Proofs of the fundamental theorem of arithmetic

Tomohiro Yamada

Abstract

In this document, I would like to give several proofs of the fundamental theorem of arithmetic, i.e., the uniqueness of prime factorization of an integer.

0 Introduction

The fundamental theorem of arithmetic states that any positive integer is a product of prime numbers in a unique way, apart from rearrangement of primes. In other words, any positive integers n can be uniquely written in the form $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where $e_1, e_2, \ldots, e_k$ are positive integers and $p_1 < p_2 < \cdots < p_k$ are primes numbers (for $n = 1$, we let $k = 0$).

In this document, I would like to give several proofs of this theorem. But, these proofs give no information for prime factorization of an integer. Indeed, it is unlikely that there exists a polynomial-time algorithm of prime factorization. But no one has proved non-existence of polynomial-time algorithm of prime factorization, which would imply P $\neq$ NP since prime factorization is a NP-problem.

The existence of a prime factorization of an integer can be easily proved by induction; assuming that any integer up from 2 to n can be factorized into a product of primes, $n + 1$ is itself prime or can be factorized into a product of two integers ab with $2 \leq a, b \leq n$, both of which can be factorized into a product of primes by the inductive assumption.

So that the interest lies on proofs of the uniqueness.

We begin by introducing the notation: $\gcd(a, b)$ denotes the greatest common divisor of a and b, $\mathrm{LCM}[a, b]$ denotes the least common multiple of a and b, $a \mid b$ denotes that a divides b.

1 Euclid's lemma

A standard proof of the fundamental theorem of arithmetic uses Euclid's lemma, which is Proposition 30 of Euclid's *Element*, Book 7 (for detail, see the last section of this document).

Lemma 1.1 (Euclid's lemma). *Let a, b be two integers. If a prime p divides ab, then p divides a or b.*

Euclid's lemma gives the fundamental theorem of arithmetic.

We begin by noting that Euclid's lemma can be extended into the fact that if p divides a product of k numbers $a_1a_2 \dots a_k$, then p divides at least one of a_i's. Indeed, p divides a product of k numbers $a_1a_2 \dots a_k$, then p divides $a_1a_2 \dots a_{k-1}$ or a_k by Euclid's lemma. In the former case, we apply Euclid's lemma again and see that p divides $a_1a_2 \dots a_{k-2}$ or a_{k-1}. Iterating this argument, we see that p divides $a_1, a_2, \dots, a_{k-1}$ or a_k.

In particular, if p divides a product of primes $q_1q_2 \dots q_k$, then p must be equal to at least one of q_i's.

Now, let n be the smallest positive integer which can be factorized into primes more than one way and p be the smallest primes appearing in a factorization of n. We see that p cannot appear in another factorization since, otherwise, $n/p < n$ must have more than one way of prime factorization. But this contradicts to the above-mentioned fact (revised in Jun. 4. 2019). This proves the uniqueness of prime factorization.

(Added in Jun. 4. 2019) We note that Euclid's lemma easily yields its dual result: If a, b are relatively prime integers dividing n, the the product ab also divides n. Since a divides n, we can write $n = am$ with m an integer. Then, since b is an integer relatively prime to a dividing $n = am$, Euclid's lemma yields that b divides m. Writing $m = lb$, we have $n = am = abl$. Thus, ab divides n.

2 Bezout's identity

There exists several proofs of Euclid's lemma. A standard one is to use Bezout's identity, which is used in [1].

Lemma 2.1 (Bezout's identity). *For any integers m, n, there exist two integers a, b such that $am + bn = \gcd(m, n)$.*

We begin by showing the following lemma, which is [1, Theorem 23].

Lemma 2.2. *Let l be the smallest positive integer of the form $am+bn$ with a, b integers. Then any integer of the form $am + bn$ with a, b integers is a multiple of l.*

Proof. Let $k = cm+dn$ with c, d integers and divide k by l with the quotient q and the remainder r, i.e., $k = ql + r$ with $0 \leq r < l$. Now, writing $l = a_0m + b_0n$ with a_0, b_0 integers, we have $r = k - ql = (cm + dn) - q(a_0m + b_0n) = (c - qa_0)m + (d - qb_0)n$ and therefore r has also the form $am + bn$ with a, b integers. But, since $0 \leq r < l$, the only possibility is that $r = 0$. Hence $k = ql$ is a multiple of l. □

Now we can see that $l = \gcd(m, n)$ (Theorem 24 of [1]), observing that l is a common divisor of $m = 1 \times m + 0 \times n$ and $n = 0 \times m + 1 \times n$ but $l = am + bn$ must be a multiple of $\gcd(m, n)$ since both m and n are multiples of $\gcd(m, n)$. Hence Bezout's identity follows.

We shall prove the following generalization of Euclid's lemma.

Lemma 2.3. *Let m, n be two integers. If $n \mid km$, then k is a multiple of $n/\gcd(m, n)$.*

Proof. By Bezout's identity there exists some integers a, b such that $am + bn = \gcd(m, n)$ and therefore $k\gcd(m, n) = akm + bkn$. Since $n \mid km$, $k\gcd(m, n) = a(km) + bkn$ is a multiple of n and therefore k is a multiple of $n/\gcd(m, n)$. □

In particular, if p is a prime and a is not divisible by p, then $\gcd(a, p) = 1$ and therefore, if $p \mid ab$, then $p = p/\gcd(a, p) \mid b$, which proves Euclid's lemma.

The proof of Euclid's lemma via Bezout's identity is a special case of a series of theorems concerning the uniqueness of prime factorization in general integral domains: any Euclidean domain is a Noetherian Bezout domain, any Bezout domain is a gcd domain, any gcd domain is a Schreier domain and any atomic (any Noetherian domain is atomic) Screier domain is a UFD.

3 Bezout's identity via Euclidean algorithm

Another proof of Bezout's identity uses Euclidean algorithm which is used to calculate $\gcd(m, n)$ for given positive integers m, n; let $a_0 = m, a_1 = n$ and define new a_n recursively by dividing a_{n-2} by a_{n-1} with the quotient q_{n-1} and the remainder a_n. a_n to be the remainder of a_{n-2} divided by a_{n-1} recursively until we have an index l with $a_l = 0$. Then we have $a_{l-1} = \gcd(m, n)$. We see that $a_2 = m - q_1 n, a_3 = n - q_2 a_2, \ldots, a_{l-2} = a_{l-4} - q_{l-3} a_{l-3}$ and $\gcd(m, n) = a_{l-1} = a_{l-3} - q_{l-2} a_{l-2}$ can be represented in the form $am + bn$ with a, b integers.

4 LCM-gcd theory

Some proofs of Euclid's lemma use theory of least common multiples and greatest common divisors. The following lemma is [5, Theorem 1.3] and [4, Theorem 1.4.1].

Lemma 4.1. *Any common multiple of a and b is a multiple of* $\mathrm{LCM}(a, b)$.

Proof. Let n be an arbitrary common multiple of a and b and divide n by $\mathrm{LCM}(a, b)$ with the quotient q and the remainder r, i.e., $n = q\,\mathrm{LCM}(a, b) + r$ with $0 \le r < \mathrm{LCM}(a, b)$. Now $r = n - q\,\mathrm{LCM}(a, b)$ is also a common multiple of a and b. But since $0 \le r < \mathrm{LCM}(a, b)$, the only possibility is that $r = 0$, i.e., n is a multiple of $\mathrm{LCM}(a, b)$. □

This lemma has the following dual, which means that the ordinary gcd satisfies the definition of the gcd in general commutative rings (In a commutative ring R, a gcd of $a, b \in R$ is defined to be a common divisor of a, b which is divisible by any other common divisor of a, b), i.e. the ring of (rational) integers are gcd domain.

Lemma 4.2. *Any common divisor of a and b divides* $\gcd(a, b)$.

Proof. Let n be a common divisor of a and b and $l = \mathrm{LCM}[n, \gcd(a, b)]$. Since both of n and $\gcd(a, b)$ divide both a and b, a and b are common multiples of n and $\gcd(a, b)$. Now the previous lemma gives that both of a and b are multiples of $l = \mathrm{LCM}[n, \gcd(a, b)]$. Hence l is a common divisor of a and b. We see that $\gcd(a, b) \le l \le \gcd(a, b)$ and therefore $l = \gcd(a, b)$, which is a multiple of n and therefore n divides $\gcd(a, b)$. □

The following lemma is used in [5].

Lemma 4.3. *Let m, n are positive integers. If $L = \mathrm{LCM}[m, n]$ and $d = \gcd(m, n)$, then we have $mn = dL$.*

Proof. Since $mn/d = m(n/d) = n(m/d)$ is a common multiple of m and n, Lemma 4.1 gives that mn/d is a multiple of L, i.e., $dL \mid mn$. On the other hand, since $mn/L = m/(L/n) = n/(L/m)$ is a common divisor of m and n, Lemma 4.2 gives that mn/L divides d, i.e., $mn \mid dL$.

Now we have $mn \mid dL \mid mn$ and therefore $mn = dL$. □

Indeed, for the proof of Euclid's lemma, it suffices to prove the following lemma.

Lemma 4.4. *For a prime p and a positive integer a not divisible by p, we have $\mathrm{LCM}[a, p] = ap$.*

Proof. Since a divides $\mathrm{LCM}[a, p]$ and, by Lemma 4.1, $\mathrm{LCM}[a, p]$ divides ap, we have $\mathrm{LCM}[a, p] = a$ or $\mathrm{LCM}[a, p] = ap$. But, since a is not a multiple of p, we must have $\mathrm{LCM}[a, p] = ap$. □

Now Euclid's lemma can be proved. If p divides ab but not a, then the above lemma gives that $\mathrm{LCM}[a, p] = ap$. Since ab is a common multiple of a and p, Lemma 4.1 gives ab is a multiple of $\mathrm{LCM}[a, p] = ap$, i.e., b is a multiple of p as stated in Euclid's lemma.

[4, Theorem 1.4.3] has a similar but slightly different use of greatest common divisors.

Lemma 4.5. *If a divides bc and $\gcd(a, b) = 1$, then a divides c.*

Proof. Since a divides bc, we have $a = \gcd(a, bc)$. Since $\gcd(a, b) = 1$, we have $c = \gcd(a, b)c$ and therefore $\gcd(a, c) = \gcd(a, \gcd(a, b)c)$. Now, if we can show $\gcd(a, bc) = \gcd(a, \gcd(a, b)c)$, then we have $a = \gcd(a, bc) = \gcd(a, \gcd(a, b)c) = \gcd(a, c)$ and therefore $a \mid c$ as desired.

Henceforth we shall show that $\gcd(a, bc) = \gcd(a, \gcd(a, b)c)$.

If l is a common divisor of a and $\gcd(a, b)c$, then $l \mid \gcd(a, b)c \mid bc$ and therefore l is a common divisor of a and bc. So that $\gcd(a, \gcd(a, b)c) \leq \gcd(a, bc)$.

Let $d = \gcd(a, bc)$. Now $d \mid a \mid ac$ and therefore d is a common divisor of ac and bc. Since ac and bc are a common multiple of c and d, we have $\mathrm{LCM}[c, d]$, as well as c and d, is a common divisor of ac and bc. Denoting

$\mathrm{LCM}[c,d] = ck$, we have k is a common dividor of a and b and therefore $k \mid \gcd(a,b)$ by Lemma 4.2. So that $\mathrm{LCM}[c,d] = ck$ divides $\gcd(a,b)c$ and therefore d is also a divisor of $\gcd(a,b)c$. Hence d is a common divisor of a and $\gcd(a,b)c$. But, since $d \geq \gcd(a, \gcd(a,b)c)$ as shown above, we have $d = \gcd(a, \gcd(a,b)c)$. □

5 Another proof of Euclid's lemma

Another simple proof of Euclid's lemma is given in [2].

Lemma 5.1. *Let a, b be two integers and k_0 be the smallest positive integer such that $k_0 a$ is a multiple of b. If ka is a multiple of b, then k is a multiple of k_0.*

Proof. We shall divide k by k_0 with the quotient q and the remainder r, i.e., Then $ra = (k - qk_0)a = ka - qk_0 a$ is also a multiple of b. But since $0 \leq r < k_0$, the only possibility is that $r = 0$, i.e., k is a multiple of k_0. □

Now we have another proof of Lemma 2.3, which gives Euclid's lemma.

Lemma 5.2. $k_0 = b / \gcd(a,b)$.

Proof. We begin by noting that we can always take $k = b$ in the situation given in the previous lemma; ba is clearly a multiple of b. So that k_0 divides b.

Now let $b = d_0 k_0$ and $k_0 a = n_0 b$. Then we have $a = n_0 d_0$ and threfore d_0 is a common divisor of a and b. For any common divisor d of a and b, $(b/d)a = ab/d = a(b/d)$ is a multiple of a and therefore b/d is a multiple of k_0, i.e., d divides $b/k_0 = d_0$. So that $d = \gcd(a,b)$ and $k_0 = b/\gcd(a,b)$. □

(Added in Jun. 4. 2019) Now we proved Euclid's lemma without Bezout's identity. We note that we can also derive Bezout's identity from Lemma 5.2.

Let $u_k (k = 0, 1, \ldots)$ be the remainder when ka is divided by b. We observe that $u_k (0 \leq k \leq k_0 - 1)$ take different values. Indeed, if $u_k = u_l (0 \leq k \leq l \leq k_0 - 1)$, $(l - k)a$ is a multiple of b and $k - l$ must be a multiple of b by Lemma 5.2 but, since $0 \leq l - k \leq k_0 - 1$, we must have $k = l$.

Now $u_k(0 \leq k \leq k_0 - 1)$ take k_0 different values. But, $u_k(0 \leq k \leq k_0 - 1)$ must take one of the $k_0 = b/\gcd(a,b)$ values $0, \gcd(a,b), \ldots, (k_0-1)\gcd(a,b)$ since $ka - lb$ must be a multiple of $\gcd(a,b)$. This means that $u_k(0 \leq k \leq k_0 - 1)$ take each of these k_0 values exactly once. In particular, there exists an index k such that $u_k = \gcd(a,b)$. In other words, there exist integers k, l such that $ka - lb = \gcd(a,b)$. This proves Bezout's identity.

6 A direct proof

A direct proof of the fundamental theorem of arithmetic is given in Section 2.11 of [1]. Let n be the smallest positive integer which can be factorized into primes more than one way. Let p be the smallest primes appearing in a factorization of n and q be the smallest primes appearing in another factorization of n. We see that p cannot appear in the second factorization since, otherwise, $n/p < n$ must have more than one way of prime factorization. In particular, $p \neq q$.

Since a prime clearly has only one way of prime factorization, n must be composite. So that $p^2 \leq n$ and $q^2 \leq n$. Since $p \neq q$, we have $pq < n$.

Let $N = n - pq$. Then we have $0 < N < n$ and therefore N has a unique factorization. Since both of p and q divides $N = n - pq$, both primes appear the factorization of N. So that N must be divisible by pq and so must $n = N + pq$. Thus n/q must be disibile by p. But, since $n/q < n$ has a unique factorization, p must appear in the prime factorization of n/q. Hence p must also appear in the second factorization of n, contrary to the above-mentioned fact that p cannot appear in the second factorization.

Thus there never exists smallest positive integer which can be factorized into primes more than one way, proving the uniqueness of prime factorization of integers.

7 Euclid's proof

It is known that Euclid does not use his algorithms to prove Euclid's lemma, by which Book 7 begins and Euclid's proof of his lemma in Book 7 has a serious gap. But the matter is not so simple. We would like to recommend to read [3] for detail. Euclid's proof needs the propositions 7.19 and 7.20: Proposition 7.19 states that $a : b = c : d$ if and only if $ad = bc$. Proposition 7.20 states that if (a, b) is the smallest positive integral pair with the ratio

$a : b$ and $a : b = c : d$, then $c = an$ and $d = an$ for some integer n.

Euclid proves Proposition 7.20 by taking $a = c(m/n), b = d(m/n)$ with m, n integers, $m \geq 2$ and $n \mid c$, and stating that $(a/m) : (b/m) = (c/n) : (d/n) = c : d$, which contradicts that (a, b) is the smallest pair with this ratio.

It seems to be easily pointed that n is not confirmed to divide d. However, it must be noted that, in Book 7, Euclid calls that $a : b$ and $c : d$ are proportional if and only if there exists a quadruple of integers m, n, x, y such that $(a, b, c, d) = (mx, nx, my, ny)$ (In Book 5, Euclid uses the ordinary definition).

However, under this definition, the proof of Proposition 7.19 must be checked. Euclid derives $a : b = c : d$ from $ad : bd = a : b$ and $bc : bd = c : d$. But, under Euclid's definition, the transitivity is not trivial.

References

[1] G. H. Hardy and E. M. Wright, D. R. Heath-Brown, J. Silverman, A. Wiles, *An Introduction to the Theory of Numbers*, the 6th edition, Oxford University Press, 2008.

[2] Trygve Nagell, *Introduction to Number Theory*, AMS Chelsea Publishing, 2001.

[3] David Pengelley and Fred Richman, Did Euclid Need the Euclidean Algorithm to Prove Unique Factorization?, *Amer. Math. Monthly* **113** (2006), 196–205, available in `https://www.math.nmsu.edu/~davidp/euclid.pdf`.

[4] Harold N. Shapiro, *Introduction to the Theory of Numbers*, Dover, 2008 (old edition, John Wiley and Sons, 1983).

[5] Teiji Takagi, *Shotō Seisūron Kōgi (Lectures on Elementary Number Theory)* (in Japanese), the 2nd edition, Kyōritsu Shuppan, 1971.