removed (the even multiples of 3 having been removed in the previous step). The smallest integer after 3 which has not yet been deleted is 5. It is not divisible by either 2 or 3—otherwise it would have been crossed out—hence it is also a prime. All proper multiples of 5 being composite numbers, we next remove 10, 15, 20, ... (some of these are, of course, already missing), while retaining 5 itself. The first surviving integer 7 is a prime, for it is not divisible by 2, 3, or 5, the only primes that preceed it. After eliminating the proper multiples of 7, the largest prime less than $\sqrt{100} = 10$, all composite integers in the sequence 2, 3, 4, ..., 100 have fallen through the sieve. The positive integers which remain, to wit, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, are all of the primes less than 100.

The table below represents the result of the completed sieve. The multiples of 2 are crossed out by \; the multiples of 3 are crossed out by /; the multiples of 5 are crossed out by —; the multiples of 7 are crossed out by $\sim$.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

By this point, an obvious question must have occurred to the reader. Is there a largest prime number, or do the primes go on forever? The answer is to be found in a remarkably simple proof given by Euclid in Book IX of his *Elements*. Euclid's argument is universally regarded as a model of mathematical elegance. Loosely speaking, it goes like this: Given any finite list of prime numbers, one can always find a prime not on the list; hence, the number of primes is infinite. The actual details appear below.

THEOREM 3-4 (Euclid). *There are an infinite number of primes.*

Proof: Euclid's proof is by contradiction. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$ be the primes in ascending order, and suppose that there is a last prime; call it p_n. Now consider the positive integer

$$P = p_1 p_2 \cdots p_n + 1.$$

Since $P > 1$, we may put Theorem 3-2 to work once again and conclude that P is divisible by some prime p. But $p_1, p_2, \ldots, p_n$ are the only prime numbers, so that p must be equal to one of $p_1, p_2, \ldots, p_n$. Combining the relation $p \mid p_1 p_2 \cdots p_n$ with $p \mid P$, we arrive at $p \mid P - p_1 p_2 \cdots p_n$ or, equivalently, $p \mid 1$. The only positive divisor of the integer 1 is 1 itself and, since $p > 1$, a contradiction arises. Thus no finite list of primes is complete, whence the number of primes is infinite.

It is interesting to note that in forming the integers

$$P_k = p_1 p_2 \cdots p_k + 1,$$

the first five, namely,

$$\begin{aligned} P_1 &= 2 + 1 = 3, \\ P_2 &= 2 \cdot 3 + 1 = 7, \\ P_3 &= 2 \cdot 3 \cdot 5 + 1 = 31, \\ P_4 &= 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211, \\ P_5 &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311, \end{aligned}$$

are all prime numbers. However,

$$P_6 = 59 \cdot 509, \quad P_7 = 19 \cdot 97 \cdot 277, \quad P_8 = 347 \cdot 27953$$

are not prime. A question to which the answer is not known is whether there exist infinitely many k for which P_k is a prime. For that matter, are there infinitely many composite P_k?

Euclid's theorem is too important for us to be content with a single proof. Here is a variation in the reasoning: Form the infinite sequence of positive integers

$$\begin{aligned} n_1 &= 2, \\ n_2 &= n_1 + 1, \\ n_3 &= n_1 n_2 + 1, \\ n_4 &= n_1 n_2 n_3 + 1, \\ &\vdots \\ n_k &= n_1 n_2 \cdots n_{k-1} + 1, \end{aligned}$$

Since each $n_k > 1$, each of these integers is divisible by a prime. But no two n_k can have the same prime divisor. To see this, let $d = \gcd(n_i, n_k)$ and suppose that $i < k$. Then d divides n_i, hence must divide $n_1 n_2 \cdots n_{k-1}$. Since $d \mid n_k$, Theorem 2-2 (7) tells us that $d \mid n_k - n_1 n_2 \cdots n_{k-1}$ or $d \mid 1$. The implication is that $d = 1$ and so the integers n_k $(k = 1, 2, \ldots)$ are pairwise relatively prime. The point which we wish to make is that there are as many distinct primes as there are integers n_k, namely, infinitely many of them.

Let p_n denote the nth of the prime numbers in their natural order. Euclid's proof shows that an estimate to the rate of increase of p_n is

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1 < p_n^n + 1.$$

For instance, when $n = 3$, the inequality states that

$$7 = p_4 < p_3^3 + 1 = 5^3 + 1 = 126.$$

One can see that this estimate is wildly extravagant. A sharper limitation to the size of p_n is given in

THEOREM 3-5. *If p_n is the nth prime number, then $p_n \leq 2^{2^{n-1}}$.*

Proof: Let us proceed by induction on n, the asserted inequality being clearly true when $n = 1$. As hypothesis of the induction, we assume that $n > 1$ and that the result holds for all integers up to n. Then

$$\begin{aligned} p_{n+1} &\leq p_1 p_2 \cdots p_n + 1 \\ &\leq 2 \cdot 2^2 \cdots 2^{2^{n-1}} + 1 = 2^{1+2+2^2+\cdots+2^{n-1}} + 1. \end{aligned}$$

Recalling the identity $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$, we obtain

$$p_{n+1} \leq 2^{2^n - 1} + 1.$$

But $1 \leq 2^{2^n - 1}$ for all n; whence

$$\begin{aligned} p_{n+1} &\leq 2^{2^n - 1} + 2^{2^n - 1} \\ &= 2 \cdot 2^{2^n - 1} = 2^{2^n}, \end{aligned}$$

completing the induction step, and the argument.

There is a corollary to Theorem 3-5 which is of interest.

COROLLARY. *For $n \geq 1$, there are at least $n+1$ primes less than 2^{2^n}.*

Proof: From the theorem, we know that $p_1, p_2, \ldots, p_{n+1}$ are all less than 2^{2^n}.

PROBLEMS 3.2

1. Determine whether the integer 701 is prime by testing all primes $p \leq \sqrt{701}$ as possible divisors. Do the same for the integer 1009.
2. Employing the Sieve of Eratosthenes, obtain all the primes between 100 and 200.
3. Given that $p \nmid n$ for all primes $p \leq \sqrt[3]{n}$, show that n is either a prime or the product of two primes. [*Hint:* Assume to the contrary that n contains at least three prime factors.]
4. Establish the following facts:
   (a) $\sqrt{p}$ is irrational for any prime p.
   (b) If $a > 0$ and $\sqrt[n]{a}$ is rational, then $\sqrt[n]{a}$ must be an integer.
   (c) For $n \geq 2$, $\sqrt[n]{n}$ is irrational. [*Hint:* Use the fact that $2^n > n$.]
5. Show that any composite three-digit number must have a prime factor less than or equal to 31.
6. Fill in any missing details in this sketch of a proof of the infinitude of primes: Assume that there are only finitely many primes, say $p_1, p_2, \ldots, p_n$. Let A be the product of any r of these primes and put $B = p_1 p_2 \cdots p_n / A$. Then each p_k divides either A or B, but not both. Since $A + B > 1$, $A + B$ has a prime divisor different from any of the p_k, a contradiction.
7. Modify Euclid's proof that there are infinitely many primes by assuming the existence of a largest prime p and using the integer $N = p! + 1$ to arrive at a contradiction.
8. Give another proof of the infinitude of primes by assuming that there are only finitely many primes, say $p_1, p_2, \ldots, p_n$, and using the integer

   $$N = p_2 p_3 \cdots p_n + p_1 p_3 \cdots p_n + \cdots + p_1 p_2 \cdots p_{n-1}$$

   to arrive at a contradiction.
9. Prove that if $n > 2$, then there exists a prime p satisfying $n < p < n!$. [*Hint:* If $n! - 1$ is not prime, then it has a prime divisor p; $p \leq n$ implies that $p \mid n!$ leading to a contradiction.]
10. If p_n denotes the nth prime number, show that none of the integers $P_n = p_1 p_2 \cdots p_n + 1$ is a perfect square. [*Hint:* Each P_n is of the form $4k + 3$.]