Primes, Composites and Integer Division

Definition (prime): A positive integer \( n > 1 \) is prime if and only if \( n \) is divisible only by itself and 1.

Definition (composite): A positive integer \( n > 1 \) is composite if and only if \( n = p \times q \), where \( 1 < p < n \) and \( 1 < q < n \) are positive integers.

Definition (equivalent): A positive integer \( n > 1 \) is composite if and only if \( n \) is not prime.

Integer Division:
For every pair of positive integers \( n \) and \( d \), there exist unique positive integers \( q \) and \( r \) such that:

\[
n = q \times d + r , \quad \text{and} \quad 0 \leq r \leq (d-1) .
\]

Quotient (definition, notation): \( q \) is called the quotient and is denoted by \( n \div d \).

Remainder (definition, notation): \( r \) is called the remainder and is denoted by \( n \div d \).

Divisibility (definition, notation):
We say that an integer \( n \) is divisible by an integer \( d \neq 0 \), and write \( d \mid n \) (meaning \( d \) divides \( n \)), if and only if, for some integer \( q \), \( n = q \times d \).

We say that an integer \( n \) is not divisible by an integer \( d \neq 0 \), and write \( d \nmid n \) (meaning \( d \) does not divide \( n \)), if and only if, for integers \( q \) and \( r \), \( n = q \times d + r \), with \( 0 < r \leq (d-1) \).
**Theorem (Infinitude of Primes):** There are infinitely many prime numbers.

**Proof:** (by contradiction).

Assume, for the purposes of contradiction, that there are finitely many prime numbers, say \( p_1 < p_2 < \ldots < p_n \).
Thus \( p_n \) is the largest prime number, implying that all numbers \( m > p_n \) are composite.
We will construct a number \( m > p_n \) that is prime,
thus contradicting the fact that \( p_n \) is the largest prime number, and, consequently,
the assumption that there are finitely many prime numbers (with \( p_n \) being the largest).
We may thus infer that the assumption that there are finitely many prime numbers is false.
Consequently, there are infinitely many prime numbers.

Here is how we construct \( m \). We consider the product of all the \( p_n \) distinct prime numbers smaller than or equal to \( p_n \), and add 1 to this product:
\[ m = (1 \times 2 \times 3 \ldots \times p_n) + 1 , \]
which we can also write using the factorial notation as
\[ m = p_n! + 1 , \]
or, using the product notation \( \prod \) as
\[ m = \left( \prod_{i=1}^{p_n} i \right) + 1 . \]

We will now argue that \( m \) is a prime number.
In particular, following the definition, we will argue that \( m \) is not divisible by any number \( d \) in the range \( 1 < d \leq (m-1) \).
To see this, realize that every \( d \) in the range \( 1 < d \leq (m-1) \) is a factor in the product \( \prod_{i=1}^{p_n} i \).
We may thus write:
\[ m = \left( \prod_{i=1}^{p_n} i \right) \times \left( \prod_{i=d+1}^{p_n} i \right) + 1 = q \times d + 1 \]
for
\[ p = \left( \prod_{i=1}^{d-1} i \right) \times \left( \prod_{i=d+1}^{p_n} i \right) . \]

Thus, for every \( d \) in the range \( 1 < d \leq (m-1) \), if \( m \) is divided by \( d \) the remainder is 1.
Thus, there does not exist \( d \) in the range \( 1 < d \leq (m-1) \) that divides \( m \).
Thus, \( m \) is only divisible by 1 and \( m \), which means that \( m \) is prime.

This completes the proof of the theorem.
Theorem (Fundamental Theorem of Arithmetic, or Prime Number Decomposition):

Every integer $n > 1$ can be written as the product of prime numbers in a unique way, ie,

$$ n = p_1^{q_1} \times p_2^{q_2} \times \ldots \times p_k^{q_k} $$

or, using product notation,

$$ n = \prod_{i=1}^{k} p_i^{q_i} $$

where the $p_i$’s are prime numbers, the $q_i$’s are integers greater than 0, and the above decomposition of $n$ in terms of the $p_i$’s and $q_i$’s is unique.

**Remark.** We will give the proof of this theorem later in the course. But, hopefully, most have seen elementary algorithms to express large integers in terms of their prime factors. We outline some examples below, and follow up with an important comment concerning computational complexity of such factoring algorithms.

**Examples**

| 2352240 | 2 | 1294800 | 2 | 2852444400 | 2 | 9889245283 | 94427       |
| 1176120 | 2 | 647400  | 2 | 1426222000 | 2 | 104729     | 104729      |
| 588060  | 2 | 323700  | 2 | 713111100 | 2 | 99425925   | 5           |
| 294030  | 2 | 161850  | 2 | 356555550 | 2 | 59425925   | 5           |
| 147015  | 3 | 80925   | 3 | 178277775 | 3 | 59425925   | 5           |
| 49005   | 3 | 26975   | 5 | 59425925 | 5 | 11885185   | 5           |
| 16335   | 3 | 5395    | 5 | 11885185 | 5 | 11885185   | 5           |
| 5445    | 3 | 1079    | 13| 2377037  | 13| 59425925   | 5           |
| 1815    | 3 | 83      | 83| 182849   | 83| 11885185   | 5           |
| 605     | 5 | 1       |   | 2203     | 2203| 59425925   | 5           |
| 121     | 11| 1       |   | 1        |   | 59425925   | 5           |
| 11      | 11|         |   | 1        |   | 59425925   | 5           |
| 1       |   |         |   | 1        |   | 59425925   | 5           |
**Theorem.** If $n$ is a positive integer and $n$ is not prime, then $n$ has at least one factor smaller than or equal to $\sqrt{n}$.

**Proof:** (by contradiction).

Assume, for the purposes of contradiction, that $n$ is composite and all the prime factors of $n$ are strictly greater than $\sqrt{n}$. Then, for all integers $q > 1$ and $p > 1$ such that

$$n = q \times p ,$$

we have

$$q > \sqrt{n}$$

and

$$p > \sqrt{n} .$$

Therefore

$$n = q \times p > \sqrt{n} \times \sqrt{n} > n ,$$

implying

$$n > n ,$$

which is obviously false.

Therefore, the original assumption that $n$ is composite and all the prime factors of $n$ are strictly greater than $\sqrt{n}$ is false.

Therefore, if $n$ is composite, then $n$ has at least one factor smaller than or equal to $\sqrt{n}$.

This completes the proof of the theorem.

\[ \square \]