Number Theory

K R Srinath

Contents

About this document

This article is a collection of different topics and concepts in Number Theory. The reason for writing the article is twofold:

1. When I write/type what I know, it helps me remember it longer and lets me know if I've understood it properly.

2. I wanted to learn LaTeX.

All the content in this article has been taken from *The Higher Arithmetic* (Eighth edition, 2008) by H. Davenport . The arrangement of topics is more or less what it is in my book (I've taken down what I like, and what I feel is important, in my book).

Since this is a single article and not a book, topics will not appear as separate chapters. Important topics will appear as sections and important points will appear as subsections. General text for explanation will appear as ordinary text in the (sub)section.

Concepts like divisibility, factorization and primes are not explained. Most theorems will be written in an informal fashion in this article.

Conventions

The word 'number' appearing in the document refers to a natural number (from the set $\mathrm{N} = \{1,2,\ldots,\infty\}$).

1 The Fundamental Theorem of Arithmetic

Any number can be represented in one and only way as the product of primes.

Restated, there exists only one factorization into primes for a given number. Thus, any number n can be written as

$$n = p^a q^b r^c \dots \tag{1}$$

where p, q, r are primes and a, b, c are their exponents. According to the fundamental theorem, p, q, r and a, b, c are all unique.

Proof of the uniqueness of factorization

Consider a number n. If n is prime, there is nothing to prove. So let n be composite.

Suppose,

$$n = pqr \dots = p'q'r' \dots \tag{2}$$

Further, suppose none of the primes in the two representations are equal.

Let p be the least of the primes p, q, r and p' the least of p', q', r'. We have

$$n \geq p^2$$

Similarly,

$$n \geq p'^2$$

Since

$$p \neq p\text{'}$$

one of the given relations is a strict inequality. Thus,

$$n > pp'$$

Now,

$$n - pp'$$

is divisible by p and also by p'. Thus,

$$n - pp' = pp'QR \dots$$

pp' is now a factor of n and p' is a factor of q, r, ... in 2. However, p' is not one of q, r, ...

Thus, we have a contradiction, implying that n can have only one factorization into primes.

Why 1 is neither prime not composite

1 cannot be composite, since there are no numbers p, q, r, less than 1 which can make up 1. Now, suppose 1 was considered in the primes. 1 could now be rewritten as

$$n = p^a q^b r^c \dots (1)^\alpha$$

It is obvious that α can take on the value of any number. Thus, there are arbitrarily many (infinite) *trivial* factorizations for a given number, in contradiction to the fundamental theorem. As a result, it is better to consider 1 as an exception to the ordinary prime/composite classification and avoid encumbering the definition.

2 Euclid's algorithm for GCD

Suppose we need to find the GCD of two numbers, a and b, with a ¿ b. Then, write out a as

$$a = qb + c$$

with $0 < c < b$. The GCD of a and b also divides $c = a$ - qb.
Thus, we have

$$b = q_1 c + d$$

The problem of finding the GCD of a and b has now reduced to the problem of finding the GCD of b and c, with both of them less than a. Hence, the process of writing out such equations must eventually terminate.

Finally, we may have

$$w = q_n y$$

q_n is the GCD of a and b.

3 Euclid's Theorem

If a prime divides the product of two numbers, it must divide atleast one of the numbers.

Another proof of the uniqueness of factorization

Let

$$n = pqr \dots = p'q'r' \dots$$

Now, since p divides $p'(q'r'\ldots)$, it must divide either p' or $q'r'\ldots$. If it divides p', $p = p'$, since p' is prime. We can now cancel p and p' from both sides and repeat this argument.

Eventually, all primes on the left turn out to be the same as those on the right.

4 The Linear Diophantine Equation

An equation of the form

$$ax - by = m$$

that can only be solved if and only if GCD(a,b) = 1.

As a special case, the equation can also be solved for

$$ax_0 - by_0 = GCD(a, b)$$

with x_0 and y_0 being the quantities to be determined.

5 The congruence notation

Introduced by Gauss, it helps express, in a convenient form, that two numbers a and b differ by an integral multiple of a fixed number m. It is said that a is congruent to b with respect to the *modulus* m. In symbols,

$$a \equiv b \pmod{m}$$

In other words, a - b is divisible by m.

Complete set of residues

Any set of m numbers is a complete set of residues (mod m) if no two numbers in the set are congruent (to each other).