University of Toronto – MAT246H1-S – LEC0201/9201 – Winter 2021

Concepts in Abstract Mathematics

3 - Prime numbers

Jean-Baptiste Campesato

Informally, prime numbers are the integers greater than 1 which can't be factorized further. More precisely they are the natural numbers admitting exactly two positive divisors. Otherwise stated, a natural number $n \geq 2$ is a prime number if and only if its only positive divisors are 1 and n itself.

They play a crucial role in number theory since every natural number admit a unique expression as a product of prime numbers. They will also appear quite often later when we will study modular arithmetic.

All the results presented below were already known in *Euclid's Elements* (circa 300BC). Nonetheless, there are still many conjectures involving prime numbers which are easy to state but still open (some of them despite several centuries of attempts). For instance:

- *Goldbach conjecture (1742):* any even natural number greater than 2 may be written as a sum of two prime numbers (e.g. $4 = 2+2$, $6 = 3+3$, $8 = 5+3$, $10 = 5+5 = 7+3$...).
- *The twin prime conjecture (1849):* there are infinitely many prime numbers p such that $p+2$ is also prime (e.g. $(3,5)$, $(5,7)$, $(11,13)$...).
- *Legendre conjecture (1912):* given $n \in \mathbb{N} \setminus \{0\}$, we may always find a prime between n^2 and $(n+1)^2$.

1 Prime numbers

Definition 1. We say that a natural number p is a *prime number* if it has exactly two distinct positive divisors. A positive natural number with more than 2 positive divisors is said to be a *composite number*.

Remark 2.
- 0 is not a prime number since any natural number is a divisor of 0.
- 1 is not a prime number because it has only one positive divisor.

Hence a natural number p is prime if and only if $p \geq 2$ and the only positive divisors of p are 1 and p.

Example 3. The first prime numbers 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...

We face two natural questions:
1. How to check whether a natural number is a prime number?
2. How many prime numbers are there?

Proposition 4. *Let $n \in \mathbb{N}$. Then n is composite if and only if there exist $a, b \in \mathbb{N} \setminus \{0,1\}$ such that $n = ab$.*

Proof. Let $n \in \mathbb{N}$.
$\Rightarrow$ assume that n is a composite number, then it admits a divisor $k \in \mathbb{N}$ such that $k \neq 1$ and $k \neq n$.
So $n = km$ for some $m \in \mathbb{N}$. Note that $k, m \neq 0$ since otherwise $n = 0$. Note that $m \neq 1$ since otherwise $k = n$.
$\Leftarrow$ Assume that $n = ab$ for some $a, b \in \mathbb{N} \setminus \{0,1\}$.
Note that $a \neq n$, since otherwise $b = 1$ and that $n \neq 1$ since otherwise $a|1$, i.e. $a = 1$.
Therefore $1, a, n$ are three distinct positive divisors of n, so that n is a composite number. ∎

Proposition 5. *A composite number a admits a positive divisor b such that $1 < b^2 \leq a$.*

Proof. Write $a = b_1 b_2$ for some $b_1, b_2 \in \mathbb{N} \setminus \{0,1\}$. Then $b_1^2, b_2^2 > 1$.
Assume by contradiction that both $b_1^2 > a$ and $b_2^2 > a$. Then $a^2 = (b_1 b_2)^2 = b_1^2 b_2^2 > a^2$. Hence a contradiction. ∎

Example 6. We want to prove that 97 is a prime number.
Since $10^2 = 100 > 97$, it is enough to check that none of 2, 3, 4, 5, 6, 7, 8 and 9 are divisors of 97.
We will see later criteria to check divisibility.

Lemma 7. *A natural number $n \geq 2$ has at least one prime divisor.*

Proof. We are going to prove with a strong induction that every natural number $n \geq 2$ has a prime divisor.
Base case at $n = 2$: 2 admits a prime divisor (itself).
Induction step: assume that all the natural numbers $2, \dots, n$ admit a prime divisor for some $n \geq 2$.

- First case: $n+1$ is a prime number, then it has a prime divisor (itself).
- Second case: $n+1$ is a composite, then $n+1 = ab$ where $a, b \in \mathbb{N} \setminus \{0, 1\}$.
  Note that $a \neq n+1$ since otherwise $b = 1$.
  Since $2 \leq a \leq n$, a admits a prime divisor p by the induction hypothesis, i.e. $a = pk$ for some $k \in \mathbb{N}$.
  Then $n+1 = ab = pkb$. Thus the prime number p is a divisor of $n+1$.

Which proves the induction step. ■

Theorem 8. *There are infinitely many prime numbers.*

Proof. Assume by contradiction that there exist only finitely many prime numbers $p_1, p_2, \dots, p_n$.
We set $q = p_1 p_2 \cdots p_n + 1$. By Lemma 7, q has a prime divisor. Thus there exists $i \in \{1, 2, \dots, n\}$ such that $p_i | q$.
Then, since $p_i | p_1 p_2 \dots p_n$ and $p_i | q$, we have that $p_i | (q - p_1 p_2 \dots p_n)$, i.e. $p_i | 1$.
Therefore $p_i = 1$, which is a contradiction because 1 is not a prime number. ■

2 The fundamental theorem of arithmetic

Lemma 9 (Euclid's lemma)**.** *Let $a, b \in \mathbb{Z}$ and p be a prime number. If $p | ab$ then $p | a$ or $p | b$ (or both).*

Proof. Let $a, b \in \mathbb{Z}$ and p be a prime number such that $p | ab$.
Assume that $p \nmid a$ then $\gcd(a, p) = 1$ since the only positive divisors of p are 1 and itself.
Hence, by Gauss' lemma, $p | b$. ■

Theorem 10 (The fundamental theorem of arithmetic)**.** *Any integer greater than 1 can be written as a product of primes, moreover this expression as a product of primes is unique up to the order of the prime factors.*

Remark 11. The above theorem states two things: the **existence** of a prime factorization, and its **uniqueness**.

Proof.

- **Existence.** We are going to prove with a strong induction that $n \geq 2$ admits a prime factorization.
  Base case for $n = 2$: 2 is a prime number, so there is nothing to do.
  Induction step: assume that all the integers $2, 3, \dots, n$ have a prime factorization for some $n \geq 2$.
  We want to prove that $n+1$ admits a prime factorization.
  By Lemma 7, $n+1$ admits a prime factor, so $n+1 = pk$ where p is a prime number and $k \in \mathbb{N} \setminus \{0\}$.
  If $k = 1$ then there is nothing to do. So we may assume that $k \geq 2$.
  Since $1 < p$, we have that $k < pk = n+1$.
  Since $2 \leq k \leq n$, by the induction hypothesis, k admits a prime factorization $k = p_1 p_2 \dots p_l$.
  Finally $n+1 = p p_1 p_2 \dots p_l$, which proves the induction step.
- **Uniqueness (up to order).**
  Assume by contradiction that there exists an integer greater than 1 with (at least) two distinct prime factorizations. Denote by n the least such integer (which exists by the well-ordering principle).
  Let $n = p_1 p_2 \dots p_r$ and $n = q_1 q_2 \dots q_s$ be two distinct prime factorizations of n.
  Then $p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$.
  By Euclid's lemma p_1 divides one of the q_j.
  Up to reordering the indices, we may assume that $p_1 | q_1$.
  Since q_1 is a prime number, either $p_1 = 1$ or $p_1 = q_1$.
  And thus $p_1 = q_1$ since p_1 is also a prime number (and 1 is not).
  Therefore, by cancellation, $m = p_2 \dots p_r = q_2 \dots q_s$ is a number with two distinct prime factorizations.
  Note that $m > 1$ since otherwise $n = p_1 = q_1$ is not two distinct prime factorizations.
  And, since $1 < p_1$ we get that $m = p_2 \dots p_r < p_1 p_2 \dots p_r = n$.
  Which contradicts the fact that n is the least integer greater than 1 with two prime factorizations. ■

Corollary 12. *Any natural number* $n \in \mathbb{N} \setminus \{0\}$ *admits a unique expression* $n = \prod_{p \text{ prime}} p^{\alpha_p}$ *where* $\alpha_p \in \mathbb{N}$ *(i.e. the* α_p *are uniquely determined).*

Remarks 13.
- The above product is finite since all but finitely many exponents are equal to 0.
- 1 is the special case when $\alpha_p = 0$ for all prime numbers p.

Example 14. $60798375 = 3^2 \times 5^3 \times 11 \times 17^3$

Corollary 15. *Write* $a = \prod_{p \text{ prime}} p^{\alpha_p}$ *and* $b = \prod_{p \text{ prime}} p^{\beta_p}$ *with* $\alpha_p, \beta_p \in \mathbb{N}$ *all but finitely many equal to* 0*. Then*
- $a|b$ *if and only if for every prime number* p, $\alpha_p \leq \beta_p$.
- $\gcd(a,b) = \prod_{p \text{ prime}} p^{\min(\alpha_p, \beta_p)}$.

Example 16. $\gcd(3^2 \times 5^3 \times 11 \times 17^3, 3 \times 5^5 \times 17^2 \times 23) = 3 \times 5^3 \times 17^2$

Corollary 17. *Write* $n = \prod_{p \text{ prime}} p^{\alpha_p}$ *with* $\alpha_p \in \mathbb{N}$ *all but finitely many equal to* 0*. Then the positive divisors of* n *are exactly the numbers of the form* $n = \prod_{p \text{ prime}} p^{\gamma_p}$ *with* $0 \leq \gamma_p \leq \alpha_p$ *for all prime numbers* p*.*

Particularly, n *has* $\prod_{p \text{ prime}} (\alpha_p + 1)$ *positive divisors.*