positive integer with exactly three factors is $2^2=4$.

b) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=4$. We can do this with $r=1$ and $e_1=3$, or with $r=2$ and $e_1=e_2=1$. The smallest numbers obtainable in these ways are $2^3=8$ and $2\cdot 3=6$, respectively. So the smallest number with four factors is 6.

c) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=5$. We can do this only with $r=1$ and $e_1=4$, so the smallest such number is $2^4=16$.

d) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=6$. We can do this with $r=1$ and $e_1=5$, or with $r=2$ and $e_1=2$ and $e_2=1$. The smallest numbers obtainable in these ways are $2^5=32$ and $2^2\cdot 3=12$, respectively. So the smallest number with six factors is 12.

e) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=10$. We can do this with $r=1$ and $e_1=9$, or with $r=2$ and $e_1=4$ and $e_2=1$. The smallest numbers obtainable in these ways are $2^9=512$ and $2^4\cdot 3=48$, respectively. So the smallest number with ten factors is 48.

30. 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) All the entries are primes. In fact, the n^{th} term is the smallest prime number greater than or equal to n.

b) Here we see that the sequence jumps at the prime locations. We can state this succinctly by saying that the n^{th} term is the number of prime numbers not exceeding n.

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

d) This sequence is actually important in number theory. The n^{th} term is -1 if n is prime, 0 if n has a repeated prime factor (for example, $12=2^2\cdot 3$, so 2 is a repeated prime factor of 12 and therefore the twelfth term is 0), and 1 otherwise (if n is not prime but is square-free).

e) The n^{th} term is 0 if n has two or more distinct prime factors, and is 1 otherwise. In other words the n^{th} term is 1 if n is a power of a prime number.

f) The n^{th} term is the square of the n^{th} prime.

32. From $a \equiv b \pmod{m}$ we know that $b = a + sm$ for some integer s. Now if d is a common divisor of a and m, then it divides the right-hand side of this equation, so it also divides b. We can rewrite the equation as $a = b - sm$, and then by similar reasoning, we see that every common divisor of b and m is also a divisor of a. This shows that the set of common divisors of a and m is equal to the set of common divisors of b and m, so certainly $\gcd(a,m)=\gcd(b,m)$.

34. We compute the first several of these: $2+1=3$ (which is prime), $2\cdot 3+1=7$ (which is prime), $2\cdot 3\cdot 5+1=31$ (which is prime), $2\cdot 3\cdot 5\cdot 7+1=211$ (which is prime), $2\cdot 3\cdot 5\cdot 7\cdot 11+1=2311$ (which is prime). However, $2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13+1=30031=59\cdot 509$, so the conjecture is false. Notice, however, that the prime factors in this last case were necessarily different from the primes being multiplied.

36. Define the function f as suggested from the positive rational numbers to the positive integers. This is a one-to-one function, because if we are given the value of $f(p/q)$, we can immediately recover p and q uniquely by writing $f(p/q)$ in base eleven and noting what appears to the left of the one and only A in the expansion and what appears to the right (and interpret these as numerals in base ten). Thus we have a one-to-one correspondence between the set of positive rational numbers and an infinite subset of the natural numbers, which is countable; therefore the set of positive rational numbers is countable.