1. The Euclidean Algorithm

The common divisors of two numbers are the numbers that are divisors of both of them. For example, the divisors of 12 are 1, 2, 3, 4, 6, 12. The divisors of 18 are 1, 2, 3, 6, 9, 18. Thus, the common divisors of 12 and 18 are 1, 2, 3, 6. The greatest among these is, perhaps unsurprisingly, called the of 12 and 18. The usual mathematical notation for the greatest common divisor of two integers a and b are denoted by (a, b). Hence,

$$(12, 18) = 6.$$

The greatest common divisor is important for many reasons. For example, it can be used to calculate the least common multiple of two numbers, i.e., the smallest positive integer that is a multiple of these numbers. The least common multiple of the numbers a and b can be calculated as

$$\frac{ab}{(a, b)}.$$

For example, the least common multiple of 12 and 18 is

$$\frac{12 \cdot 18}{(12, 18)} = \frac{12 \cdot 18}{6}.$$

Note that, in order to calculate the right-hand side here it would be counter-productive to multiply 12 and 18 together. It is much easier to do the calculation as follows:

$$\frac{12 \cdot 18}{6} = \frac{12}{6 \cdot 18} = 2 \cdot 18 = 36.$$

That is, the least common multiple of 12 and 18 is 36. It is important to know the least common multiple when adding two fractions. For example, noting that $12 \cdot 3 = 36$ and $18 \cdot 2 = 36$, we have

$$\frac{5}{12} + \frac{7}{18} = \frac{5 \cdot 3}{12 \cdot 3} + \frac{7 \cdot 2}{18 \cdot 2} = \frac{15}{36} + \frac{14}{36} = \frac{15 + 14}{36} = \frac{29}{36}.$$

Note that this way of calculating the least common multiple works only for two numbers. We will not discuss the case of more than two numbers; our main interest here is the greatest common divisor. First note that we usually consider only positive divisors. Thus the common divisors of -12 and -18 are 1, 2, 3, 6, i.e., the same as those of 12 and 18. So their greatest common divisor is also 6; i.e., $(-12, -18) = 6$. Similarly, $(-12, 18) = 6$.

Every positive integer is a divisor of 0. Thus the common divisors of 0 and 18 are just the divisors of 18. The greatest common divisor of 0 and 18 is thus the greatest divisor of 18, i.e., 18 itself: $(0, 18) = 18$. Similarly, $(12, 0) = 12$. Note that $(0, 0)$ is undefined, since any positive integer is a divisor of 0 and 0. On the other hand, while it may be uninteresting to consider the greatest common divisor $(12, 12)$, the definition is meaningful in this case, and we have $(12, 12) = 12$.

A way of determining the greatest common divisor of two integers was described by Euclid about 2400 years ago. This method, called the *Euclidean algorithm*, even though it was probably not invented by Euclid himself, or its minor modifications, is still the best method to determine the greatest common divisor of two numbers.

While the greatest common divisor of 12 and 18 can be easily guessed, the situation is different when larger numbers are involved.

We illustrate the Euclidean algorithm by determining the greatest common divisor of 546 and 422.

Step 1. Divide 422 into 546; the remainder is 124. We replace 546 by this remainder. That is, in place of the original numbers 546 and 422, we will work with 422 and 124.

Step 2. Divide 124 into 422; the remainder is 50. We replace 422 with this remainder. That is, in place of 422 and 124, we will work with 124 and 50.

Step 3. Divide 50 into 124; the remainder is 24. We replace 124 with this remainder. That is, in place of 124 and 50, we will work with 50 and 24.

Step 4. Divide 24 into 50; the remainder is 2. We replace 50 with this remainder. That is, in place of 50 and 24, we will work with 2 and 24.

Step 5. Divide 2 into 24; the remainder is 0. The remainder being 0, we stop. The greatest common divisor is the last nonzero remainder, that is, 2.

Why does this procedure work? Before we answer this question, note that the procedure will always terminate. In fact, in each step we work with smaller numbers, so in the end we must reach 0 as a remainder, if no sooner, then at the point when the last divisor is 1.

To explain why the method works it is sufficient to note that each of the pairs we work with have the same greatest common divisor:

$$(546, 422) = (422, 124) = (124, 50) = (50, 24) = (24, 2) = (2, 0).$$

We never actually worked with the last pair, 2 and 0, since there is no reason to go on, because it is clear that $(2, 0) = 2$. It is easy to justify any of these equalities; we will illustrate this with the discussion of the equality

$$(422, 124) = (124, 50).$$

To see this, note that 50 was obtained as the remainder when dividing 124 into 422; in fact,

$$422 = 3 \cdot 124 + 50.$$

This equation shows that any common divisor of 124 and 50 is also a divisor of 422. if one writes this equation as

$$50 = 422 - 3 \cdot 124,$$

then one can see that any common divisor 422 and 124 is also a divisor of 50. Therefore, the common divisors of the numbers 422 and 124 are the same as the common divisors of the numbers 124 and 50; i.e., the greatest common divisor of 422 and 124 is the same as the greatest common divisor of 124 and 50.

2. Representing the Greatest Common Divisor as a Linear Combination

The greatest common divisor of any two integers can be written as a sum of multiples of these integers. Instead of sum of multiples, we will say *linear combination*, since this, perhaps more intimidating, term is the one commonly accepted in the mathematical literature. For example, the greatest common divisor of 422 and 546 is 2, and we have

$$2 = 422 \cdot 22 + 546 \cdot (-17).$$

This is such an important observation that we will formulate it as a theorem:

THEOREM. *For any two integers a and b at least one of which is assumed to be different from 0, there are integers x and y such that*

$$(a, b) = ax + by.$$

It is important to assume that not both of the numbers a and b are zero, since, as we mentioned above, the greatest common divisor $(0, 0)$ is meaningless.

The reason this is true is that in fact all the numbers occurring in the course of the Euclidean algorithm are so expressible. Indeed, we using the above example of the numbers 422 and 546, we have

$$\begin{aligned}
546 &= 422 \cdot 0 + 546 \cdot 1 \\
422 &= 422 \cdot 1 + 546 \cdot 0 \\
124 &= 422 \cdot (-1) + 546 \cdot 1 \\
50 &= 422 \cdot 4 + 546 \cdot (-3) \\
24 &= 422 \cdot (-9) + 546 \cdot 7 \\
2 &= 422 \cdot 22 + 546 \cdot (-17)
\end{aligned}$$

The first two equations here are obvious. Each of the other equations can be derived from the preceding two equations. To derive the fifth equation, for example, recall that 24 is the remainder when 50 is divided into 124. This is expressed by the equation,

$$124 = 2 \cdot 50 + 24,$$

saying that 2 is the quotient and 24 is the remainder of the division $124 \div 50$. 24 can be expressed from here as

$$24 = 124 - 50 \cdot 2,$$

where we found in convenient to change the order of the factors in the product. Taking the expression for 124 from the third and the expression for 50 from the fourth equation, we can now write this as follows:

$$24 = \big(422 \cdot (-1) + 546 \cdot 1\big) - \big(422 \cdot 4 + 546 \cdot (-3)\big) \cdot 2.$$

This can be algebraically simplified as

$$24 = 422 \cdot \big((-1) - 4 \cdot 2\big) + 546 \cdot \big(1 - (-3) \cdot 2\big).$$

If we carry out the operations indicated in the parentheses, we obtain

$$24 = 422 \cdot (-9) + 546 \cdot 7.$$

Thus we obtained the fifth equation from the third and fourth equations, as we promised we would do. The Euclidean algorithm performed with these additional calculations so that the greatest common divisor is obtained as a linear combination of the original numbers is called the *extended Euclidean algorithm.*

Problem

1. Using the extended Euclidean algorithm, find the greatest common divisors of the following pairs of numbers, and represent them as linear combinations of the given numbers: *a)* 14 and 25, *b)* 384 and 488, *c)* 645 and 242, *d)* 122 and 48, *e)* 735 and 141, *f)* 452 and 984.

3. The Fundamental Theorem of Arithmetic

An integer is a prime if it is greater than one and its only divisors are one and itself. The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31,.... It is not hard to see that every positive integer greater than one can be written as a product of primes. For example,

$$2599443 = 3 \cdot 3 \cdot 7 \cdot 11 \cdot 11 \cdot 11 \cdot 31.$$

The product on the right-hand side is called the *prime factorization* of the number on the left. The only other ways to write the number on the left as a product of primes to write the same primes in a different order; e.g.,

$$2599443 = 7 \cdot 3 \cdot 31 \cdot 11 \cdot 3 \cdot 11 \cdot 11,$$

but since changing the order of factors will not change the product, this prime factorization is not essentially different. The fact that a positive can be written only one way as a product of primes, aside from the order of factors is called the Fundamental Theorem of Arithmetic. It can formally be stated as

The Fundamental Theorem of Arithmetic. *The prime factorization of every integer greater than one is unique, aside from the order of factors.*

The key result needed in order to prove this is the following lemma, described by Euclid. Euclid, however, does not mention the Fundamental Theorem of Arithmetic itself; the Fundamental Theorem was first formulated and proved by the German mathematician Karl Friedrich Gauss in 1801, even though it had been used long before.

Lemma. *Let a and b be integers and let p be a prime. If ab is divisible by p then either a is divisible by p or b is divisible by p.*

Note that in mathematics, "or" is always used in the inclusive sense; that is, the possibility that both a and b are divisible by p is allowed. We will give a formal proof.

Proof. We will suppose that a and b are both positive (the case when a or b equals 0 can easily be dealt with, and when a or b is negative, it is harmless to consider their absolute values instead). Assume that a is not divisible by p; we will then have to show that b is divisible by p. With this assumption, we have $(a, p) = 1$. Indeed, p being a prime number, its only divisors are 1 and p. As we assumed that p is not a divisor of a, the greatest common divisor of a and p can only be one. As we saw above, this greatest common divisor can be represented as a linear combination. That is, we have integers x and y such that

$$1 = ax + py.$$

Multiplying both sides by b, we obtain

$$b = abx + pby.$$

Both terms on the right-hand side are divisible by p; indeed, our assumption was that ab is divisible by p. Hence the left-hand side, that is, b, is also divisible by p. This is what we wanted to show.

Note that it is easy to conclude from the above lemma a similar statement for the product of more than two integers. For example, if, for some integers, a, b, and c, and for some prime number p, the product abc is divisible by p, then either a or b or c is divisible by p. To see this, write $abc = (ab)c$. Then, by using the lemma, we can see that either ab or c is divisible by p. If now ab is divisible by p, then, using the lemma again, we can see that either a or b is divisible by p. Similarly for the product of four or more integers.

We can now use the above lemma, or, rather, its extension to a product of more than two factors, to present the

Proof of the Fundamental Theorem of Arithmetic. Assume, on the contrary, that there are positive ,integers with two different prime factorizations. Let n be the smallest such integer, and let its two different prime factorizations be

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l.$$

Note first that each of the primes p_i must be different from each of the primes q_j. Indeed, if, for example, we had $p_1 = q_1$ then the number

$$n/p_1 = p_2 p_3 \dots p_k = q_2 q_3 \dots q_l$$

would be a number smaller than n with two different prime factorizations, in contradiction with our assumption.

On the other hand, the equation above shows that the prime number p_1 is a divisor of the product $q_1 q_2 \dots q_l$. So, by the lemma above, or, rather, by its extension to more than two factors, at least one of the numbers q_1, q_2,... q_l, say q_j for a certain j with $1 \le j \le l$, must be divisible by p_1. As q_j is a prime, its only divisors are 1 and itself. As p_1, being a prime, is different from 1, we must have $p_1 = q_j$. This is a contradiction, since, as we stated above, p_1 must be different from q_j. This contradiction shows that our initial assumption was wrong; that is, there are no integers with two different prime factorizations.

The above method of proof, involving the consideration of the least positive integer with a certain property (i.e., the existence of two different prime factorizations, in the above example) to be disproved is called the *method of infinite descent*. It is a variant of *mathematical induction*.

Problems

1. You should be able to answer this question without doing any calculations(in fact, the numbers given are probably too big even for your calculator): Given that you know that

$$\begin{aligned} &7,324,472,493,949 \cdot 4,057,012,961,706 \\ &\quad = 13 \cdot 2,285,806,141,970,012,665,670,538 \end{aligned}$$

and

$$4,057,012,961,706 = 13 \cdot 312,077,920,131 + 3,$$

decide whether $7,324,472,493,949$ is divisible by 13. Give reasons; the correct reason is just as important as the correct answer. Do not waste your time by dividing 13 into $7,324,472,493,949$, since the answer can be given much more quickly by reasoning.

2. Using the second equation in Problem 1, determine the greatest common divisor 13 and $4,057,012,961,706$.

4. Solution to Problem 1 in Section 2

$a)$

$$\begin{aligned} 25 &= 14 \cdot 0 + 25 \cdot 1 \\ 14 &= 14 \cdot 1 + 25 \cdot 0 \\ 11 &= 14 \cdot (-1) + 25 \cdot 1 \\ 3 &= 14 \cdot 2 + 25 \cdot (-1) \\ 2 &= 14 \cdot (-7) + 25 \cdot 4 \\ 1 &= 14 \cdot 9 + 25 \cdot (-5) \end{aligned}$$

$b)$

$$\begin{aligned} 488 &= 384 \cdot 0 + 488 \cdot 1 \\ 384 &= 384 \cdot 1 + 488 \cdot 0 \\ 104 &= 384 \cdot (-1) + 488 \cdot 1 \\ 72 &= 384 \cdot 4 + 488 \cdot (-3) \\ 32 &= 384 \cdot (-5) + 488 \cdot 4 \\ 8 &= 384 \cdot 14 + 488 \cdot (-11) \end{aligned}$$

$c)$

$$\begin{aligned} 645 &= 242 \cdot 0 + 645 \cdot 1 \\ 242 &= 242 \cdot 1 + 645 \cdot 0 \\ 161 &= 242 \cdot (-2) + 645 \cdot 1 \\ 81 &= 242 \cdot 3 + 645 \cdot (-1) \\ 80 &= 242 \cdot (-5) + 645 \cdot 2 \\ 1 &= 242 \cdot 8 + 645 \cdot (-3) \end{aligned}$$

$d)$

$$\begin{aligned} 122 &= 48 \cdot 0 + 122 \cdot 1 \\ 48 &= 48 \cdot 1 + 122 \cdot 0 \\ 26 &= 48 \cdot (-2) + 122 \cdot 1 \\ 22 &= 48 \cdot 3 + 122 \cdot (-1) \\ 4 &= 48 \cdot (-5) + 122 \cdot 2 \\ 2 &= 48 \cdot 28 + 122 \cdot (-11) \end{aligned}$$

$e)$

$$\begin{aligned} 735 &= 141 \cdot 0 + 735 \cdot 1 \\ 141 &= 141 \cdot 1 + 735 \cdot 0 \\ 30 &= 141 \cdot (-5) + 735 \cdot 1 \\ 21 &= 141 \cdot 21 + 735 \cdot (-4) \\ 9 &= 141 \cdot (-26) + 735 \cdot 5 \\ 3 &= 141 \cdot 73 + 735 \cdot (-14) \end{aligned}$$

$f)$

$$\begin{aligned} 984 &= 452 \cdot 0 + 984 \cdot 1 \\ 452 &= 452 \cdot 1 + 984 \cdot 0 \\ 80 &= 452 \cdot (-2) + 984 \cdot 1 \\ 52 &= 452 \cdot 11 + 984 \cdot (-5) \\ 28 &= 452 \cdot (-13) + 984 \cdot 6 \\ 24 &= 452 \cdot 24 + 984 \cdot (-11) \\ 4 &= 452 \cdot (-37) + 984 \cdot 17 \end{aligned}$$