Chapter 2
The Natural Numbers

'O θεὸζ ἀριθμητίζει
– Carl Friedrich Gauss

Here we encounter such basic concepts as *integers, composites*, and *primes*, and we learn the very fundamental fact that the composites can be represented in a *unique* way as a product of primes.

The *least common multiple* and the *greatest common divisor* of two or more integers may be familiar from high school, but they are ideas that pervade all of number theory. Here we demonstrate some of their basic properties and point to some natural phenomena in the real world of gears, planetary motion, and musical pitch.

If integers can be prime, pairs of integers can be "mutually prime" or *coprime* if they have no common factors, in other words, if their greatest common divisor is 1. Coprimality is another important property of two (or more) integers.

One of the very early tools of number theory is *Euclid's algorithm*; it allows us to find, in a systematic manner, the greatest common divisor of two integers without solving the often difficult problem of factoring the two integers. As we shall later see, Euclid's algorithm generalizes to polynomials and allows us to solve important integer equations, the so-called Diophantine equations.

2.1 The Fundamental Theorem

We will speak here of the "whole numbers" or *integers* ... -3, -2, -1, 0, 1, 2, 3, ..., denoted by the letter $\mathbb{Z}$, and more often of the so-called "natural" numbers or positive integers: 1, 2, 3, 4, 5 and so forth. Some of these are divisible by others without leaving a remainder. Thus, $6 = 2 \cdot 3$, i. e., 6 is divisible by 2 and by 3 without a remainder. Such numbers are called *composites*.

Other numbers have no divisors other than 1 and themselves, such as 2, 3, 5, 7, 11, 13, 17, etc. These numbers are called *prime* numbers or simply *primes*. All primes are odd, except 2 – the "oddest" prime (a designation alluding to the special role which 2 plays among the primes). The number 1 is considered neither prime nor

M. Schroeder, *Number Theory in Science and Communication*, 5th ed.,
DOI 10.1007/978-3-540-85298-8_2,

composite. Otherwise some theorems would require very awkward formulations – such as the following.

The *fundamental theorem of arithmetic* states that each natural number n can be uniquely factored into primes:

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \dots p_r^{e_r} = \prod_i p_i^{e_i}. \tag{2.1}$$

Here the order of the factors is considered irrelevant.

Equation (2.1) can be read in two ways:

1) p_i is the ith prime – in which case the exponent e_i has to be zero if p_i is not a factor of n.
2) Only those primes that are factors of n appear in (2.1). We will use either reading of (2.1) and state which if it makes a difference.

There is no corresponding theorem for the *additive* decomposition of natural numbers into primes. This is one of the reasons why additive number theory, for example partitions (Chap. 22), is such a difficult subject. In this book we will be mostly concerned with *multiplicative* number theory, which has many more applications.

2.2 The Least Common Multiple

Two integers n and m have a least common multiple (LCM) $[n,m]$. The LCM is needed to combine two fractions with denominators n and m into a single fraction. In fact, that is where the everyday expression "to find the least common denominator" (of divergent views, for example) comes from. For example, for $n = 6$ and $m = 9$, $[6,9] = 18$.

Example: $\dfrac{1}{6} + \dfrac{2}{9} = \dfrac{3}{18} + \dfrac{4}{18} = \dfrac{7}{18}$.

It is easily seen that with n as in (2.1) and

$$m = \prod_i p_i^{f_i}, \tag{2.2}$$

$$[n,m] = \prod_i p_i^{\max(e_i,f_i)}, \tag{2.3}$$

because in the LCM each prime factor p_i must occur at *least* as often as it does in either n or m. Thus, for $n = 6 = 2^1 \cdot 3^1$ and $m = 9 = 3^2$, $[6,9] = 2^1 \cdot 3^2 = 18$.

There are numerous applications of the LCM. Consider two gears with n and m teeth meshing, and suppose we mark with a white dot one of the n teeth on the first gear and one of the m spaces between teeth of the second gear. When the gears turn, how often will the two white dots meet? Perhaps never! But if they meet once, they will meet again for the first time after $[n,m]$ teeth have passed the point of

contact, i. e., after the first gear has undergone $[n,m]/n$ (an integer!) revolutions and the second gear an integer $[n,m]/m$ revolutions.

2.3 Planetary "Gears"

Our "gears", of course, could be any of a plethora of other objects that can be modelled as meshing gears even if no teeth are visible. Thus, the revolutions of the planet Mercury around itself and the Sun are locked by gravitational forces as if geared: during two revolutions around the Sun, Mercury revolves three times around itself. (As a consequence, one day on Mercury lasts two Mercury years. Strange gears – and even stranger seasons!) Similarly, the Earth's moon revolves exactly once around itself while completing one orbit around the Earth; that is why it always shows us the same side. On the moon, Earth day (or night) lasts forever.

The "teeth" that keep the moon locked to the Earth are, as in the case of Mercury and the sun, gravitational forces. But these "gravitational teeth" are relatively weak and would not "engage" if unfavourable initial conditions were not damped out by friction such as that provided by the ocean tides on Earth. (Eventually, the Earth day may lock in with the Earth year, which will play havoc with night and day as we know it.)

And not long ago, it was discovered that even the distant planets Pluto and Neptune are coupled to each other strongly enough to be locked into an integer "resonance" (in the astronomer's lingo).

Another question answered by the LCM, although no teeth are in evidence, has to do with the coincidence of dates and weekdays. Because the number of days per year (365) is not divisible by the numer of days per week (7), coincidences of dates and weekdays do not recur from one year to the next. Furthermore, because every fourth year is a leap year, coincidences are not equally spaced in years. However, even without knowing when leap years occur, we can always guarantee that a coincidence will recur after 28 years, 28 being the LCM of 4 and 7. (In the year 2100 the leap day will be dropped, temporarily violating the 28-year cycle.)

Equation (2.3) easily generalizes to more than two integers: the max function in (2.3) then contains as many entries as there are integers whose LCM we want to determine.

As we indicated above when introducing the meshing gear picture, the two white markers may never meet. More learnedly, we would say that a certain linear Diophantine equation (see Chap. 7) has no solution. This can happen only if n and m have a greatest common divisor greater than 1. This brings us to our next topic.

2.4 The Greatest Common Divisor

Another important relation between integers is their greatest common divisor (GCD). For two integers n and m given by (2.1) and (2.2), the GCD is

$$(n,m) = \prod_i p_i^{\min(e_i,f_i)}, \tag{2.4}$$

because for the GCD to divide both n and m it cannot have the factor p_i more often than it is contained in either n or m, whichever is *less*.

Example: $n = 10 = 2^1 \cdot 5^1$ and $m = 25 = 5^2$. Thus $(10,25) = 5$.

Two numbers n and m that have no common factors are called relatively prime, mutually prime or *coprime*. In this case the GCD equals 1.

Example: $(6,35) = (2{\cdot}3, 5{\cdot}7) = 1$.

For any two numbers n and m, the product of the GCD and the LCM equals the product of n and m:

$$(n,m)[n,m] = nm,$$

because whenever the formula (2.4) for the GCD picks the exponent e_i for p_i, the formula (2.3) for the LCM picks the exponent f_i, and vice versa.

Thus,

$$(n,m)[n,m] = \prod_i p_i^{e_i+f_i} = nm. \tag{2.5}$$

Example:

$$(4,10) = (2^2, \underline{2}{\cdot}5) = 2; \quad [4,10] = [\underline{2}^2, 2{\cdot}\underline{5}] = 20; \quad 2 \cdot 20 = 4 \cdot 10\,. \ \textit{Check}!$$

The generalization of (2.5) to three integers is

$$(n,m,k)[nm,mk,kn] = nmk, \tag{2.6}$$

which is easily verified. Assume that a given prime p occurring in the prime factorization of the product nmk occurs e_n times in n, e_m times in m and e_k times in k and that, without loss of generality,

$$e_n \le e_m \le e_k.$$

Then the exponent of p in (n,m,k) is e_n, and in $[nm,mk,kn]$ it is $e_m + e_k$. Thus the left side of (2.6) has the prime p with the exponent $e_n + e_m + e_k$, as does the right side of (2.6). The same is true for all primes occurring in nmk. The correctness of (2.6) then follows from the fundamental theorem of arithmetic.

The *dual* of (2.6) is

$$[n,m,k](nm,mk,kn) = nmk, \tag{2.7}$$

which is proved by the same reasoning. Generalizations of (2.6) and (2.7) to more than three factors should be obvious.

For more than two integers, some particularly interesting relations between GCD and LCM exist. For example, two such relations are the "distributive law"

$$(k[m,n]) = [(k,m),(k,n)], \tag{2.8}$$

and its *dual*

$$[k,(m,n)] = ([k,m],[k,n]), \tag{2.9}$$

both of which are a direct consequence of the properties of the min and max functions in (2.4) and (2.3).

There is even a very pretty *self-dual* relation:

$$([k,m],[k,n],[m,n]) = [(k,m),(k,n),(m,n)], \tag{2.10}$$

i. e., in the expression appearing on either side of (2.10), the operations LCM and GCD can be completely interchanged without affecting their validity!

However, from a practical point of view there *is* a difference: The right-hand side of (2.10), i. e., doing GCDs before the LCMs, is usually easier to figure out. Thus, (2.10) can be exploited to computational advantage.

It is interesting to note that relations such as (2.6–2.10) occur in many other mathematical fields, such as mathematical logic or set theory, where our LCM corresponds to the set-theoretic *union* $\cup$ and the GCD corresponds to *intersection* $\cap$.

But what, in number theory, corresponds to the set-theoretic relation

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B},$$

where the bar stands for complement?

For additional relations see [2.1].

The GCD appears in the solution to many, seemingly unrelated, problems. For example, take n jugs with capacities of $L_1, L_2, \ldots, L_n$ liters. What amounts k of water (or wine) can be dispensed by these $n/1$ jugs?

Answer: k must be a multiple of the GCD $[L_1, L_2, \ldots, L_n]$. (After T. J. Pfaff and M. M. Tran. *The Pi Mu Epsilon Journal* 12:1 (2004), 37–38.)

2.5 Human Pitch Perception

An interesting and most surprising application of the GCD occurs in human perception of pitch: the brain, upon being presented with a set of harmonically related frequencies, will perceive the GCD of these frequencies as the pitch. Thus, the subjective pitch of the two-tone chord (320 Hz and 560 Hz) is $(320, 560) = 80$ Hz, and *not* the difference frequency (240 Hz).

Upon a frequency shift of $+5$ Hz applied to both frequencies, the GCD drops to 5 Hz; and for an irrational frequency shift, the GCD even drops to 0 Hz. But that is

not what the ear perceives as the pitch. Rather it tries to find a *close match* in the range of pitches above 50 Hz. For the frequencies 325 Hz and 565 Hz such a match is given by 81 Hz, which is the GCD of 324 Hz and 567 Hz – close to the two given frequencies.

Note that the concept that pitch is given by the difference frequency or "beat" frequency has been beaten: if both frequencies are shifted by the same amount, their difference remains unchanged. Yet psychoacoustic experiments clearly show that the perceived pitch is increased, from 80 Hz to about 81 Hz in our example, just as the amplified GCD model predicts [2.2].

What this tells us is that the human brain switches on something like a GCD-spectral matching computer program when listening to tone complexes. Fascinating? Indeed. Unbelievable? Well, the brain has been caught doing much trickier things than that.

2.6 Octaves, Temperament, Kilos and Decibels

The Pythagoreans discovered that subdividing the string of a musical instrument into the ratio of small integers resulted in pleasing musical intervals. Thus, dividing the string into 2 equal parts gives a frequency ratio (compared with the full-length string) of $2:1$ – the musical octave. Shortening the string by one third gives rise to the frequency ratio $3:2$ – the musical fifth. And dividing the string into 4 equal parts results in the frequency ratio $4:3$ – the musical fourth.

The Pythagorean musical scale was constructed from these simple ratios. How do they fit together? How many fifths make an integral number of octaves? Or, what is x in

$$\left[\frac{3}{2}\right]^x = 2^y,$$

or, equivalently,

$$3^x = 2^z,$$

where $z = y + x$? The fundamental theorem (Sect. 2.1) tells us that there are *no* integer solutions. But there are *approximate* solutions, even in small integers. Thus,

$$3^5 = 243 \approx 256 = 2^8. \tag{2.11}$$

Consequently, 5 musical fifths equal *about* 3 octaves. To make the octave come out correctly, we would have to tamper with the ratio $3:2 = 1.5$, increasing it by about 1% to 1.515…, to achieve a well-tempered temperament.

The fact that $(3/2)^5$, with a little tampering, equals 2^3 also has its effect on the musical fourth: from

$$\left[\frac{3}{2}\right]^5 \approx 2^3$$

follows directly

$$\left[\frac{4}{3}\right]^5 \approx 2^2;$$

in other words, 5 fourths make about 2 octaves. The tampering required on the fourth to make it fit 2 octaves exactly is, as in the case of the fifth, only one part in a hundred.

We shall leave the musical details to J. S. Bach and his well-tempered clavier and ask ourselves the more general question of how we can find approximate integer solutions to equations like $a^x = b^y$ in a more systematic way. The answer: by expanding logarithms into continued fractions, as will be explained in Sect. 5.1. There we learn that for $a = 3$ and $b = 2$, for example, the next best approximation (after $3^5 \approx 2^8$) is $3^{12} \approx 2^{19}$, requiring an adjustment of the musical fifth by only one part in a thousand so that 12 "tampered" fifths will make 7 octaves, thereby avoiding the *Pythagorean comma*. This is of great interest to musicians because it allows the construction of a complete key from ascending fifths (the famous Circle of Fifths).

A much closer numerical coincidence, with important consequences in music, computer memory, photography and power measurements, is the approximation

$$5^3 = 125 \approx 128 = 2^7. \tag{2.12}$$

Musically, this means that 3 major thirds (frequency ratio $= 5 : 4$) equal about *one* octave:

$$\left[\frac{5}{4}\right]^3 \approx 2,$$

which requires an adjustment of less than 8 parts in a thousand in the major third so that 3 of them match the octave exactly.

Another consequence of (2.12) is that

$$2^{10} = 1024 \approx 10^3.$$

According to international standards, the factor 10^3 is denoted by the prefix *kilo*, as in kilometre. But computer memories are not measured in kilometres or weighed in kilograms; rather they are *addressed*, and the proper form of address is *binary*. As a consequence, memory sizes are usually powers of 2, and in computerese a 256-kilobit memory chip can actually store 262144 bits of information because, to hard- and software types, kilo means 1024 – not 1000.

The near coincidence of 5^3 and 2^7 also shows up among camera exposure times, where $1/125$ of a second is 7 lens-aperture "stops" away from 1 second. But 7 stops correspond to a light energy factor of $2^7 = 128$.

Still another application in which $5^3 \approx 2^7$ is exploited is the field of power or intensity measurement. The preferred logarithmic measure of intensity is the *decibel*,[1] 10 decibels being equal to an intensity ratio of 10 : 1. Thus, twice as much power (of a loudspeaker output, for example) means an extra 3 decibels – almost exactly. (A better figure would be 3.01 decibels, but who can hear a hundredth of a decibel?)

J. R. Pierce, lately of Stanford University, has recently proposed a new musical scale based on dividing the frequency ratio 3 : 1 (instead of the 2 : 1 octave) into 13 (instead of 12) equal parts. This scale matches such simple integer ratios as 5 : 3 *and* 7 : 5 (and 9 : 7) with an uncanny accuracy, resulting from the number-theoretic fluke that certain 13th powers of *both* 5 *and* 7 are very close to integer powers of 3. To wit: $5^{13} = 3.0077^{19}$, and $7^{13} = 3.0037^{23}$. Since the integers appearing in the exponents (13, 19, 23) are also coprime (in fact, all three are prime), it is easy to construct complete musical scales exclusively from the small-integer ratios 5 : 3 and 7 : 5. The basic chords of the new scale, 3 : 5 : 7 and 5 : 7 : 9, are superbly approximated by the equal tempered scale $3^{k/13}$ and were found by M. V. Mathews, A. Reeves, and L. Roberts to provide a strong harmonic foundation for music written in the new scale.

2.7 Coprimes

Two integers are said to be *coprime* if their GCD equals 1. Thus, 5 and 9 are coprime: $(5,9) = 1$, while 6 and 9 are *not* coprime: $(6,9) = 3 \neq 1$.

The *probability* that two "randomly selected" integers will be coprime is $6/\pi^2$ (see Sect. 4.4). This is also the probability that a randomly selected integer is "squarefree" (not divisible by a square).

Of three or more integers it is often said that they are *pairwise coprime* if all possible pairs are coprime. Thus, 2, 5 and 9 are pairwise coprime: $(2,5) = (2,9) = (5,9) = 1$. However, 2, 5 and 8 are *not* pairwise coprime because $(2,8) = 2$, although the three numbers seen as a *triplet* have no common factor. The probability that three randomly selected integers will be pairwise coprime is $0.28\ldots$ (see Sect. 4.4).

2.8 Euclid's Algorithm

If the GCD is so important, how does one go about finding it? Answer: by Euclid's algorithm, which is best illustrated by an example. To find the GCD of 35 and 21, first divide the larger number by the smaller:

$$\frac{35}{21} = 1 + \frac{14}{21},$$

[1] Curiously, one never hears about the full unit, the bel, perhaps because a difference of 10 bel is the difference between the sound of a babbling brook and an earsplitting screech.

and repeat the process on the remainder:

$$\frac{21}{14} = 1 + \frac{7}{14},$$

until the remainder is 0:

$$\frac{14}{7} = 2 + 0,$$

which is guaranteed to happen sooner or later. The GCD is the last divisor, 7 in our case. Thus, $(35,21) = 7$, which is the correct answer.

The philosophy behind Euclid's algorithm is the following. It is easy to show that $(a,b) = (a-kb,b)$, where k is an integer. If $a > b > 0$ and if one picks k as large as possible without making $a-kb$ negative, then $a-kb < b$. Thus, we have reduced the problem of computing the GCD of a and b to that of two smaller numbers, namely $a-kb$ and b. Now b is the larger number of the pair, and it can be reduced by subtracting a proper multiple of $a-kb$. Continuing this simple process generates smaller and smaller number pairs all having the same GCD. Finally we must arrive at two numbers that are multiples of each other and the smaller of the two numbers is the GCD. (If a and b are coprime that "smaller number" is of course 1.) This is how and why the Euclidean algorithm works: it chops large numbers down to manageable size.

2.9 The Decimal System Decimated

One of the greatest arithmetical inventions was that of the 0 as a *place holder*. Thus, in the decimal system, 903 means 9 times 100 plus 3 times 1. Their sensitivity to place is the foundation of the decimal, the binary and similar number systems based on place.

But choosing a base, 10 say, there are other ways to represent the integers which does not depend on the customary place principle while still using only the 10 digits 0 through 9. For example, 100 integers from 0 to 99 can be thought of as the *direct sum* of two sets of integers each of size 10: $\{0,1,2,\ldots,9\}$ and $\{0,10,20,\ldots,90\}$. (Direct sum of two sets means every member of one set is added to every member of the other set.) Representing the integers from 0 through 99 by the direct sum of the above two sets is of course analoguous to the standard decimal representation. And, if the base is a prime, this representation is unique. But if the base, like 10 can be factored, there are other *nonstandard* representations by the direct sum of two sets, each of size 10. For example, the sets $\{0,20,22,40,42,60,62,80,82\}$ and $\{0,1,4,5,8,9,12,13,16,17\}$ are two such sets.

Are there other such sets? And how many? What is the "sister" set of $\{0,1,2,3,4,25,26,27,28,29\}$?