Integer Factorization

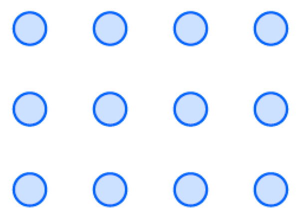
- **Reading:** Introduction
  10 min
- **Reading:** Prime Numbers
  10 min
- **Practice Quiz:** Puzzle: Arrange Apples
  2 questions
- **Reading:** Factoring: Existence
  10 min
- **Reading:** Factoring: Uniqueness
  10 min
- **Reading:** Unique Factoring: Consequences
  10 min
- **Quiz:** Integer Factorization
  6 questions

Chinese Remainder Theorem

Modular Exponentiation

Prime Numbers

You can easily arrange 12 apples in three rows and four columns:



This is possible because $3 \times 4 = 12$ or, in other words, because 12 can be represented as a product of two smaller numbers, 3 and 4. But the same idea does not work for 13 apples: either the table will consist of only one row or column, or some cells will be missing an apple.

Stop and think! Why? What happens for other numbers, say, $20, 21, 22$, or 23?

The difference is that $12, 20, 21$, and 22 are all *composite* numbers and can be represented as the product of two smaller numbers (sometimes in many different ways):

$12 = 2 \times 6 = 3 \times 4 = 4 \times 3 = 6 \times 2$

$20 = 2 \times 10 = 4 \times 5 = 5 \times 4 = 10 \times 2$

$21 = 3 \times 7 = 7 \times 3$

$22 = 2 \times 11 = 11 \times 2$

Note that we do not include "trivial" decompositions like $21 = 1 \times 21$ (a rectangle with one row or one column).

On the other hand, 23 does not have any "non-trivial" decompositions (only 1×23 and 23×1), meaning it is *prime*.

Definition

A *prime* number is a positive integer $p > 1$ that cannot be represented as the product of two smaller positive integers.

Stop and think! We previously defined the notion of a *divisor*. Using it, could you finish the statement: "A number $p > 1$ is prime if it does not have$\ldots$"?

A number $p > 1$ is prime if it does not have positive integer divisors except for 1 and p. Indeed, if $m = uv$ is composite where u and v are non-trivial divisors, then u and v are both smaller than m, making it impossible for either one to be equal to 1. And if a number $m > 1$ has some non-trivial divisor d, then for some positive integer q we must have $m = dq$ by the definition of a divisor, and neither d nor q can be equal to 1, so both must be smaller than m.

Stop and think! Is 1 a prime number?

It is tempting to guess that 1 is prime since it cannot be expressed as the product of smaller positive integers (there are no smaller positive integers to pick from!). Still, our definition explicitly requires $p > 1$ for a prime, so 1 is not considered a prime number (nor is it considered composite). But this is just a *decision* that most mathematicians agree with, not a theorem. (See, for example, this long stackexchange discussion.)

Problem

Show that a composite number m has a divisor d such that $1 < d \leq \sqrt{m}$.

Solution

For a decomposition $m = uv$, we know that both divisors are greater than 1 (if u or v were equal to 1, the other would have to be equal to m, but both are smaller). Now, suppose both u and v did exceed $\sqrt{m}$: then their product would exceed $\sqrt{m} \cdot \sqrt{m} = m$. Thus, at least one must be less than or equal to $\sqrt{m}$, satisfying the existence of d as described.

This problems shows that it is not necessary to check every possible number between 1 and m in search of a divisor if we want to check whether m is prime. It is enough to check the numbers that do not exceed $\sqrt{m}$: if there are no divisors among them, then m must be prime.

```python
# Finds the smallest divisor>1 of the given integer m>1
def min_divisor(m):
    for d in range(2, m + 1):
        if m % d == 0:
            return d
        # optimization:
        if d * d > m:
            return m

for i in range (2, 25):
    divisor = min_divisor(i)
    print(f'\nThe smallest divisor of {i} is {divisor}', end='')
    if divisor == i:
        print(f' (hence, {i} is prime)', end='')
```

Run

Reset

```
The smallest divisor of 2 is 2 (hence, 2 is prime)
The smallest divisor of 3 is 3 (hence, 3 is prime)
The smallest divisor of 4 is 2
The smallest divisor of 5 is 5 (hence, 5 is prime)
The smallest divisor of 6 is 2
The smallest divisor of 7 is 7 (hence, 7 is prime)
The smallest divisor of 8 is 2
The smallest divisor of 9 is 3
The smallest divisor of 10 is 2
The smallest divisor of 11 is 11 (hence, 11 is prime)
The smallest divisor of 12 is 2
The smallest divisor of 13 is 13 (hence, 13 is prime)
The smallest divisor of 14 is 2
The smallest divisor of 15 is 3
The smallest divisor of 16 is 2
The smallest divisor of 17 is 17 (hence, 17 is prime)
The smallest divisor of 18 is 2
The smallest divisor of 19 is 19 (hence, 19 is prime)
The smallest divisor of 20 is 2
The smallest divisor of 21 is 3
The smallest divisor of 22 is 2
The smallest divisor of 23 is 23 (hence, 23 is prime)
The smallest divisor of 24 is 2
```

The function `min_divisor(m)` is applied to an integer $\mathtt{m} > 1\}$ and returns the smallest divisor of `m` (not counting 1). It tests all $\mathtt{d} \in \{2, \ldots, \mathtt{m}\}$ (note that in python, `range(a,b)` includes `a`, but not `b`) until a divisor is found. It will return `m` if there are no other divisors, i.e. if `m` is prime. The last two lines of this function take advantage of the optimization mentioned above: if `d` is too large (exceeding $\sqrt{\mathtt{m}}$, which is true when `d*d>m`), then we know that `m` is prime and return `m` immediately.

```
The minimal divisor of 2 is 2 (hence, 2 is prime)
The minimal divisor of 3 is 3 (hence, 3 is prime)
The minimal divisor of 4 is 2
The minimal divisor of 5 is 5 (hence, 5 is prime)
The minimal divisor of 6 is 2
The minimal divisor of 7 is 7 (hence, 7 is prime)
The minimal divisor of 8 is 2
The minimal divisor of 9 is 3
The minimal divisor of 10 is 2
The minimal divisor of 11 is 11 (hence, 11 is prime)
The minimal divisor of 12 is 2
The minimal divisor of 13 is 13 (hence, 13 is prime)
The minimal divisor of 14 is 2
The minimal divisor of 15 is 3
The minimal divisor of 16 is 2
The minimal divisor of 17 is 17 (hence, 17 is prime)
The minimal divisor of 18 is 2
The minimal divisor of 19 is 19 (hence, 19 is prime)
The minimal divisor of 20 is 2
The minimal divisor of 21 is 3
The minimal divisor of 22 is 2
The minimal divisor of 23 is 23 (hence, 23 is prime)
The minimal divisor of 24 is 2
```

In the output you may easily recognize prime numbers (rows with two identical numbers).

The following example shows a function that returns an ordered list of the first n primes:

```python
# Finds the minimal divisor>1 of the given integer m>1
def min_divisor(m):
    for d in range(2, m + 1):
        if m % d == 0:
            return d
        # optimization:
        if d * d > m:
            return m


def is_prime(m):
    return m == min_divisor(m)


def primes_list(n):
    lst = []
    boundary = 2
    # primes < boundary are in lst
    while len(lst) < n:
        if is_prime(boundary):
            lst.append(boundary)
        boundary += 1

    return lst


print('The first ten primes:')
print(primes_list(10))
```

Run

Reset

```
The first ten primes:
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29]
```

We store in `lst` the list of all the primes smaller than `boundary`; initially `boundary` is 2 and `lst` is empty. Then, while `lst` is not yet long enough, we increase `boundary` by 1 after updating the list (appending the old value of `boundary` if it was prime).

```
The first ten primes:
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29]
```