The Carus Mathematical Monographs

NUMBER NINE

THE THEORY OF ALGEBRAIC NUMBERS

HARRY POLLARD
Cornell University

Published by
THE MATHEMATICAL ASSOCIATION OF AMERICA
Distributed by
JOHN WILEY AND SONS, INC.

To H. M. P.

PREFACE

The purpose of this monograph is to make available in English the elementary parts of classical algebraic number theory. An earlier version in mimeographed form was used at Cornell University in the spring term of 1947–48, and the present version has accordingly profited from the criticisms of several readers. I am particularly indebted to Miss Leila R. Raines for her painstaking assistance in the revision and preparation of the manuscript for publication.

HARRY POLLARD

CONTENTS

Chapter I

DIVISIBILITY

1. **Uniqueness of factorization.** Elementary number theory has for its object the study of the integers 0, ± 1, ± 2, $\cdots$. Certain of these, the *prime* numbers, occupy a special position; they are the numbers m which are different from 0 and ± 1, and which possess no factors other than ± 1 and $\pm m$. For example $2, 3, -5$ are prime, whereas $6 = 2 \cdot 3$, $9 = 3^2$ are not. The importance of the primes is due to the fact that, together with 0 and ± 1, all the other integers can be constructed from them. The fundamental theorem of arithmetic asserts that *every integer greater than* 1 *can be factored in one and only one way, apart from order, as the product of positive prime numbers.* Thus

$$12 = 2^2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2^2$$

are the only factorizations of 12 into positive prime factors, and these factorizations all yield precisely the same factors; the only difference among them is in the order of appearance of the factors.

We shall give a proof of the fundamental theorem of arithmetic. In the course of it the following fact will play a decisive role: every collection, finite or infinite, of non-negative integers contains a smallest one. The validity of this assumption will not be debated here; it is certainly clear intuitively, and the reader may take it to be one of the defining properties of integers. Some preliminary theorems will be established first.

Theorem 1.1. *If a and b are integers, $b > 0$, then there exist integers q and r such that*

$$a = bq + r,$$

where $0 \leq r < b$. The integers q and r are unique.

Consider the rational number $\frac{a}{b}$ and let q be the largest integer which does not exceed it. Then $q \leq \frac{a}{b}$, but $q+1 > \frac{a}{b}$. Define r as $a - bq$. Since $\frac{r}{b} = \frac{a}{b} - q \geq 0$, and $b > 0$, it follows that $r \geq 0$. Also from $1 > \frac{a}{b} - q = \frac{a - bq}{b} = \frac{r}{b}$ we conclude that $r < b$.

To show that q and r are unique suppose that q' and r' is any pair of integers for which

$$a = bq' + r', \qquad 0 \leq r' < b.$$

If $q' > q$, then $q' \geq q + 1$, so that

$$r' = a - bq' \leq a - b(q+1) = r - b < 0;$$

this contradicts $r' \geq 0$. If $q' < q$, then $q \leq q - 1$, so that

$$r' = q - bq' \geq a - b(q-1) = r + b \geq b;$$

this contradicts $r' < b$.

Then both possibilities $q' > q$, $q' < q$ are ruled out. It follows that $q' = q$, and hence that $r' = r$. This completes the proof of Theorem 1.1.

We shall say that two integers a and b are *relatively prime* if they share no factors except ± 1. Thus 5 and 9 are relatively prime, whereas 6 and 9 are not.

THEOREM 1.2. *If a and b are relatively prime then there exist integers s and t for which $as + bt = 1$.*

Observe that there is no assertion about the uniqueness of s and t. In fact if $a = 3$, $b = 5$ we have

$$2 \cdot 3 - 1 \cdot 5 = 1, \qquad -3 \cdot 3 + 2 \cdot 5 = 1.$$

To prove the theorem note first that neither a nor b can be zero. Consider the set of all numbers of the form

$ax + by$, where x and y are integers. If we choose $x = 1$, $y = 0$, and then $x = -1$, $y = 0$, it is clear that a and $-a$ are both in the set. Since $a \neq 0$, one of a and $-a$ is positive, so the set contains some positive numbers. Let d be the smallest positive number in the set, and write $d = as + bt$.

By Theorem 1.1 we can find q and r so that

$$b = dq + r, \qquad 0 \leq r < d.$$

Then

$$r = b - dq = b - (as + bt)q = a(-sq) + b(1 - qt),$$

so that r is also in the set. Now $0 < r < d$ is not possible, since d is the *least* positive number in the set. The only alternative is $r = 0$. Hence $b = dq$. A similar argument, beginning with

$$a = dq' + r', \qquad 0 \leq r' < d$$

shows that $r' = 0$, $a = dq'$.

This proves that d is a factor shared by both a and b. But a and b are relatively prime, so that $d = \pm 1$; moreover d is positive, so it must be 1. Hence $1 = as + bt$.

In what follows the notation "$m \mid n$" means "m divides n" or "m is a factor of n". If m is not a factor of n we write $m \nmid n$. The following theorem is the key to unique factorization.

THEOREM 1.3. *If p is a prime number and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

The possibility that $p \mid a$ *and* $p \mid b$ is not excluded by the theorem.

If $p \mid a$ there is nothing to prove. Suppose then that $p \nmid a$; we shall show that in this case p must divide b. Since p and a are relatively prime there exist integers l and m for which

$$lp + ma = 1, \qquad lpb + mab = b.$$

This follows from the preceding theorem. Since $p \mid ab$ we can write $ab = pq$. The last formula becomes $p(lb + mq) = b$, so that $p \mid b$.

COROLLARY 1.4. *If a prime number p divides a product $a_1a_2 \cdots a_n$ of integers, it divides at least one of the a_i.*

For if p divides no a_i, then by Theorem 1.3 it cannot divide any of

$$a_1a_2 , (a_1a_2)a_3 , \cdots , (a_1a_2 \cdots a_{n-1})a_n .$$

We are now in a position to prove the fundamental theorem stated in the opening paragraph of the chapter. Let m be a positive integer not 1. If it is not prime suppose it factors as $m = m_1m_2$, where $m_1 > 1$, $m_2 > 1$. If m_1 and m_2 are primes, stop; otherwise repeat the procedure for m_1 and m_2, and continue it for the new factors which appear. Eventually we must arrive at a stage where none of the factors will decompose again. Otherwise m, which is a finite integer, would be the product of an arbitrarily large number of factors all greater than 1.

Thus we arrive at a factorization

$$m = p_1p_2 \cdots p_r ,$$

where each p_i is positive and prime. Suppose

$$m = q_1q_2 \cdots q_s$$

is any other factorization of m into positive primes. We must prove that the two factorizations differ at most in the order in which the primes appear. Since

$$p_1p_2 \cdots p_r = q_1q_2 \cdots q_s$$

it follows from Corollary 1.4 that q_1 must divide one of the p_i. We may suppose it to be p_1, by renumbering the p_i if necessary. Then $q_1 \mid p_1$. Since p_1 and q_1 are positive and prime $p_1 = q_1$. Hence, dividing out $p_1 = q_1$, we obtain

$$p_2 \cdots p_r = q_2 \cdots q_s .$$

This procedure can be repeated with $q_2, \cdots$, until all the prime factors on one side are exhausted. At this stage all the factors on the other side must also be exhausted; otherwise we should have a product of primes on one side equal to 1 on the other. Then $r = s$ and we are done.

If we try to apply the principle of unique factorization to negative integers, we encounter an obvious difficulty in the possible presence of minus signs in the factors. Thus

$$-12 = 2^2(-3) = (-2)\,(-3)\,(-2)$$

are two factorizations of -12 into primes, and these factorizations differ not merely in the order of the factors, but in the factors themselves. For in the first case the factors are $2, 2, -3$; in the second case they are $-2, -3, -2$. This difficulty can be remedied by a slight restatement of the fundamental theorem to include negative numbers. Let 1 and -1 be called *units*. The new statement is this.

THEOREM 1.5. (*The Fundamental Theorem*). *Each integer not zero or a unit can be factored into the product of primes which are uniquely determined to within order and multiplication by units.*

The slight change in the original proof which is needed here will be left to the reader.

2. **A general problem.** We are now in a position to state the basic problem of algebraic number theory: if we extend the meaning of "integer" to include a wider class of numbers than the numbers $0, \pm 1, \pm 2, \cdots$ is there still a valid analogue of Theorem 1.5? The nature of the question can best be made plain by examples.

For this purpose we select first the *Gaussian* integers. By such an integer we shall mean a number of the form $a + bi$, where a and b are ordinary integers, and $i = \sqrt{-1}$. To avoid confusion later we shall refer to the ordinary

integers as the *rational* integers. Let G denote the set of all Gaussian integers, and J the set of all rational integers. Note that in each set the sum, difference and product of integers are integers.

If α and β are numbers in G we say that α divides β, written $\alpha \mid \beta$, if there is a number γ in G such that $\beta = \alpha\gamma$. An element of G is a *unit* if it divides 1, and hence also every element of G. A number π is *prime* if it is not a unit and if in every factorization $\pi = \alpha\beta$ one of α or β is a unit. With this terminology Theorem 1.5 becomes meaningful for the integers of G.

But is it *true*? It is, as we shall show presently. This fact may strike the reader as only what is to be expected. That such an impression is erroneous we demonstrate by exhibiting another simple class of "integers" for which Theorem 1.5 is meaningful, but false.

Let us now mean by an "integer" any number of the form $a + b\sqrt{-5}$, where a and b are rational integers. Clearly the sum, difference and product of such integers are of the same form. We shall denote the totality of them by H. Define unit and prime just as we did for the Gaussian integers by simply reading H for G wherever the latter occurs. As we shall prove a little later, ± 1 are the only units in H; the numbers $3, 7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$ will turn out to be prime in H. But observe that

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}),$$

so that the factorization of 21 into prime factors is *not* unique to within order and multiplication by units.

It is therefore reasonable to ask for which classes of "integers" the fundamental theorem holds, and for which it does not. In particular how does one explain the discrepancy in behavior between the sets J and G on the one hand and H on the other? The answer to these questions

must be postponed until later. For the present we content ourselves with demonstrating the assertions just made concerning the sets G and H.

3. **The Gaussian integers.** If $\alpha = a + bi$ is an element of G its *norm* $N(\alpha)$, or simply $N\alpha$, is defined to be $\alpha\bar{\alpha} = |\alpha|^2 = a^2 + b^2$. ($\bar{\alpha}$ is the complex-conjugate of α). The following list contains the fundamental properties of the norm.

(i) If α is in J as well as in G, then $N\alpha = \alpha^2$.
(ii) $N(\alpha\beta) = N\alpha N\beta$.
(iii) $N\alpha = 1$ if and only if α is a unit.
(iv)

$$N\alpha \begin{cases} = 0 & \text{if } \alpha = 0, \\ = 1 & \text{if } \alpha = \pm 1 \text{ or } \pm i, \\ > 1 & \text{otherwise.} \end{cases}$$

(v) If $N\alpha$ is prime in J, then α is prime in G.

The proof of (i) is obvious since $b = 0$. To prove (ii) observe that if $\alpha = a + bi$, $\beta = c + di$, then

$$(\alpha\beta)\,(\overline{\alpha\beta}) = (\alpha\bar{\alpha})\,(\beta\bar{\beta}).$$

As for (iii), suppose first that α is a unit. Then $\alpha \mid 1$, so $\alpha\beta = 1$ for some β. By (ii) $N\alpha N\beta = N1 = 1$, and $N\alpha \mid 1$. Since $N\alpha$ must be a non-negative integer, $N\alpha = 1$. Conversely if $N\alpha = 1$, $a^2 + b^2 = 1$, so that $a = 0$ or $b = 0$. Then $\alpha = 1, -1, i$ or $-i$, and these are obviously units. This argument also establishes most of (iv); the rest we leave to the reader.

Finally to prove (v), suppose $N\alpha$ is prime and $\alpha = \beta\gamma$. Then $N\alpha = N\beta N\gamma$ is prime in J. So one of $N\beta$ or $N\gamma$ is equal to 1, and by (iii) either β or γ is a unit.

The converse of (v) is false. To see this it is enough to

show that 3 is prime in G, for $N3 = 3^2 = 9$. Suppose $3 = \alpha\beta$. Then $9 = N\alpha N\beta$. If neither α nor β is a unit $N\alpha \neq 1$, $N\beta \neq 1$, so $N\alpha = N\beta = 3$. But this means that if $\alpha = a + bi$, then $a^2 + b^2 = 3$; this is impossible for any pair of integers a, b in J. (why?)

In proving that Theorem 1.5 holds for the Gaussian integers we shall imitate as far as possible the proof already given for rational integers.

THEOREM 1.6. *If α and β are Gaussian integers, $\beta \neq 0$, then there exist two integers π and ρ such that*

$$\alpha = \pi\beta + \rho, \qquad N\rho < N\beta.$$

Consider the number $\dfrac{\alpha}{\beta} = A + Bi$, where A and B are ordinary rational numbers. Choose rational integers s and t such that

$$|A - s| \leq \tfrac{1}{2}, \qquad |B - t| \leq \tfrac{1}{2}.$$

This we can always do by choosing s and t as rational integers nearest to A and B respectively. Now let $\pi = s + ti$, $\rho = \alpha - \pi\beta$.

To show that $N\rho < N\beta$ observe that

$$|\rho| = |\alpha - \pi\beta| = |\alpha - (s + ti)\beta| = |\beta| \left|\frac{\alpha}{\beta} - s - ti\right|$$

$$= |\beta|\,|(A - s) + (B - t)i| = |\beta|\{(A - s)^2 + (B - t)^2\}^{1/2}$$

$$\leq |\beta| \left\{\frac{1}{2^2} + \frac{1}{2^2}\right\}^{1/2} < |\beta|.$$

Since $N\rho = |\rho|^2 < |\beta|^2 = N\beta$, the inequality is established.

As an example let $\alpha = 5 - i$, $\beta = 1 + 2i$. Then

$$\frac{\alpha}{\beta} = \frac{(5 - i)(1 - 2i)}{(1 + 2i)(1 - 2i)} = \frac{3}{5} - \frac{11}{5}\,i,$$

so $A = \frac{3}{5}$, $B = -\frac{11}{5}$. Take $s = 1$, $t = -2$, $\pi = 1 - 2i$, $\rho = (5 - i) - (1 - 2i)(1 + 2i) = 5 - i - 5 = -i$. Then

$$5 - i = (1 - 2i)(1 + 2i) - i,$$

and $N(-i) < N(1 + 2i)$.

Let the reader show by an example that, in contrast to Theorem 1.1, π and ρ are *not* uniquely determined.

THEOREM 1.7. *If π is a prime and $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$.*

If $\pi \mid \alpha$ we are done; so suppose $\pi \nmid \alpha$. We shall prove that $\pi \mid \beta$.

By Theorem 1.6 we can find δ and ρ so that

$$\alpha = \delta\pi + \rho, \qquad N\rho < N\pi.$$

Moreover $N\rho \neq 0$, for otherwise $\rho = 0$ so that $\pi \mid \alpha$, contrary to assumption. So $0 < N\rho < N\pi$.

Consider all integers in G which are different from zero and are of the form $\alpha\xi + \pi\eta$. Call the totality of them T. $\rho = \alpha - \pi\delta$ is an integer in T. By property (iv) of norms in G, every element in T has norm at least equal to 1, so there must be one of them $\gamma = \alpha\xi_0 + \pi\eta_0$ which is of least positive norm. Now $\rho = \alpha - \pi\delta$ is in T and has norm less than $N\pi$. Since γ is of least norm, then also $N\gamma < N\pi$. We show next that γ is actually a unit.

Choose θ and ζ so that

$$\pi = \theta\gamma + \zeta, \qquad N\zeta < N\gamma.$$

Since $\zeta = \pi - \theta\gamma = \pi - \theta(\alpha\xi_0 + \pi\eta_0) = \alpha(-\theta\xi_0) + \pi(1 - \theta\eta_0)$, $N\zeta = 0$, for if $N\zeta \neq 0$, then ζ would be an element of T of smaller norm than γ. So $\zeta = 0$ and $\pi = \theta\gamma$, $N\pi = N\theta N\gamma$. One of θ and γ is a unit since π is a prime. But if $N\theta = 1$, then $N\pi = N\gamma$, which contradicts $N\pi > N\gamma$. So θ is not a unit, which means that γ is.

Hence $\gamma = \alpha\xi_0 + \pi\eta_0$ is a unit. Now

$$\alpha\beta\xi_0 + \pi\beta\eta_0 = \gamma\beta.$$

Since $\pi \mid \alpha\beta$ by hypothesis and $\pi \mid \pi\beta\eta_0$, then also $\pi \mid \gamma\beta$. So $\gamma\beta = \pi\tau$ for some τ in G. Then $\beta = \pi(\tau/\gamma)$ and $\pi \mid \beta$, for τ/γ is in G.

To prove that Theorem 1.5 is valid for the integers of G we proceed much as in the case of the rational integers. If α is not a unit or a prime let $\alpha = \alpha_1\alpha_2$, where $N\alpha_1 > 1$, $N\alpha_2 > 1$. Repeat this procedure for α_1 and α_2, and continue it. It must stop sometime, for otherwise $N\alpha$ would be the product of an arbitrarily large number of factors each greater than 1. So $\alpha = \pi_1 \cdots \pi_r$, where the π_i are primes. If also $\alpha = \sigma_1 \cdots \sigma_t$, where the σ_i are primes, then by Theorem 1.7 σ_1 must divide one of the π_i, say π_1. Hence $\sigma_1 = \pi_1\epsilon_1$, where ϵ_1 is a unit. Then

$$\pi_2 \cdots \pi_r = \epsilon_1\sigma_2 \cdots \sigma_t.$$

We can now complete the proof as we did for J.

It remains finally to establish the still unproved statements about H made in the preceding section, namely that ± 1 are the only units, and that $3, 7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$ are prime numbers in H.

If $\alpha = a + b\sqrt{-5}$, define $N\alpha = \alpha\bar{\alpha} = a^2 + 5b^2$. As before, $N(\alpha\beta) = N\alpha N\beta$. α is a unit if and only if $N\alpha = 1$; the proof goes as in the case of the Gaussian integers. But $a^2 + 5b^2 = 1$ only when $b = 0$, $a = \pm 1$, so $\alpha = \pm 1$ are the only units in H.

To show that 3 is a prime, suppose $3 = \alpha\beta$, where neither α nor β is a unit — that is, $N\alpha \neq 1$, $N\beta \neq 1$. Since $9 = N3 = N\alpha \cdot N\beta$, then $N\alpha = N\beta = 3$, so $a^2 + 5b^2 = 3$. If $b \neq 0$ then $a^2 + 5b^2 > 3$, so b must be zero. But then $a^2 = 3$, which cannot occur for an integer a in J. Similarly if $7 = \alpha\beta$, $N\alpha \neq 1$, $N\beta \neq 1$, then $a^2 + 5b^2 = 7$. If $b^2 \neq 0$,

$b^2 \neq 1$ then $a^2 + 5b^2 > 7$. So either $b = 0$, $a^2 = 7$, which is impossible, or $b = \pm 1$, $a^2 = 2$, which is also impossible.

The numbers $1 \pm 2\sqrt{-5}$ are prime, for if $1 \pm 2\sqrt{-5} = \alpha\beta$, then $N(1 \pm 2\sqrt{-5}) = 21 = N\alpha N\beta$. Unless one of α or β is a unit $N\alpha = 3$ or $N\beta = 3$, and this possibility has already been excluded.

An additional example of a class of "integers" for which unique factorization is valid is given by the set of numbers $a + b\omega$, where $\omega = \frac{1}{2}(-1 + \sqrt{-3})$. The reader who is interested in the details will find them given in Chapter XII of the book of Hardy and Wright listed in the bibliography.

Chapter II

THE GAUSSIAN PRIMES

1. **Rational and Gaussian primes.** It is not difficult to establish the existence of an infinite number of rational primes—that is, primes in J. The simplest proof, due to Euclid, goes as follows. Suppose $p_1, p_2, \cdots, p_n$ are known to be prime. Then the number $N = 1 + p_1 p_2 \cdots p_n$ cannot have any one of the p_i as a factor, since then 1 would also have that p_i as a factor. Then any prime factor of N is different from $p_1, \cdots, p_n$. This means that if any finite set of prime numbers is given, there is a prime different from any of them; so there are an infinite number if there is at least one. But 2 is a prime, and the conclusion follows.

Precisely the same proof is valid for Gaussian primes provided only that we can find one prime. But 3 has already been shown to be a Gaussian prime, so that G contains an infinity of primes. We can accomplish considerably more: we shall characterize explicitly all the primes in G in terms of those in J. In order to achieve this we shall need some material from elementary number theory. Actually we shall prove somewhat more than we need for the present purpose. The additional results will find application later.

2. **Congruences.** In this section we deal only with rational integers.

Let m be an integer not zero. Two integers a and b are said to be *congruent modulo* m, written

$$a \equiv b \pmod{m} \quad or \quad a \equiv b \quad (m),$$

if $m \mid (a - b)$. If a and b are not congruent mod m we write $a \not\equiv b \quad (m)$.