An algorithm to test whether an integer $n > 1$ is a prime

Step 1 Check whether n is 2. If n is 2, then n is a prime. If not go to step 2.

Step 2 Check whether 2 divides n. If 2 divides n, then n is not a prime. If 2 does not divide n, then go to step 3.

Step 3 Find all odd primes $p \leq \sqrt{n}$. If there is no such odd prime, then n is a prime. Otherwise go to step 4.

Step 4 Check whether p divides n, where p is a prime obtained in step 3. If p divides n, then n is not a prime. If p does not divide n for any prime p obtained in step 3, then n is a prime.

Example 1 check whether 119 is a prime or not.

Solution: 2 does not divide 119. Let us now find all odd primes p such that $p^2 \leq 119$. These primes are 3, 5, 7. Now 3 does not divides 119, 5 does not divide 119. But 7 divides 119. Hence 119 is not a prime.

Example 2 Check whether 131 is a prime or not

Solution: 2 does not divides 131. Now we find all odd primes p such that $p^2 \leq 131$. These primes are 3, 5, 7, 11. Now 131 is not divisible by 3, 5, 7 and 11. Hence 131 is a prime.

We now show how to find all primes less than or equal to a fixed positive integer $n > 1$. Let us take $n = 100$. First we find all primes p such that $p^2 \leq 100$. These primes are 2, 3, 5, 7. So, to find all primes less than or equal to 100 we need only to find those numbers which are not divisible by 2, 3, 5 and 7. For this we follow the following steps:

Step 1 Make a list of all integers from 2 to 100

Step 2 Cross out all multiples of 2 which are greater than 2 and less than or equal to 100.

Step 3 Cross out those integers remaining in the list that are multiple of 3, other than 3

Step 4 Cross out those integers remaining in the list that are multiple 5 other than 5

Step 5 Cross out those integers remaining in the list that are multiple of 7 other than 7.

All remaining integers in the list must be prime

The table below demonstrate the result of this process. The multiples of 2 are crossed out by /, the multiples of 3 are crossed out by —, the multiples of 5 are crossed out by X and the multiples of 7 are crossed out by \.

	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~~

The remaining integers are 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

These are the primes less than 100

The above process of finding all the primes less than a fixed positive integer is called the Sieve of Erastosthenes.

Exercises 1. Check whether these positive integers are prime or not:
(i) 137 (ii) 231 (iii) 323

2. Find all the prime numbers less than 124 by Sieve of Eratosthenes.

Fundamental Theorem of Arithmatic (Theorem 13): Every integer $n \geq 2$ can be expressed uniquely as a product of (one or more) primes, upto the order of the factors. More precisely, any integer $n \geq 2$ can be expressed as $n = p_1 p_2 \cdots p_r$ where $p_1, p_2, \ldots, p_r$ are primes. Moreover, if $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$ are two factorisations of n as product of primes, then $r = s$ and the q_i can be relabelled so that $p_i = q_i$ for all $i = 1, 2, \ldots, r$

Proof: Let $n > 1$ be an integer. We divide the proof into two parts - existence and uniqueness.

Let $P(n)$ be the statement: n can be expressed as a product of primes. We prove that for all integers $n \geq 2$, $P(n)$ is true. We use induction for this.

If $n = 2$ then $P(2)$ is true as $2 = 2$ and 2 is prime.

Assume that k is a positive integer, $k \geq 2$ and each of the integers $2, 3, \ldots, k-1, k$ can be expressed as a product of primes.

We now show that $P(k+1)$ is true, i.e., the integer $k+1$ can be expressed as a product of primes.

If $k+1$ is prime, then $P(k+1)$ is true as we can write $k+1 = k+1$. Suppose that $k+1$ is composite. Then there exist integers r and s such that $k+1 = r.s$ where $2 \leq r \leq k$ and $2 \leq s \leq k$. By our assumption both r and s can be expressed as product of primes. Let $r = a_1 a_2 \ldots a_k$ and $s = b_1 b_2 \ldots b_m$ where $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_m$ are primes.

So, we have $(k+1) : a_1 a_2 \cdots a_l b_1 b_2 \cdots b_m$ which is a product of primes.

So $P(n)$ is true for all $n \geq 2$. So n can be expressed as a product of primes for $n \geq 2$.

Now to show the uniqueness of the representation of n as a product of primes we assume that n can be expressed as a product of primes in two ways, say $n = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_r$ ... (1)

where p_i and q_j are primes, $i = 1, 2, \ldots, t$, $j = 1, 2, \ldots, r$ are such that

$$p_1 \leq p_2 \leq \cdots \leq p_t$$

and $q_1 \leq q_2 \leq \cdots \leq q_r$

Suppose $t < r$. Now p_1 divides n. Hence p_1 divides $q_1 q_2 \cdots q_r$. Then by corollary 1 of Page - 56, p_1 divides one of $q_1, q_2, \ldots, q_r$, say p_1 divides q_k. Since p_1 and q_k are primes, it follows that $p_1 = q_k$ But $q_k \geq q_1$. So, $p_1 \geq q_1$. Similarly, we can show that $q_1 \geq p_1$

Hence $p_1 = q_1$. We cancell the common factor from (1) and obtain

$$p_2 p_3 \cdots p_t = q_2 q_3 \cdots q_r \quad \ldots \quad (2)$$

We repeat the above process and obtain $p_2 = q_2$. Now Cancle this factor from (2) and write

$$p_3 p_4 \cdots p_t = q_3 q_4 \cdots q_r$$

Continuing this way, we obtain

$1 = q_{t+1} q_{t+2} \cdots q_r$ which is

not true since $q_i > 1$. Hence $t \nless r$. Similarly, we can show that $r \nless t$. So, we find that $t = r$ and $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r$. So, we conclude that n can be expressed as a product of primes uniquely.

Example: $24 = 2^3 \cdot 3$ $\quad 57 = 3 \cdot 19$, $\quad 100 = 2^2 \times 5^2$ etc.

Some more problems: 1. Determine whether 287 is a prime or not. Solution: First we find all primes p such that $p^2 \leq 287$. These primes are 2, 3, 5, 7, 11, 13. Now 7 divides 287. Hence 287 is not a prime

2. Find all prime divisors of 40! (factorial 40)

Solution: Since 40! is the product of all integers from 1 to 40, it follows that the prime divisors of 40! are those primes which are less than 40. Hence the prime divisors are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37.

3. If n is a positive integer such that n^3+1 is a prime then prove that $n=1$

Solution: Suppose n is a positive integer and n^3+1 is prime. Now $n^3+1 = (n+1)(n^2-n+1)$. Since n^3+1 is a prime, either $n+1=1$ or $n^2-n+1=0$. But $n+1 \neq 1$ Hence $n^2-n+1=1$. This implies $n(n-1)=0$. Since $n>0$, we find that $n-1=0$ or, $n=1$.

Exercises 1. Determine which of the following integers are prime? (a) 283 (b) 1901 (c) 2001

2. Find all prime numbers p such that $100 \leq p \leq 150$

3. If p is a prime integer such that $p = n^2-4$ for some integer n, then show that $p=5$.

4. Let k be a positive integer. Prove that the following integers $(k+1)!+2, (k+1)!+3, \cdots, (k+1)!+k, (k+1)!+(k+1)$ are k consecutive composite integers.

5. Find seven consecutive composite integers.