Number theory

Dr. Payman A. Rashed

Salahaddin University-Erbil

College of Basic Education

Department of Mathematics

Fourth Stage \ 2023-2024

Chapter one

Number theory

Number theory divided in to three branches as follow:

i- Elementary number theory
ii- Algebraic number theory
iii- Analytic number theory

The theory of numbers is concerned, at least in its elementary aspects, with properties of the integers and more particularly with the positive integers 1, 2, 3, ... (also known as the natural numbers). The origin of this misnomer harks back to the early Greeks for whom the word number meant positive integer, and nothing else. The natural numbers have been known to us for so long that the mathematician Leopold Kronecker once remarked, **"God created the natural numbers, and all the rest is the work of man."** Far from being a gift from Heaven, number theory has had a long and sometimes painful evolution, a story that is told in the ensuing pages. We shall make no attempt to construct the integers axiomatically, assuming instead that they are already given and that any reader of this book is familiar with many elementary facts about them. Among these is the Well-Ordering Principle, stated here to refresh the memory.

Definition1.1: Well-Ordering Principle.

Every nonempty set S of nonnegative integers contains a least element; that is, there is some integer a in S such that $a \leq b$ for all b's belonging to S.

Because this principle plays a critical role in the proofs here and in subsequent chapters, let us use it to show that the set of positive integers has what is known as the Archimedean property.

Theorem 1.2: Archimedean property.

If a and b are any positive integers, then there exists a positive integer n such that $na \geq b$. **Proof.** Assume that the statement of the theorem is not true,

so that for some a and b, $na < b$ for every positive integer n.

Then the set $S = \{b - na \mid n \text{ a positive integer}\}$ consists entirely of positive integers. By the Well-Ordering Principle, S will possess a least element, say, b - ma.

Notice that b - (m + l)a also lies in S, because S contains all integers of this form.

Furthermore, we have b - (m + l)a = (b - ma) - a < b - ma contrary to the choice of b - ma as the smallest integer in S.

This contradiction arose out of our original assumption that the Archimedean property did not hold; hence, this property is proven true.

Mathematical induction

With the Well-Ordering Principle available, it is an easy matter to derive the First Principle of Finite Induction, which provides a basis for a method of proof called mathematical induction. Loosely speaking, the First Principle of Finite Induction asserts that if a set of positive integers has two specific properties, then it is the set of all positive integers. To be less cryptic, we state this principle in Theorem 1.3.

Theorem 1.3: First Principle of Finite Induction.

Let S be a set of positive integers with the following properties:

(a) The integer 1 belongs to S.

(b) Whenever the integer k is in S, the next integer k + 1 must also be in S.

Then S is the set of all positive integers.

Here is a typical formula that can be established by mathematical induction:

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(2n+1)(n+1)}{6} \qquad (1)$$

for n = 1, 2, 3, ...

In anticipation of using Theorem 1.2, let S denote the set of all positive integers n for which Eq. (1) is true. We observe that when n = 1, the formula becomes

$$1^2 = \frac{1(2+1)(1+1)}{6} = 1$$

This means that 1 is in S. Next, assume that k belongs to S (where k is a fixed but unspecified integer) so that

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(2k+1)(k+1)}{6} \qquad (2)$$

To obtain the sum of the first k + 1 squares, we merely add the next one, (k + 1)2, to both sides of Eq. (2). This gives

$$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{k(2k+1)(k+1)}{6} + (k+1)^2$$

After some algebraic manipulation, the right-hand side becomes

$$(k+1)\left[\frac{k(2k+1)+6(k+1)}{6}\right] = (k+1)\left[\frac{2k^2+7k+6}{6}\right]$$
$$= \frac{(k+1)(2k+3)(k+2)}{6}$$

which is precisely the right-hand member of Eq. (1) when n = k + 1. Our reasoning shows that the set S contains the integer k + 1 whenever it contains the integer k. By Theorem 1.2, S must be all the positive integers; that is, the given formula is true for n = 1, 2, 3, ...

Although mathematical induction provides a standard technique for attempting to prove a statement about the positive integers, one disadvantage is that it gives no aid in formulating such statements. Of course, if we can make an "educated guess" at a property that we believe might hold in general, then its validity can often be tested by the induction principle. Consider, for instance, the list of equalities

$$1 = 1$$
$$1 + 2 = 3$$
$$1 + 2 + 2^2 = 7$$
$$1 + 2 + 2^2 + 2^3 = 15$$
$$1 + 2 + 2^2 + 2^3 + 2^4 = 31$$
$$1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 = 63$$

We seek a rule that gives the integers on the right-hand side. After a little reflection, the reader might notice that

$$1 = 2 - 1 \qquad 3 = 2^2 - 1 \qquad 7 = 2^3 - 1$$
$$15 = 2^4 - 1 \qquad 31 = 2^5 - 1 \qquad 63 = 2^6 - 1$$

expression $1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1}$; namely,

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^n - 1 \qquad (3)$$

for every positive integer n. (3) To confirm that our guess is correct, let S be the set of positive integers n for which Eq. (3) holds. For n = 1, Eq. (3) is certainly true, whence 1 belongs to the set S. We assume that Eq. (3) is true for a fixed integer k, so that for this k

$$1 + 2 + 2^2 + \cdots + 2^{k-1} = 2^k - 1$$

for every positive integer n.

To confirm that our guess is correct, let S be the set of positive integers n for which Eq. (3) holds. For $n = 1$, Eq. (3) is certainly true, whence 1 belongs to the set S. We assume that Eq. (3) is true for a fixed integer k, so that for this k

$$1 + 2 + 2^2 + \cdots + 2^{k-1} = 2^k - 1$$

and we attempt to prove the validity of the formula for $k + 1$. Addition of the term 2^k to both sides of the last-written equation leads to

$$\begin{aligned} 1 + 2 + 2^2 + \cdots + 2^{k-1} + 2^k &= 2^k - 1 + 2^k \\ &= 2 \cdot 2^k - 1 = 2^{k+1} - 1 \end{aligned}$$

But this says that Eq. (3) holds when n = k + 1, putting the integer k + 1 in S so that k + 1 is in S whenever k is in S. According to the induction principle, S must be the set of all positive integers. Mathematical induction is often used as a method of definition as well as a method of proof. For example, a common way of introducing the symbol n ! (pronounced "n factorial") is by means of the inductive definition

(a) $1! = 1$,
(b) $n! = n \cdot (n - 1)!$ for $n > 1$.

Binomial Theorem 1.4: For any positive integer n and any integer k satisfying 0 < k < n, the binomial coefficient defined by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

By canceling out either $k!$ or $(n-k)!$, $\binom{n}{k}$ can be written as

$$\binom{n}{k} = \frac{n(n-1)\cdots(k+1)}{(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

For example, with $n = 8$ and $k = 3$, we have

$$\binom{8}{3} = \frac{8!}{3!5!} = \frac{8\cdot 7\cdot 6\cdot 5\cdot 4}{5!} = \frac{8\cdot 7\cdot 6}{3!} = 56$$

Also observe that if $k = 0$ or $k = n$, the quantity $0!$ appears on the right-hand side of the definition of $\binom{n}{k}$; because we have taken $0!$ as 1, these special values of k give

$$\binom{n}{0} = \binom{n}{n} = 1$$

Theorem 1.5: (Pascal's Rule) For $1 \leq k \leq n$

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

The so-called *binomial theorem* is in reality a formula for the complete expansion of $(a+b)^n$, $n \geq 1$, into a sum of powers of a and b. This expression appears with great frequency in all phases of number theory, and it is well worth our time to look at it now. By direct multiplication, it is easy to verify that

$$(a+b)^1 = a + b$$
$$(a+b)^2 = a^2 + 2ab + b^2$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$
$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4, \text{ etc.}$$

This leads us to suspect that the general binomial expansion takes the form

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

or, written more compactly,

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

Mathematical induction provides the best means for confirming this guess. When $n = 1$, the conjectured formula reduces to

$$(a+b)^1 = \sum_{k=0}^{1}\binom{1}{k}a^{1-k}b^k = \binom{1}{0}a^1b^0 + \binom{1}{1}a^0b^1 = a + b$$

2- The Division Algorithm.

Theorem 2.1: Division Algorithm. Given integers a and b, with b > 0, there exist unique integers q and r satisfying a= qb + r , $0 \leq r < b$.

The integers q and r are called, respectively, the quotient and remainder in the division of a by b.

Corollary 2.2: If a and b are integers, with b ≠ 0, then there exist unique integers q and r such that a = qb + r, $0 \leq r < |b|$.

To illustrate the Division Algorithm when b < 0, let us take b = -7. Then, for the choices of a = 1, -2, 61, and -59, we obtain the expressions

$$\begin{aligned} 1 &= 0(-7) + 1 \\ -2 &= 1(-7) + 5 \\ 61 &= (-8)(-7) + 5 \\ -59 &= 9(-7) + 4 \end{aligned}$$

Remark: We wish to focus our attention on the applications of the Division Algorithm, and not so much on the algorithm itself. As a first illustration, note that with b = 2 the possible remainders are r = 0 and r = 1.

When r = 0, the integer a has the form a = 2K and is called even; when r = 1, the integer a has the form a = 2K + 1 and is called odd, for some k.

Example-1: a^2 is either of the form $(2q)^2 = 4k$ or $(2q + 1)^2 = 4(q^2+q)+1 = 4k + 1$. The point to be made is that the square of an integer leaves the remainder 0 or 1 upon division by 4. We also can show the following: the square of any odd integer is of the form 8k + 1. For, by the division Algorithm, any integer is representable as one of the four forms: 4q, 4q + 1, 4q + 2, 4q + 3. In this classification, only those integers of the forms 4q + 1 and 4q + 3 are odd. When the latter are squared, we find that

$(4q + 1)^2 = 8(2q^2 + q) + 1 = 8k + 1$ and similarly

$(4q + 3)^2 = 8(2q^2 + 3q + 1) + 1 = 8k +1$

As examples, the square of the odd integer 7 is $7^2 = 49 = 8 \cdot 6 + 1$, and the square of 13 is $13^2 = 169 = 8 \cdot 21 + 1$.

3- THE GREATEST COMMON DIVISOR

Definition 3.1: An integer b is said to be divisible by an integer $a \neq 0$, in symbols a | b, if there exits some integer c such that b = ac.

We write a ∤ b to indicate that b is not divisible by a.

Example -2:

(1) 3 | 12,

(2) 3 ∤ 10.

Theorem 3.2. For integers a, b, c, d, the following hold:

1. a | 0, 1 | a, a | a.

2. a | 1 if and only if $a = \pm 1$.

3. If a | b and c | d, then ac | bd.

4. If a | b and b | c, then a | c.

5. a | b and b | a if and only if $a = \pm b$.

6. If a | b and $b \neq 0$, then $|a| \leq |b|$.

7. If a | b and a | c, then a | (bx + cy) for arbitrary integers x and y.

Definition 3.3: If a and b are arbitrary integers, then an integer d is said to be a common divisor of a and b if both d | a and d | b.

Definition 3.4: Let a and b be given integers, with at least one of them different form zero. The greatest common divisor of a and b, dented by gcd(a, b), is the positive integer d satisfying

1. d | a and d | b,

2. if c | a and c | b, then $c \leq d$.

Example-3: The positive divisors of −12 are 1, 2, 3, 4, 6, 12, while those of 30 are 1, 2, 3, 5, 6, 10, 15, 30, hence, the positive common divisors of −12 and 30 are 1, 2, 3, 6. Since 6 is the largest of these integers, it follows that

gcd(−12, 30) = 6.

Example -4: gcd(−5, 5) = 5,

gcd(8, 15) = 1, and gcd(−8, −36) = 4.

Theorem 3.4: Given integers a and b, not both of which are zero, there exist integers x and y such that gcd(a, b) = ax + by.

Corollary 3.5: If a and b are given integers, not both zero, then the set T = {ax + by | x, y are integers} is precisely the set of all multiples of d = gcd(a, b).

Example -5:

gcd(−12, 30) = 6 = (−12) · 2 + (30) · 1,

gcd(−8, −36) = 4 = (−8) · 4 + (−36) · (−1).

Definition 3.5: Two integers a and b, not both of which are zero, are said to be relatively prime whenever gcd(a, b) = 1.

Example -6: Since gcd(8, 15) = 1, then 8 and 15 are relatively prime.

Definition 3.6: Two integers a and b, not both of which are zero, are said to be relatively prime whenever gcd(a, b) = 1.

Theorem 3.7: Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that 1 = ax + by.

Corollary 3.8: If gcd(a, b) = d, then gcd(a/d, b/d) = 1.

Example-7: gcd(−12, 30) = 6

and gcd(−12/6, 30/6) = gcd(−2, 5) = 1.

Remark: It is not true, without adding an extra condition, that a | c and b | c together give ab | c.

For instance, 10 | 30 and 15 | 30, but 10·15 ∤ 30.

Corollary 3.9: If a | c and b | c, with gcd(a, b) = 1, then ab | c.

Theorem 3.10: (Euclid's Lemma)

If a | bc, with gcd(a, b) = 1, then a | c.

Proof: We start again from Theorem 3.4, writing 1 = ax + by, where x and y are integers.

Multiplication of this equation by e produces

$e = 1 \cdot e = (ax + by)e = aex + bey$

Because $a \mid ae$ and $a \mid be$, it follows that $a \mid (aex + bey)$, which can be recast as $a \mid e$.

Remark: If a and b are not relatively prime, then the conclusion of Euclid's Lemma may fail to hold.

Example-8: $10 \mid 5 \cdot 6$ but $10 \nmid 5$ and $10 \nmid 6$.

$12 \mid 9 \cdot 8$, but $12 \mid 9$ and $12 \mid 8$.

Theorem 3.11: Let a, b be integers, not both zero, for a positive integer d, d = gcd(a, b) if and only if

1. d | a and d | b,

2. whenever c | a and c | b, then c | d.

The Euclidean algorithm

The Euclidean Algorithm may be described as follows: Let a and b be two integers whose greatest common divisor is desired. Because gcd(|a|, |b|)= gcd(a, b), there is no harm in assuming that a> b > 0.

The first step is to apply the Division Algorithm to a and b to get $a = q_1 b + r_1$, $0 \leq r_1 < b$

If it happens that $r_1 = 0$, then $b \mid a$ and gcd(a, b) = b.

When $r_1 \neq 0$, divide b by r_1 to produce integers q2 and r2 satisfying $b = q_2 r_1 + r_2$,

$0 \leq r_2 < r_1$ If $r_2 = 0$, then we stop; otherwise, proceed as before to obtain

$$r_1 = q_3 r_2 + r_3 \qquad 0 \le r_3 < r_2$$

The result is the following system of equations:

$$\begin{aligned}
a &= q_1 b + r_1 && 0 < r_1 < b \\
b &= q_2 r_1 + r_2 && 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 && 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

We argue that r_n, the last nonzero remainder that appears in this manner, is equal to gcd(a, b). Our proof is based on the lemma below.

Lemma 3.12: If a = qb + r, then gcd(a, b) = gcd(b, r).

Proof. If $d = \gcd(a, b)$, then the relations $d \mid a$ and $d \mid b$ together imply that $d \mid (a - qb)$, or $d \mid r$. Thus, d is a common divisor of both b and r. On the other hand, if c is an arbitrary common divisor of b and r, then $c \mid (qb + r)$, whence $c \mid a$. This makes c a common divisor of a and b, so that $c \le d$. It now follows from the definition of $\gcd(b, r)$ that $d = \gcd(b, r)$.

Using the result of this lemma, we simply work down the displayed system of equations, obtaining

$$\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$$

Starting with the next-to-last equation arising from the algorithm, we write

$$r_n = r_{n-2} - q_n r_{n-1}$$

Now solve the preceding equation in the algorithm for r_{n-1} and substitute to obtain

$$\begin{aligned}
r_n &= r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) \\
&= (1 + q_n q_{n-1}) r_{n-2} + (-q_n) r_{n-3}
\end{aligned}$$

This represents r_n as a linear combination of r_{n-2} and r_{n-3}. Continuing backward through the system of equations, we successively eliminate the remainders r_{n-1}, $r_{n-2}, \ldots, r_2, r_1$ until a stage is reached where $r_n = \gcd(a, b)$ is expressed as a linear combination of a and b.

Example: Let us see how the Euclidean Algorithm works in a concrete case by calculating, say, gcd(12378, 3054). The appropriate applications of the Division Algorithm produce the equations

$$\begin{aligned} 12378 &= 4 \cdot 3054 + 162 \\ 3054 &= 18 \cdot 162 + 138 \\ 162 &= 1 \cdot 138 + 24 \\ 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0 \end{aligned}$$

Our previous discussion tells us that the last nonzero remainder appearing in these equations, namely, the integer 6, is the greatest common divisor of 12378 and 3054:

6 = gcd(12378,3054).

To represent 6 as a linear combination of the integers 12378 and 3054, we start with the next-to-last of the displayed equations and successively eliminate the remainders

18, 24, 138, and 162:

$$\begin{aligned} 6 &= 24 - 18 \\ &= 24 - (138 - 5 \cdot 24) \\ &= 6 \cdot 24 - 138 \\ &= 6(162 - 138) - 138 \\ &= 6 \cdot 162 - 7 \cdot 138 \\ &= 6 \cdot 162 - 7(3054 - 18 \cdot 162) \\ &= 132 \cdot 162 - 7 \cdot 3054 \\ &= 132(12378 - 4 \cdot 3054) - 7 \cdot 3054 \\ &= 132 \cdot 12378 + (-535)3054 \end{aligned}$$

Thus we have 6 = gcd(l2378, 3054) = 12378x + 3054y

where x = 132 and y = -535. Note that this is not the only way to express the integer 6 as a linear combination of 12378 and 3054; among other possibilities, we could add and subtract 3054 · 12378 to get

6 = (132 + 3054)12378 + (-535 - 12378)3054 = 3186. 12378 + (-12913)3054

Theorem 3.13: If k > 0, then gcd(ka, kb)= k gcd(a, b).

Proof. If each of the equations appearing in the Euclidean Algorithm for a and b is multiplied by k, we obtain

But this is clearly the Euclidean Algorithm applied to the integers ak and bk, so that their greatest common divisor is the last nonzero remainder $r_n k$; that is,

$$\gcd(ka, kb) = r_n k = k \gcd(a, b)$$

$$\begin{aligned}
ak &= q_1(bk) + r_1 k & 0 < r_1 k < bk \\
bk &= q_2(r_1 k) + r_2 k & 0 < r_2 k < r_1 k \\
&\vdots \\
r_{n-2}k &= q_n(r_{n-1}k) + r_n k & 0 < r_n k < r_{n-1}k \\
r_{n-1}k &= q_{n+1}(r_n k) + 0
\end{aligned}$$

But this is clearly the Euclidean Algorithm applied to the integers ak and bk, so that their greatest common divisor is the last nonzero remainder $r_n k$; that is,

$$\gcd(ka, kb) = r_n k = k \gcd(a, b)$$

as stated in the theorem.

Corollary 3.14: For any integer k ≠0, gcd(ka, kb)= $|k|$ gcd(a, b).

Proof: It suffices to consider the case in which k<0.

Then -k = I k I > 0 and, by Theorem 3.13

$$\begin{aligned}
\gcd(ak, bk) &= \gcd(-ak, -bk) \\
&= \gcd(a\,|k|, b\,|k|) \\
&= |k| \gcd(a, b)
\end{aligned}$$

,

For example gcd(l2, 30) = 3 gcd(4, 10) = 3 · 2 gcd(2, 5) = 6 · 1 = 6

Definition 3.15: The least common multiple of two nonzero integers a and b, denoted by lcm(a, b), is the positive integer m satisfying the following:

(a) a │m and b │m.

(b) If a │ c and b │ c, with c > 0, then m ≤ c.

As an example, the positive common multiples of the integers -12 and 30 are 60, 120, 1 80, ... ; hence, lcm(-12, 30) = 60. The following remark is clear from our discussion: given nonzero integers a and b, lcm(a, b) always exists and lcm(a, b) < I ab I. We lack a relationship between the ideas of greatest common divisor and least common multiple. This gap is filled by the following theorem.

Theorem 3.16: For positive integers a and b gcd(a, b) lcm(a, b) =ab

Proof. To begin, put $d = \gcd(a, b)$ and write $a = dr$, $b = ds$ for integers r and s. If $m = ab/d$, then $m = as = rb$, the effect of which is to make m a (positive) common multiple of a and b.

Now let c be any positive integer that is a common multiple of a and b; say, for definiteness, $c = au = bv$. As we know, there exist integers x and y satisfying $d = ax + by$. In consequence,

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax + by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = vx + uy$$

This equation states that $m \mid c$, allowing us to conclude that $m \leq c$. Thus, in accordance with Definition 2.4, $m = \text{lcm}(a, b)$; that is,

$$\text{lcm}(a, b) = \frac{ab}{d} = \frac{ab}{\gcd(a, b)}$$

which is what we started out to prove.

Corollary3.17: For any choice of positive integers a and b, lcm(a, b) = ab if and only if gcd(a, b) = 1.

Perhaps the chief virtue of Theorem we found that gcd(3054, 12378) = 6; whence,

$$\text{lcm}(3054, 12378) = \frac{3054 \cdot 12378}{6} = 6300402$$

Remark: In the case of three integers, a, b, c, not all zero, gcd(a, b, c) is defined to be the positive integer d having the following properties:

(a) d is a divisor of each of a, b, c.

(b) If e divides the integers a, b, c, then e $\leq$ d.

We cite two examples: gcd(39, 42, 54) = 3 and 31 gcd(49, 210, 350) = 7

The reader is cautioned that it is possible for three integers to be relatively prime as a triple (in other words, gcd(a, b, c) = 1), yet not relatively prime in pairs; this is brought out by the integers 6, 10, and 15.

4-**THE DIOPHANTINE EQUATION ax +by = c**

Definition 4.1: Any equation in one or more unknowns which is to be solved in integers is called **Diophantine equation.**

The linear Diophantine equation in two unknowns is of the form ax + by = c, where a, b, c are given integers and a, b not both zero.

A solution of this equation is a pair of integers x_0, y_0 which satisfy it.

Example -1: The equation 3x + 6y = 18 has solutions

3.4 + 6.1 = 18,

3(−6) + 6.6 = 18,

3.10 + 6(−2) = 18

Theorem 4.2: The linear Diophantine equation ax + by = c has a solution if and only if d | c, where d = gcd(a, b). If x_o, y_o is any particular solution of this equation, then all other solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)t \qquad y = y_0 - \left(\frac{a}{d}\right)t$$

where t is an arbitrary integer.

Example -2: Solve the linear Diophantine equation 172x + 20y = 1000.

Applying the Euclidean's Algorithm to the evaluation of gcd(172, 20), we find that

$$\begin{aligned} 172 &= 8 \cdot 20 + 12 \\ 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 \end{aligned}$$

whence gcd(172, 20) = 4. Because 4 | 1000, a solution to this equation exists. To obtain the integer 4 as a linear combination of 172 and 20, we work backward through the previous calculations, as follows:

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2 \cdot 12 - 20 \\ &= 2(172 - 8 \cdot 20) - 20 \\ &= 2 \cdot 172 + (-17)20 \end{aligned}$$

Upon multiplying this relation by 250, we arrive at

$$\begin{aligned} 1000 = 250 \cdot 4 &= 250[2 \cdot 172 + (-17)20] \\ &= 500 \cdot 172 + (-4250)20 \end{aligned}$$

so that $x = 500$ and $y = -4250$ provide one solution to the Diophantine equation in question. All other solutions are expressed by

$$\begin{aligned} x &= 500 + (20/4)t = 500 + 5t \\ y &= -4250 - (172/4)t = -4250 - 43t \end{aligned}$$

for some integer t.

Corollary 4.3: If gcd(a, b) = 1 and if x_o, y_o is a particular solution of the linear Diophantine equation ax + by = c, then all solutions are given by

$x = x_0 + bt$ $\quad$ $y = y_o - at$ $\quad$ for integral values of t.

Here is an example. The equation $5x + 22y = 18$ has $x_0 = 8$, $y_0 = -1$ as one solution; from the corollary, a complete solution is given by $x = 8 + 22t$, $y = -1 - 5t$ for arbitrary t.