# Foundations of Arithmetic

## Notation

We shall denote the sum and product of numbers in the usual notation as

$$a_2 + a_2 + a_3 + \cdots + a_k = \sum_{i=1}^{k} a_i\,, \quad a_1 a_2 a_3 \ldots a_k = \prod_{i=1}^{k} a_i$$

The notation $a \mid b$ means $a$ divides $b$, i.e. $ac = b$ where $c$ is an integer, and $a \nmid b$ means $a$ does not divide $b$. If $ac = b$ $(|b| > 1)$ implies $a = \pm 1$ or $a = \pm b$ then $b$ is a *prime number*. A number $b$ $(|b| > 1)$ that is not prime is said to be *composite*.

Let

$$\max(a,b) = \begin{cases} a & (a > b) \\ b & (b > a) \end{cases}, \quad \min(a,b) = \begin{cases} b & (a > b) \\ a & (b > a) \end{cases}, \quad \max(a,a) = \min(a,a) = a.$$

It is obvious that

$$\max(a,b) + \min(a,b) = a + b. \tag{1}$$

## The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that any number $m \geq 1$ is expressed uniquely as a product of powers of prime numbers. Denote the $i^{th}$ prime number by $p_i$, i.e. $p_1 = 2,\ p_2 = 3,\ p_3 = 5, \ldots, p_8 = 19$, etc. Then

$$m = \prod_{i=1}^{\infty} p_i^{j_i} \quad (j_i \geq 0). \tag{2}$$

If $p_k$, say, is not a prime factor of $m$ then $j_k = 0$ so that the factor $p_k^{j_k} = 1$. If $p_M$ is the largest prime factor of $m$ then $j_i = 0$ for $i > M$ so that all the factors involving primes greater than $p_M$ reduce to 1. If $m = 1$ then $j_i = 0$ for $i \geq 1$

The representation (2) can be proved by induction. Assume it is true for $1 \leq m \leq n-1$. When $m = n$, $n$ can be either prime, in which case the representation (2) is trivially true, or it is composite and can therefore be expressed as $n = ab$, where $1 < a \leq n-1$ and $1 < b \leq n-1$. But by the induction hypothesis both $a$ and $b$ can be expressed as a product of primes as in (2) so that the product $ab$ can also be expressed as a product of primes. It follows that (2) is true for $m = n = ab$ and by induction the result is proved for all $m$.

It remains to be shown that (2) is unique. Suppose there are two different representations of $m$ expressed in the form of (2), i.e.

$$m = \prod_{i=1}^{\infty} p_i^{j_i} = \prod_{i=1}^{\infty} p_i^{k_i} \quad (j_i \geq 0, \;\; k_i \geq 0). \tag{3}$$

Consider a prime factor $p_s$ for which $\max(j_s, k_s) \neq 0$ and $j_s \neq k_s$ and assume for the sake of argument that $j_s > k_s$. Then (3) can be written as

$$p_s^{j_s - k_s} \prod_{i=1}^{s-1} p_i^{j_i} \prod_{i=s+1}^{\infty} p_i^{j_i} = \prod_{i=1}^{s-1} p_i^{k_i} \prod_{i=s+1}^{\infty} p_i^{k_i} \quad (j_i \geq 0, \;\; k_i \geq 0).$$

(Note if $k_s > j_s$, a factor $p_s^{k_s - j_s}$ would be taken out of the right-hand side instead.) If $j_s \neq k_s$ the left-hand side of this equation is divisible by $p_s$ but the right-hand side is not, which is impossible. Thus $j_s = k_s$ and since this applies to all prime factors $p_i$ whose exponents are not already equal, we deduce that the two products in (3) are identical. Therefore, the representation of a number $m$ as a product of primes is unique.

Let us now consider a couple of consequences of the Fundamental Theorem.

(i) ***The highest common factor and lowest common multiple of two numbers***

By analogy with (2), another number $n \geq 1$ can be represented as

$$n = \prod_{i=1}^{\infty} p_i^{k_i} \quad (k_i \geq 0)$$

where $k_i = 0$ for $i > N$ when $p_N$ is the largest prime factor of $n$. The Highest Common Factor (HCF) of two numbers $m$ and $n$ is the largest divisor of both numbers (which is why it is sometimes called the Greatest Common Divisor or GCD). Clearly the HCF must include all the common prime factors of both numbers. If $p_i$ is a common factor raised to the powers $j_i$ and $k_i$ respectively, then the largest factor common to both $m$ and $n$ is $p_i^{\min(j_i, k_i)}$. Note that if $p_i$ is *not* a common factor but occurs only in the representation of $m$ (say) then it is necessary that $k_i = 0$ in order to exclude it from the representation of $n$, as required. In this case $\min(j_i, k_i) = 0$ so that $p_i$ is omitted from the HCF as well, as indeed it should be. Thus all cases are included in the formal definition

$$\mathrm{HCF}(m, n) = \prod_{i=1}^{\infty} p_i^{\min(j_i, k_i)}$$

The Lowest Common Multiple (LCM) is the smallest number that is divisible by both $m$ and $n$. This time we must choose $p_i$ raised to the greater of the two powers $j_i$ and $k_i$ in order for both $m$ and $n$ to be divisors of the LCM. Thus we define

$$\mathrm{LCM}(m, n) = \prod_{i=1}^{\infty} p_i^{\max(j_i, k_i)}$$

Using (1) we obtain

$$\prod_{i=1}^{\infty} p_i^{\min(j_i,k_i)} \prod_{i=1}^{\infty} p_i^{\max(j_i,k_i)} = \prod_{i=1}^{\infty} p_i^{\max(j_i,k_i)+\min(j_i,k_i)} = \prod_{i=1}^{\infty} p_i^{j_i+k_i} = \prod_{i=1}^{\infty} p_i^{j_i} \prod_{i=1}^{\infty} p_i^{k_i}$$

Hence

$$\mathrm{HCF}(m,n) \cdot \mathrm{LCM}(m,n) = mn.$$

Thus once the HCF is known the LCM is easily found.

A familiar way of calculating the HCF dates back to Euclid. Let $h = \mathrm{HCF}(m,n)$ and suppose $m \geq n$. Then

$$m = c_1 n + r_1 \quad (0 \leq r_1 < n). \tag{4}$$

Here $r_1$ is the remainder left after dividing $m$ by $n$. If $n \mid m$ then $r_1 = 0$ and the HCF is simply $n$ itself. Otherwise $r_1$ must be smaller than $n$ because $c_1$ is the maximum number of times $n$ goes into $m$. Since $h \mid m$ and $h \mid n$ it is obvious from (4) that $h \mid r_1$ as well, and because $n > r_1$ we may therefore write by analogy with (4)

$$n = c_2 r_1 + r_2 \quad (0 \leq r_2 < r_1). \tag{5}$$

Again we have $h \mid r_2$ because it also divides both $n$ and $r_1$ in the above equation. The procedure continues in this way, the next step yielding

$$r_1 = c_3 r_2 + r_3 \quad (0 \leq r_3 < r_2)$$

where $h \mid r_3$ and so on until we reach the $(k-1)^{\text{th}}$ and $k^{\text{th}}$ steps

$$r_{k-2} = c_k r_{k-1} + r_k \quad (0 \leq r_k < r_{k-1}) \tag{6}$$

$$r_{k-1} = c_{k+1} r_k + r_{k+1} \quad (0 \leq r_{k+1} < r_k).$$

The sequence of positive integers $r_1 > r_2 > \cdots > r_{k-1} > r_k$ is decreasing so must eventually terminate in 0. Let $r_{k+1} = 0$ so that the last equation above reduces to

$$r_{k-1} = c_{k+1} r_k \quad (0 < r_k) \tag{7}$$

where $h \mid r_k$ which implies $h \leq r_k$.

Reversing the argument, we see from (7) that $r_k \mid r_{k-1}$ and $r_k \mid r_{k-1} \Rightarrow r_k \mid r_{k-2}$ by (6). Likewise

$$r_k \mid r_{k-2} \Rightarrow r_k \mid r_{k-3} \Rightarrow r_k \mid r_{k-4} \Rightarrow \cdots \Rightarrow r_k \mid r_2 \Rightarrow r_k \mid r_1 \Rightarrow r_k \mid n \Rightarrow r_k \mid m$$

the last two steps following from (5) and (4). Thus $r_k$ is a common factor of both $m$ and $n$, but because $h$ is the *highest* common factor it must satisfy $h \geq r_k$. We have now proved that $h$ satisfies both $h \leq r_k$ and $h \geq r_k$ from which we conclude $h = r_k$, the final remainder in Euclid's algorithm.

As a numerical example of its application, let us calculate the HCF of 2472 and 9216:

$$9216 = 3 \times 2472 + 1800$$

$$2472 = 1 \times 1800 + 672$$

$$1800 = 2 \times 672 + 456$$

$$672 = 1 \times 456 + 216$$

$$456 = 2 \times 216 + 24$$

$$216 = 9 \times 24$$

Thus 24, the last remainder, is the HCF of 2472 and 9216.

Finally, we derive from this algorithm a property of the HCF that is not particularly obvious from its definition, namely that there exist integers $a$ and $b$ (one of them being negative) such that $h = am + bn$. For, from (6) we have

$$h = r_k = r_{k-2} - c_k r_{k-1} = r_{k-2} - c_k(r_{k-3} - c_{k-1}r_{k-2}) = ur_{k-2} - c_k r_{k-3} = ur_{k-4} - vr_{k-3}$$
$$= wr_{k-4} - vr_{k-5} = \cdots$$

where $u = 1 + c_k c_{k-1}$, $v = c_k + uc_{k-2}$, $w = u(1 + c_{k-2}c_{k-3}) + c_k c_{k-3}$. Note that $c_k, u, v, w,$ etc. are all positive numbers so that one term in each step is positive and the other negative. The procedure continues as we work backwards through the algorithm to the final two equations, which according to (4) and (5), will take the form $h = \cdots = cn + ar_1 = am + bn$ with $a$, $b$ and $c$ representing integers to be determined.

Using the same numerical example ($m = 9216,\ n = 2472$) to illustrate the theory, we find that successive stages of the calculation give

$$m = 3n + 1800 \Rightarrow m - 3n = 1800$$

$$n = 1 \times (m - 3n) + 672 \Rightarrow 4n - m = 672$$

$$m - 3n = 2 \times (4n - m) + 456 \Rightarrow 3m - 11n = 456$$

$$4n - m = 1 \times (3m - 11n) + 216 \Rightarrow 15n - 4m = 216$$

$$3m - 11n = 2 \times (15n - 4m) + h \Rightarrow h = 11m - 41n.$$

Thus $a = 11$ and $b = -41$ in this example. Checking we see that

$$11 \times 9216 - 41 \times 2472 = 101{,}376 - 101{,}352 = 24$$

which verifies the stated property of the HCF.

(ii) ***Analytical form of the fundamental theorem***

Now consider the expression

$$f_k(s) = \prod_{i=1}^{k} \frac{1}{1 - p_i^{-s}} \qquad (s > 1).$$

Since $(1-x)^{-1} = \Sigma_{r=0}^{\infty} x^r$ for $|x| < 1$, and since $p_i \geq 2$, the expression under the product sign can be expanded in a convergent series, i.e.

$$f_k(s) = \prod_{i=1}^{k} \sum_{r=0}^{\infty} (p_i^{-s})^r \qquad (s > 1).$$

Suppose $k = 2$ for simplicity, then

$$f_2(s) = \sum_{r=0}^{\infty} (p_1^{-s})^r \sum_{t=0}^{\infty} (p_2^{-s})^t = \sum_{r=0}^{\infty} \sum_{t=0}^{\infty} (p_1^r p_2^t)^{-s}$$

where $p_1 = 2$ and $p_2 = 3$ of course. Clearly all numbers that have prime factors 2 and 3 raised to all possible combinations of powers will be included within the brackets of this double summation. For example,

$$1^{-s} = (2^0 \times 3^0)^{-s},\ 2^{-s} = (2^1 \times 3^0)^{-s},\ 3^{-s} = (2^0 \times 3^1)^{-s},\ 72^{-s} = (2^3 \times 3^2)^{-s},$$
$$(124{,}416)^{-s} = (2^9 \times 3^5)^{-s}$$

are five such terms in the sum defining $f_2(s)$. Thus we may write

$$f_2(s) = \sum_{p_1, p_2} n^{-s}$$

where the notation implies that summation is over all numbers $n$ whose prime factors comprise every possible combination of powers of $p_1$ and $p_2$. By the Fundamental Theorem each $n$ is uniquely expressed and can therefore only appear once in the summation. Likewise, $f_3(s)$ will be the sum of all numbers with prime factors 2, 3 and 5 raised to all possible combinations of powers. In general, we have

$$f_k(s) = \sum_{p_1, p_2 \ldots p_k} n^{-s} > \sum_{n=1}^{p_k} n^{-s}$$

the inequality resulting from the fact that the numbers from 1 to $p_k$ are already included in the first summation, as indicated by the first three terms in the example above for $f_2(s)$.

Since $s > 1$, the infinite series $\Sigma_{n=1}^{\infty} n^{-s}$ is convergent. It is in fact the well-known Riemann zeta function $\zeta(s)$. It follows from the inequality above that

$$f_k(s) > \sum_{n=1}^{p_k} n^{-s} = \sum_{n=1}^{\infty} n^{-s} - \sum_{n=p_k+1}^{\infty} n^{-s} > 0$$

which, on rearrangement, becomes

$$0 < \zeta(s) - f_k(s) < \sum_{n=p_k+1}^{\infty} n^{-s}.$$

Now let $k \to \infty$ which means $p_k \to \infty$ as well. Then the right-hand side of this equation tends to 0 so that $f_\infty(s) = \lim_{k\to\infty} f_k(s) = \zeta(s)$, or with reference to the original definition of $f_k(s)$,

$$\zeta(s) = \prod_{i=1}^{\infty} \frac{1}{1 - p_i^{-s}}.$$

Hardy and Wright (*An Introduction to the Theory of Numbers*, 4th Edition, Oxford University Press, 1960) call this an analytical expression of the Fundamental Theorem of Arithmetic. It is an important result in the theory of primes as it relates them to the zeta function which has been extensively analysed.

## The product of $n$ consecutive positive integers is divisible by $n!$

This is a simple result but it provides a good example of proof by induction.

We want to prove $n! \mid m(m+1)(m+2)\ldots(m+n-1)$, for $m \geq 1$ and $n \geq 1$. In one sense this is obvious because

$$\frac{m(m+1)(m+2)\ldots(m+n-1)}{n!} = \frac{(m+n-1)!}{(m-1)!\,n!} = {}^{m+n-1}\mathrm{C}_n$$

where ${}^{m+n-1}\mathrm{C}_n$ is the familiar notation for the number of ways of selecting $n$ objects from a collection of $m+n-1$ unlike objects. Since this is a countable number it must be an integer and the result is verified. A more formal proof that doesn't rely on a practical interpretation is by induction.

Define $k = m+n$ and $P(k) = (k-n)(k-n+1)(k-n+2)\ldots(k-1)$, and let $\mathcal{S}(k)$ represent the statement $n! \mid P(k)$ for $k \geq 2$ and $1 \leq n \leq k-1$ which is equivalent to the statement to be proved. Note that each value of $k > 2$ covers several cases, e.g. $\mathcal{S}(9)$ includes $5! \mid 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8$ and $3! \mid 6 \cdot 7 \cdot 8$ among six other possibilities. The case $k = 2$ corresponds to $m = n = 1$. Thus $P(2) = 1$ and $\mathcal{S}(2)$ is trivially true. Assume that $\mathcal{S}(k)$ is true for $2 \leq k \leq K$ so that in particular $\mathcal{S}(K)$ is true, i.e. $n! \mid P(K)$ for $1 \leq n \leq K-1$, or written out in full

$$n! \mid (K-n)(K-n+1)(K-n+2)\ldots(K-1) \quad (1 \leq n \leq K-1). \tag{8}$$

Since $1 \leq n-1 < n \leq K-1$ for $n \geq 2$, we also have

$$(n-1)! \mid (K-n+1)(K-n+2)\ldots(K-1) \qquad (n \geq 2). \tag{9}$$

Now

$$P(K+1) = (K-n+1)(K-n+2)\ldots(K-1)K = (K-n)(K-n+1)\ldots(K-1) + n(K-n+1)(K-n+2)\ldots(K-1).$$

By (8) the first term on the right-hand side is divisible by $n!$ for $1 \leq n \leq K-1$ and because of its additional factor $n$, the second term is also divisible by $n!$ for $n \geq 2$ according to (9). Thus $n! \mid P(K+1)$ for $2 \leq n \leq K-1$. Furthermore, for $n = K$ the statement $n! \mid P(K+1)$ becomes $K! \mid 1 \cdot 2 \cdot 3 \ldots K$ which is obviously true and it reduces to the trivial result $1! \mid K$ for $n = 1$. Thus $n! \mid P(K+1)$ for $1 \leq n \leq K$ and therefore $\mathcal{S}(K+1)$ is true if $\mathcal{S}(k)$ is true for $2 \leq k \leq K$. Since we have shown $\mathcal{S}(2)$ to be true it follows by induction that $\mathcal{S}(k)$ is true for all $k \geq 2$ and the result is proved.

## A number is divisible by nine if and only if the sum of its digits is nine

This familiar arithmetical trick is known to many school students who otherwise have little interest in mathematics. Its proof, however, serves as an elementary introduction to modular arithmetic and congruences.

If $a, r$ and $m$ are integers, then the statement $a$ is congruent to $r$ modulo $m$ means $m \mid (a-r)$ and is written formally as $a \equiv r \pmod{m}$. In other words, $a-r$ is some multiple of $m$, that is $a = r + km$ where $0 \leq r < m$ and $k$ is a positive integer. This last expression shows that $r$ is the remainder when $a$ is divided by $m$, but there are other numbers, namely those that differ from $a$ by a multiple of $m$, that have the same remainder $r$ when divided by $m$. Modular arithmetic doesn't distinguish between such numbers; they are all regarded as equivalent. For example $10 \equiv 1 \pmod{9}$ but so is $19 \equiv 1 \pmod{9}$, and also 28, 37 and so on. Moreover, if $10^n \equiv 1 \pmod{9}$ then $10^{n+1} - 1 = 10(10^n - 1) + 9$ is also divisible by 9, showing that $10^{n+1} \equiv 1 \pmod{9}$. Hence by induction $10^n \equiv 1 \pmod{9}$ for all positive $n$ since it is true for $n = 0$.

Clearly if $a \equiv r \pmod{m}$ and $b \equiv s \pmod{m}$, then $a + b \equiv r + s \pmod{m}$ because both terms $a-r$ and $b-s$ are divisible by $m$. Similarly, $ka \equiv kr \pmod{m}$ because $m \mid k(a-r)$. We proved in the last paragraph that $10^n \equiv 1 \pmod{9}$ so it follows that $a10^n \equiv a \pmod{9}$ and hence $a10^n + b10^q \equiv a + b \pmod{9}$.

Now let a number $c$ be written in the usual way as $a_n a_{n-1} \ldots a_1 a_0$, e.g. if $c = 9704$ we have $a_0 = 4,\ a_1 = 0,\ a_2 = 7, a_3 = 9$. This standard notation is, of course, shorthand for the expression $c = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n$. By virtue of the result in the preceding paragraph we deduce that $c \equiv a_0 + a_1 + a_2 + \cdots + a_n \pmod{9}$ or $9 \mid [c - (a_0 + a_1 + \cdots a_n)]$. Thus if $c$ is divisible by 9 then the sum of its digits must also be divisible by 9 and conversely, if 9 divides the sum of the digits of $c$ then $c$ itself is divisible by 9.