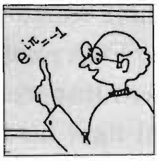
Classroom



In this section of* Resonance*, we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

Dinesh Khurana
Department of Mathematics
Panjab University
Chandigarh 160014, India.
Email: dkhurana@pu.ac.in

On GCD and LCM in Domains — A Conjecture of Gauss

By an integral domain (or simply by a domain) D, one shall mean a commutative ring with identity in which the product of two non-zero elements is not zero. The ring of integers $\mathbb{Z}$, the field of rational numbers $\mathbb{Q}$ (or any field) are some examples of domains. The ring $A[X]$ of all polynomials in a variable X with coefficients in any commutative ring A is itself a commutative ring; it is a domain if, and only if, A is a domain. On the other hand, the commutative ring of integers modulo 4 (or, more generally, any nonprime) under addition and multiplication modulo 4 is not a domain. For instance, in this ring, the product of 2 with itself is the zero element. A class of domains occurring in modern number theory is the class of rings $\mathbb{Z}[\sqrt{d}]$; this consists of all complex numbers of the form $a+b\sqrt{d}$, where a, b are integers and d is any fixed integer (positive or negative) which is not a perfect square and $\sqrt{d}$ is a fixed square root of d in $\mathbb{C}$. When $d = -1$, one calls this the ring of Gaussian integers denoted by $\mathbb{Z}[i]$ where i is a fixed square root of -1 in $\mathbb{C}$. The Gaussian ring $\mathbb{Z}[i]$ is, for instance, used to prove that every prime number of the form $4n + 1$ is a sum of two squares of integers. One major difference between the familiar ring $\mathbb{Z}$ of integers and such gen-

This article arose out of Classroom discussions with the BSc Final year students.

eral domains is that factorisation becomes a nontrivial point. For instance, the prime number 2 is a product $(1+i)(1-i)$ in $\mathbb{Z}[i]$ and one needs to look closely as to whether 2 – when considered as an element in $\mathbb{Z}[i]$ – has properties that a prime number has. Indeed, a major aim of algebraic number theory is to understand how usual prime numbers *factorise* in such *general number rings*. To clarify these issues, let us look at the familiar concept of GCD (greatest common divisor) and of LCM (least common multiple).

A major aim of algebraic number theory is to understand how usual prime numbers factorise in such general number rings.

If a, b are two nonzero elements of a domain D, then GCD of a and b, denoted by (a, b), is defined to be a common divisor of a and b which is divisible by any other common divisor of a and b. Here and elsewhere, one says a divides b in D to mean that $b = ac$ for some $c \in D$. The point to note is that there is no guarantee that two given elements do indeed possess such a GCD. Analogously, LCM of a and b, denoted by $[a, b]$, is a common multiple of a and b which divides any other common mutiple of a and b. In fact, the aim here is to clarify what the existence of GCD or LCM entails. First, we note a simple but important point viz., that for two integers, say 4 and 6, one could take their GCD to be 2 or one could take it to be -2. After all both 2 and -2 satisfy the definition. Here there are only two equally-valid candidates for the GCD and they are negatives of each other. The reason is that 1 and -1 are the only integers which are *units* i.e., have multiplicative inverses which are again integers. Thus, for any domain D, one defines a *unit in D* to be an element a such that there is a corresponding element a' in D so that $aa' = 1$. Thus, in the familiar ring of integers, a prime number p would have only the factors $1, p, -1, -p$. The prime numbers can also be characterized by the equivalent property that if p divides a product ab, then p must divide one of them. However, as it turns out, for a general domain, these two properties may not be equivalent. In a domain D, one calls two elements a and b *associates* if $a = bu$ for some unit u in D. One defines a nonzero, non-unit element a to be an *irreducible element* if, whenever $a = bc$ in D, either b or c is a unit. Therefore, the only divisors of an irreducible element a are units and the associates of a. Further, a nonzero non-unit element p of a domain is called a *prime element* if, whenever p divides a product of two elements it divides at least one of the two.

The main reason for Fermat's last theorem not being an elementary exercise is that for some prime numbers p, the ring generated by $e^{2i\pi/p}$ may not be a UFD.

We first observe:

In any domain D, a prime element is always irreducible.

Indeed, if p is a prime element and a divides p, then $p = ab$, for some b. Thus either p divides a or p divides b. Now if $a = pc$, then $p = pcb$ and so b is a unit. Similarily if p divides b then a is a unit. This shows that p is irreducible.

But the converse may not be true. For instance, in the ring $\mathbb{Z}[\sqrt{-3}]$, the element 2 is irreducible but not prime; the last paragraph of this note has a proof. The fundamental theorem of arithmetic asserts that every nonzero nonunit integer is a product of prime powers uniquely, up to ordering and sign. Once again, this property does not hold for general domains. A domain is called a *unique factorization domain* (UFD) if every nonzero nonunit element can be written as a product of irreducible elements and the product is unique upto associates i.e., if

$$a = \prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i,$$

where p_i and q_i are irreducible elements, then $m = n$ and there exists a permutation σ on $\{1, 2, ..., n\}$ such that p_i and $q_{\sigma(i)}$ are associates. The main reason for Fermat's last theorem not being an elementary exercise is that for some prime numbers p, the ring generated by $e^{2i\pi/p}$ may not be a UFD. The ring here consists of all the numbers

$$a_0 + a_1 e^{2i\pi/p} + a_2 e^{4i\pi/p} + \quad + a_{p-2} e^{2(p-2)i\pi/p},$$

where $a_i \in \mathbb{Z}$.

Gauss proved the famous theorem that if D is any UFD, then so is $D[X]$. In a UFD, any two elements have GCD as well as LCM. To see this, look at the irreducible factorizations of two elements a and b;

$$a = \prod_{i=1}^{r} l_i^{k_i}, \qquad b = \prod_{j=1}^{s} q_j^{m_j},$$

where l_i are distinct irreducible elements and q_j are also distinct irreducible elements. We may write both of these in the form

$$a = \prod_{i=1}^{r} p_i^{n_i}, \qquad b = \prod_{i=1}^{r} p_i^{m_i},$$

where p_i are distinct irreducible elements and some of the exponents n_i, m_i may be zero. Then $\prod_{i=1}^{n} p_i^{\alpha_i}$ is clearly their GCD (a, b) and $\prod_{i=1}^{n} p_i^{\beta_i}$ is their LCM $[a, b]$, where α_i and β_i, respectively, are minimum and maximum of n_i and m_i. We note the simple but important point that:

In a UFD every irreducible element is prime. In other words, the two concepts coincide.

Indeed, if p is irreducible and $p|ab$, say $ab = pc$, then either p is an associate of some irreducible divisor of a or an associate of some irreducible divisor of b. So p either divides a or b.

A suitable reference for the above discussion would be [1]. During discussions with an undergraduate class of algebra, the following questions arose:

Q1. *Does the existence of GCD of two elements in a domain imply the existence of their LCM?*

In each $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$ not a perfect square, we show the existence of two elements which have a GCD but fail to have an LCM.

Q2. *Does the existence of LCM of two elements in a domain imply the existence of their GCD?*

We observed the interesting fact that while the answer to the second question is in the affirmative, the answer to the first one is in the negative. In fact, we show the existence of two elements in each $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$ not a square, which have a GCD but fail to have an LCM. As we observed above that in a UFD any two elements have an LCM, it follows immediately that $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$ is not a UFD. It is well known that $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$ are UFDs (in fact, they are even Euclidean domains i.e., have a Euclidean division algorithm like $\mathbb{Z}$). In $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$, we also use the proof to exhibit an irreducible element which is not prime. This again reproves that $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$, is not a UFD. Stark ([2], Theorem 8.25) proves this result but our proof is more elementary. A short proof that $\mathbb{Z}[\sqrt{-d}]$ is not a Euclidean domain when $d > 2$ and $-d \equiv 2$ *or* 3(mod 4) may also be found in [3].

Before going into our proof, we point out an important fact. We remarked that in number theory, one studies the rings $\mathbb{Z}[\sqrt{d}]$ for square-free d. Note that any element of this ring is $u = a + b\sqrt{d}$ which is a root of the polynomial $(X - a)^2 - db^2$; this is a polynomial which has integer coefficients and is monic (i.e., has top coefficient 1). Such complex numbers go under the name of *algebraic integers.* Thus, elements of $\mathbb{Z}[\sqrt{d}]$ are algebraic integers. However, in number theory one actually needs to study the set of *all* the algebraic integers in a particular number field like $\mathbb{Q}[\sqrt{d}]$. In $\mathbb{Q}[\sqrt{d}]$, which consists of all complex numbers of the form $s + t\sqrt{d}$ with s, t rational numbers, the ring of all algebraic integers may be larger than $\mathbb{Z}[\sqrt{d}]$. For instance, for $d = -3$, the number $\frac{1}{2} + \frac{\sqrt{-3}}{2}$ is also an algebraic integer. Indeed, the ring of algebraic integers in $\mathbb{Q}[\sqrt{d}]$ is $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[(d + \sqrt{d})/2]$ according as whether $d \equiv 2$ or 3 mod 4 or as $d \equiv 1$ mod 4. One calls the set of all algebraic integers in $K = \mathbb{Q}[\sqrt{d}]$ the *ring of integers of* K. It was proved by Gauss that the ring of integers of quadratic field $\mathbb{Q}[\sqrt{-d}]$ is a UFD for $d = 1, 2, 3, 7, 11, 19, 43, 67$ and 163 (see e.g., [2], Theorem 8.22). Gauss also conjectured that for no other positive squarefree d is the ring of integers of $\mathbb{Q}[\sqrt{-d}]$ a UFD. This conjecture was proved, after about 150 years, in 1966 by Baker [4] and Stark [5] independently. As the ring of integers of $\mathbb{Q}[\sqrt{-d}]$ is $\mathbb{Z}[\sqrt{-d}]$ if $d \equiv 2$ or $3 (\text{mod } 4)$, so an elementary proof of Gauss conjecture in these two cases follows.

It was proved by Gauss that the ring of integers of quadratic field $\mathbb{Q}[\sqrt{-d}]$ is a UFD for $d = 1, 2, 3, 7, 11, 19, 43, 67$ and 163

During the rest of the discussion, by "$a \in D$" we shall mean that a is a non-zero element of D.

Lemma 1 *Let $a, b, r \in D$. If (ra, rb) exists then (a, b) exists and $r(a, b) = (ra, rb)$.*

Proof As r divides both ra, rb, $g = (ra, rb)/r$ is in D. Now as (ra, rb) divides ra and rb, g divides a and b. Now if d divides a and b, then dr divides ar and br and thus dr divides (ar, br). This implies that d divides $(ar, br)/r$. ■

The following result, in particular, answers Q2 in the affirmative.

Theorem 2 *Let $a, b \in D$. Then $[a, b]$ exists if and only if (ra, rb) exists for all $r \in D$.*

Proof Suppose $[a, b]$ exists. We show that $d := ab/[a, b]$ equals (a, b). As $a = d[a, b]/b$ and $b = d[a, b]/a$, d divides both a and b. Now suppose that h is a common divisor of a and b. Now as a, b both divide ab/h, $[a, b]$ divides ab/h which implies that h divides $ab/[a, b] = d$. Thus if $[a, b]$ exist then so does (a, b) and equals $ab/[a, b]$.

Now we show that if $[a, b]$ exists then so does $[ra, rb]$ for all in D. First note that ra, rb both divide $r[a, b]$. Now suppose m is a common multiple of ra, rb. Then r divides m and a, b both divide m/r. Thus $[a, b]$ divides m/r and so $r[a, b]$ divides m. Thus $[ra, rb] = r[a, b]$.

Now, we show that if (ra, rb) exists for all r, then $[a, b]$ exists and equals $l := ab/(a, b)$. Clearly a, b both divide l. Now suppose a, b both divide m. Then ab is a common divisor of ma and mb and so ab divides $(ma, mb) = m(a, b)$ by Lemma 1. This implies that $ab/(a, b)$ divides m. ■

The proof of Theorem 2 gives the following

Corollary 3 *If* $[a, b]$ *exists then* (a, b) *exists and* $[a, b](a, b) = ab$.

Theorem 4 *In each* $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$ *a nonsquare integer, there exist two elements* a, b *such that* (a, b) *exists but* $[a, b]$ *does not exist. In particular,* $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$ *nonsquare, is not a UFD.*

Proof First suppose that $d + 1$ is not a prime number. Let $d + 1 = pk$, where p is a prime and $k \geq 2$. Clearly $a^2 + db^2 \neq p$ for any $a, b \in \mathbb{Z}$ because the left hand side is bigger than p if $b \neq 0$. If $p = (a + b\sqrt{-d})(u + v\sqrt{-d})$ in $\mathbb{Z}[\sqrt{-d}]$, then taking complex conjugates we see that $u = a, v = -b$. Thus, $p = a^2 + db^2$, which is impossible as observed above. Therefore, p is an irreducible element in $\mathbb{Z}[\sqrt{-d}]$. Also p does not divide $1 + \sqrt{-d}$ because $p(a+b\sqrt{-d}) = 1+\sqrt{-d}$ gives $pa = 1$ which is impossible. Thus, $(p, 1 + \sqrt{-d})$ exists and equals 1. We shall show that $(pk, (1 + \sqrt{-d})k)$ does not exist. If it did, then by Lemma 1, $(pk, (1 + \sqrt{-d})k) = k$. Then as $1 + \sqrt{-d}$ divides $pk = 1 + d$ and $(1 + \sqrt{-d})k$, $1 + \sqrt{-d}$ divides k. Let $k = (1 + \sqrt{-d})(a + b\sqrt{-d}) = (a - bd) + (a + b)\sqrt{-d}$. This gives $a = -b$ and $a - bd = a + ad = k$. Thus $apk = a(1 + d) = k$ which is a contradiction. In view of Theorem 2, it follows that $[p, 1 + \sqrt{-d}]$ does not exist.

Now suppose that $d + 1$ is a prime. Then d and $d + 4$ are even integers. Let $d + 4 = 2k$, for some $k > 1$. As above, one easily checks that 2 is irreducible and 2 does not divide $2 + \sqrt{-d}$. Thus $(2, 2 + \sqrt{-d})$ exists and equals 1. We show that $(2k, (2 + \sqrt{-d})k)$ does not exist.

If it did, then as above, $2+\sqrt{-d}$ divides k and which in turn implies that $4+d$ divides $k=(4+d)/2$ in $\mathbb{Z}$. This contradiction shows by Theorem 2 that $[2, 2+\sqrt{-d}]$ does not exist. ■

In the proof of Theorem 4, note that when $d+1=pk$, p divides $d+1=(1+\sqrt{-d})(1-\sqrt{-d})$ but p clearly does not divide either of $1+\sqrt{-d}$ and $1-\sqrt{-d}$, showing that p, which is irreducible, is not prime. Similarly in the second part of the proof, 2 divides $d+4=(2+\sqrt{-d})(2-\sqrt{-d})$ but does not divide either of them, which shows that 2 is not prime. This also proves that $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$ nonsquare, is not a UFD.

Suggested Reading

[1] J B Fraleigh, *A first course in Abstract Algebra*, Addison Wesley ublishing Company, Inc, USA 1982.

[2] H M Stark, *An Introduction to Number Theory*, Markham ublishing Company, Chicago 1970.

[3] S Singh, Non-Euclidean domains: An Example, *Mathematics Magazine*, 49,p. 243, 1976.

[4] A Baker, Linear forms in the logarithms of algebraic numbers, *Mathematika*, 13, pp. 204-216, 1996.

[5] A complete determination of the complex quadratic fields of class-number one, *Michigan Math. J.*, 14, pp. 1-27, 1967.

The chess-board is the world; the pieces are the phenomena of the universe; the rules of the game are what we call the laws of Nature. The player on the other side is hidden from us. We know that his play is always fair, and patient. But also we know, to our cost, that he never overlooks a mistake, or makes the smallest allowance for ignorance.

Thomas Henry Huxley
(1825-95) English Biologist