Fundamental Theorem of Arithmetic for Part IA Discrete Mathematics

Note: This handout contains some basic exercises for the *Fundamental theorem of arithmetic* and the existence of an infinite number of prime numbers.

You can read more about the Fundamental Theorem of Arithmetic in Chapter 3.1 in "Elementary Number Theory" of D. M. Burton or Chapter 2 and 12 in "An introduction to the theory of numbers" by G. H. Hardy.

Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic basically says that every number has a unique factorisation. This means that we can perceive each number as a sort of vector (or bag) of prime factors.

Theorem 1. Every positive integer $n \geq 2$ can be uniquely written as the ordered product of primes.

Note: Ordered means that we consider $2 \cdot 3 \cdot 5$ the same as $5 \cdot 3 \cdot 2$.

In the lectures this is broken down into two parts *existence* and *uniqueness*.

Lemma 1. Every integer $n \geq 2$ either is a prime or can be written as a product of primes. (see slides 260-262)

Lemma 2. For every integer $n \geq 2$, there is a unique finite ordered sequence of primes $p_1 \leq \ldots \leq p_\ell$ with $\ell \in \mathbb{N}$ such that $n = \prod(p_1, \ldots, p_\ell)$. (see slides 264-269)

Combine the two Lemmas above to state the Fundamental Theorem of Arithmetic.

Example 1. The following numbers can be factorised as:

- $60 = 2^2 \cdot 3 \cdot 5$
- $1032 = 2^3 \cdot 2 \cdot 43$
- $25200 = 3^2 \cdot 2^4 \cdot 5^2 \cdot 7$

Exercise 1. Find the prime factorisation of 22!.

(optional) Uniqueness of factorisation is not obvious

As discussed in the supervisions, if we consider the set of even integers, i.e. $S = \{2, 4, 6, 8, \ldots\}$, then the set is closed under addition and multiplication, meaning that for $a, b \in S$, $a + b \in S$ and $a \cdot b \in S$ (*why?*).

We call an *even-composite* an even number that can be written as the product of two even numbers, otherwise we call it *even-composite*. For example, 10 is even-prime since it cannot be written as the product of two even numbers, but $20 = 2 \cdot 10$ is even-composite.

Does there exist an even number that has two even-prime factorisations? For example, 20 has a unique. (see answer at the end of the document)

Basic properties

Property 1. For naturals a and b, such that $a = p_1^{a_1} \cdot \ldots p_k^{a_k}$ and $b = p_1^{b_1} \cdot \ldots \cdot p_k^{b_k}$, $a \mid b$ iff $a_i \leq b_i$ for every i.

Property 2. For naturals a and b, such that $a = p_1^{a_1} \cdot \ldots p_k^{a_k}$ and $b = p_1^{b_1} \cdot \ldots \cdot p_k^{b_k}$, $\gcd(a, b)$ is given by $p_1^{\min(a_1, b_1)} \cdot \ldots \cdot p_k^{\min(a_k, b_k)}$.

Property 3. For $a = p_1^{a_1} \cdot \ldots p_k^{a_k}$ and $b = p_1^{b_1} \cdot \ldots \cdot p_k^{b_k}$ the *lowest common multiple* $\mathrm{lcm}(a, b)$ is given by $p_1^{\max(a_1, b_1)} \cdot \ldots \cdot p_k^{\max(a_k, b_k)}$.

Exercise 2. (*a*) Find the unique prime factorisation of 5577 and 99099. (*Hint:* Use the divisibility criteria).

(*b*) Compute $\gcd(5577, 99099)$ and $\operatorname{lcm}(5577, 99099)$, expressing each of your answers as a product of prime numbers.

Property 4. Prove that $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$.

Proof.

$$\begin{aligned}\gcd(a,b) \cdot \operatorname{lcm}(a,b) &= p_1^{\max(a_1,b_1)} \cdot \ldots \cdot p_k^{\max(a_k,b_k)} \cdot p_1^{\min(a_1,b_1)} \cdot \ldots \cdot p_k^{\min(a_k,b_k)} \\ &= p_1^{\min(a_1,b_1)+\max(a_1,b_1)} \cdot \ldots \cdot p_k^{\min(a_k,b_k)+\max(a_k,b_k)} \\ &= p_1^{a_1+b_1} \cdot \ldots \cdot p_k^{a_k+b_k}\end{aligned}$$

□

Property 5. The number of divisors of $N = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ is given by $(a_1+1) \cdot \ldots \cdot (a_k+1)$.

*Proof.*By Property 1, all divisors will have the form $p_1^{b_1} \cdot \ldots \cdot p_k^{b_k}$ for $b_i \leq a_i$ and different assignments of b_i will give a different divisor. Hence, for the i-th factor we could set b_i to $0, 1, \ldots, a_i$, so $a_i + 1$ values. Since each b_i is chosen independently, there are $(a_1+1) \cdot (a_2+1) \cdot \ldots \cdot (a_k+1)$ possible assignments and hence divisors. □

Example 2. Count the divisors of 60.

Proof. We find the prime factorisation of 60 to be $2^2 \cdot 3^1 \cdot 5^1$. Hence, using the above formula the total number of divisors is $(2+1)(1+1)(1+1) = 12$.

The divisors of 60 are $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$, which confirms the count. □

Examples

Example 3. Let p be a prime and $p \mid a^n$ for naturals a and $n \geq 1$. Show that $p^n \mid a^n$.

Proof. Let $a = p_1^{a_1} p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$, then

$$a^n = p_1^{na_1} p_2^{na_2} \cdot \ldots \cdot p_k^{na_k}.$$

Since $p \mid a^n$, $p = p_i$ for some i. Hence, a^n has as a factor p^{na_i} where $a_i \geq 1$. Hence, $p^n \mid a^n$. □

Example 4. Find all primes p such that $7p + 1 = n^2$ for natural $n \geq 1$.

Proof. We start by factorising,

$$7p = n^2 - 1 = (n-1)(n+1)$$

Since 7 and p are primes, there are the following cases:

- $n - 1 = 7$ and $n + 1 = p$, so $n = 8$ and $p = 9$ (impossible since 9 not prime)
- $n - 1 = 7p$ and $n + 1 = 1$ (impossible since $n + 1 > n - 1$)
- $n - 1 = p$ and $n + 1 = 7$, so $n = 6$ and $p = 5$.
- $n - 1 = 1$ and $n + 1 = 7p$ (impossible since $p \geq 2$ which would imply that $n + 1 > 7(n - 1)$).

□

Exercise 3. Find all primes p and q with $p \neq q$, such that $(2p + 3q - 11)(p + q - 1) = 4$.

Exercise 4. Prove that there is exactly one natural number n for with $2^8 + 2^{11} + 2^n$ is a perfect square. (*Hint:* $2^8 + 2^{11}$ is a square)

Example 5. Show that $\log_{10}(7)$ is irrational.

*Proof.*Assume that it is rational, so $p/q = \log_{10}(7)$, then $10^{p/q} = 7$ and so $10^p = 7^q$. This means that $2^p 5^p = 7^q$. This will only be possible if $p = q = 0$, which cannot be the case. □

Exercise 5. Show that $\log(3)/\log(2)$ is irrational.

Example 6. Find the smallest positive integer such that $n/2$ is a square (of a natural) and $n/3$ is a cube (of a natural).

*Proof.*Assume that $n/2 = k^2 \Rightarrow n = 2k^2$ and $n/3 = m^3 \Rightarrow 3 \cdot m^3$. Since, we are searching for the smaller such number, we don't have to assume that n has any divisors other than 2 and 3. We have to pick natural x and y such that $n = 2^x 3^y$ satisfies the above two conditions.

$n = 2^x 3^y = 2k^2 \Rightarrow 2^{x-1} 3^y = k^2$ so $2 \mid (x-1)$ and $2 \mid y$. Similarly, $3 \mid x$ and $3 \mid (y-1)$. This is essentially a system of modulo equations, but we can also just check $x, y = 0, 1, 2, 3, \ldots$ and see that $x = 3$ and $y = 4$ are the smallest solutions, giving $n = 648$. □

Exercise 6. Prove that in any set of 33 distinct integers with prime factors amongst $\{5, 7, 11, 13, 23\}$, there must be two whose product is a square. (*Hint:* Use the pigeonhole principle)

Exercise 7. Prove that

$$\frac{\operatorname{lcm}(a,b,c)^2}{\operatorname{lcm}(a,b)\operatorname{lcm}(b,c)\operatorname{lcm}(c,a)} = \frac{\gcd(a,b,c)^2}{\gcd(a,b)\gcd(b,c)\gcd(c,a)}$$

Exercise 8. Show that if n is composite, then $n \mid (n-1)!$.

Exercise 9. Prove some of the gcd properties using the Fundamental Theorem of Arithmetic.

Infinitely many primes

The existence of an infinite number of primes is a useful thing on its own, as it tells us that we can find primes to use e.g. in cryptographic applications. An even more important thing is how many primes there are below a given number x.

Theorem 2. There is an infinite number of prime numbers.

*Proof.***(Euclid's proof)** Assume there is a finite number of prime numbers and let $p_1, \ldots, p_k$ be these primes. Then, consider $P = p_1 \cdot \ldots p_k + 1$. We will show that P has not prime factors. Assume not and let $p_i \mid P$, then $p_i \mid p_1 \cdot \ldots p_k$ and also divides the difference $p_i \mid (P - p_1 \cdot \ldots p_k)$ so $p_i \mid 1$. This means that $p_i = 1$.

(Alternative proofs) There exists a proof that does not make use of Euclid's theorem. You can find this on wikipedia. □

Example 7. (*a*) Show that the product of two numbers of the form $4k+1$ is also of the same form.

(*b*) Show that there are infinitely many primes of the form $4k+3$.

Proof.(a) OK. (b) Assume not and consider the primes of the form $4k+3$ to be $p_1, \ldots, p_n$ and consider $N = 4(p_1 \ldots p_n) - 1$. Then N cannot have all prime factors of the form $4k+1$, as by part (a) this would imply that N is also of that form. So, there is a prime $p = 4\ell + 3$ such that $p \mid N$. However, $p \mid N$ and $p \mid 4(p_1 \ldots p_n$ so $p \mid -1$ (contradiction). So, there must be infinite primes of this form. □

Exercise 10. Show that there are infinite primes of the form $6k+5$.

Example 8. For every natural n, there exist n consecutive natural numbers.

*Proof.*We are searching for a natural K such that if we add $1, 2, \ldots, n$, then we get composite numbers. One idea is to try to find K with the property that $i \mid K + i$ for every i. This means that $i \mid K$ for every i. One such number is $K = (n+1)!$. Then for every i, $i \mid K$, so $i \mid K + i$. □

Past papers

COMPUTER SCIENCE TRIPOS Part IA – 2003 – Paper 1

7 Discrete Mathematics (MPF)

(*a*) Prove that there are infinitely many prime numbers. [4 marks]

(*b*) Let $p_1, p_2, \ldots, p_k$ be the first k primes. Show that the number of positive integers less than n and having no prime factors other than $p_1, p_2, \ldots, p_k$ is less than $\sqrt{n}2^k$. [8 marks]

[Hint: All such numbers are of the form $m^2\, p_1^{\varepsilon_1}\, p_2^{\varepsilon_2} \cdots p_k^{\varepsilon_k}$ where each ε_i is 0 or 1.]

Deduce that the k^{th} prime is less than 4^k. [4 marks]

COMPUTER SCIENCE TRIPOS Part IA – 2001 – Paper 1

2 Discrete Mathematics (MPF)

(*a*) Prove the fundamental theorem of arithmetic, that any natural number can be expressed as a product of powers of primes and that such an expression is unique up to the order of the primes. [4 marks]

(*b*) Given a natural number n, let $d(n)$ be the number of divisors of n (including 1 and n).

If $p_1, p_2, \ldots, p_k$ are distinct primes, prove that

$$d({p_1}^{\alpha_1} {p_2}^{\alpha_2} \ldots {p_k}^{\alpha_k}) = \prod_{i=1}^{k} (\alpha_i + 1).$$ [3 marks]

(c) What is the smallest number with 36 factors? [3 marks]

Answer to the even factorisation: The special property of the set S is that for $x = 60$, we can write it as $6 \cdot 10$ or $2 \cdot 30$ and notice that $2, 6, 10, 30$ are even-primes.