THE EULER ϕ-FUNCTION IN THE GAUSSIAN INTEGERS

JAMES T. CROSS
Department of Mathematics, The University of the South, Sewanee, TN 37375

1. Introduction. The set of all complex numbers $a + bi$, where a and b are integers, forms an integral domain with the usual complex number operations. This domain, the *Gaussian Integers*, which we denote by G, includes Z, the domain of *rational* (*ordinary*) *integers*, and behaves like Z in many respects.

Let β denote a nonzero Gaussian integer and $G/(\beta)$ the quotient ring of G (mod β). It is fun to discover that these rings furnish accessible and interesting examples of familiar concepts including equivalence classes, fields, cyclic and noncyclic groups, and the Euler ϕ-function. In this section we review the ϕ-function, extend it to G, and discuss some questions whose answers are well known in Z and which we intend to study in G.

Let n be a nonzero member of Z and let $Z/(n)$ denote the quotient ring of Z (mod n). If $n > 0$, then

$$Z/(n) = \{[0], [1], [2], \ldots, [n-1]\},$$

where the brackets denote *equivalence classes*. The rings $Z/(n)$ and $Z/(-n)$ are identical, so that we may confine our attention to positive n. The *units* (those members having multiplicative inverses) of this ring form a multiplicative group which is denoted by $\Phi_Z(n)$ and the Euler ϕ-function $\phi_Z(n)$ is defined to be the order of this group. A simple argument in elementary number theory proves that the member $[k]$ of $Z/(n)$ is a unit if and only if $(k, n) = 1$; that is, if and only if k and n are *relatively prime*. Thus for $n > 1$, $\phi_Z(n)$ is the number of positive integers less than n and prime to n. If $\Phi_Z(n)$ is cyclic and $[k]$ generates this group, then k is called a *primitive root* for n. Simple construction of multiplication tables leads to the conclusion that primitive roots exist for $n = 1, 2, 3, 4, 5, 6$, and 7. However no primitive root exists for 8 since $\Phi_Z(8) = \{[1], [3], [5], [7]\}$ has members of orders 1 and 2 only.

The determination of those integers that have primitive roots is a popular undertaking in number theory. There it is proved that n has primitive roots if and only if $n = 2$ or 4, or n is a power of an odd prime or twice a power of an odd prime. In fact, a great deal more is established. Let the symbol $\simeq$ denote *isomorphism* and Z_n denote the (cyclic) additive group of $Z/(n)$. Then for $m > 1$, the structure of $\Phi_Z(m)$ is given as follows [**1**, pages 46–51]:

$\Phi_Z(2) \simeq Z_1$,

$\Phi_Z(4) \simeq Z_2$,

$\Phi_Z(2^n) \simeq Z_2 \times Z_{2^{n-2}}$ if $n > 2$,

$\Phi_Z(p^n) \simeq Z_{p^n - p^{n-1}}$ if p is an odd prime,

Φ_Z is multiplicative in the sense that $\Phi_Z(mn) \simeq \Phi_Z(m) \times \Phi_Z(n)$ if $(m, n) = 1$.
(The structure of $\Phi_Z(m)$ for arbitrary m is gotten through its prime factorization.)

The Euler ϕ-function extends naturally to G. Since Z is contained in G and the units of $G/(\beta)$ also form a multiplicative group, we let $\Phi_G(\beta)$ denote this group and let $\phi_G(\beta)$ denote its order. The following questions arise immediately:

James T. Cross: I received the Ph.D. from the University of Tennessee where Professor Eckford Cohen directed my work. I majored in mathematics at Brown University, took an M.S. in applied mathematics at Harvard, and have been at Sewanee since 1955. The problem discussed in this paper occurred to me as a result of some "primitive root" studies done by two of my senior honors students. My extracurricular activities are extensive and intensive (too much so). I mention two: mini-farming and ping-pong.

1. If p is an odd rational prime, then is $\Phi_G(p^n)$ still cyclic in this larger setting?
2. More generally, which Gaussian integers have primitive roots?
3. Can we determine the structure of $\Phi_G(\beta^n)$, where β is prime in G?
4. If the answer to question 3 is yes, can we extend our results to an arbitrary Gaussian integer through its prime factorization?

Question 1 can be settled quickly in the negative by determining the orders of the members of $\Phi_G(3^2)$. As we shall show later in Example 4, a complete and nonrepeating set of representatives for the members (equivalence classes) of this group is the set of all $a + bi$, where a and b range independently from 0 through 8 and at least one of a and b is prime to 3. The 72 members of this group, and their orders, are tabulated in Fig. 1. This table is taken from an unpublished paper [**2**], written by my student, Michael S. Crowe, who answered questions 1 and 2.

	$[i]$ 4	$[2i]$ 12		$[4i]$ 12	$[5i]$ 12		$[7i]$ 12	$[8i]$ 4
$[1]$ 1	$[1 + i]$ 24	$[1 + 2i]$ 24	$[1 + 3i]$ 3	$[1 + 4i]$ 24	$[1 + 5i]$ 24	$[1 + 6i]$ 3	$[1 + 7i]$ 24	$[1 + 8i]$ 24
$[2]$ 6	$[2 + i]$ 24	$[2 + 2i]$ 8	$[2 + 3i]$ 6	$[2 + 4i]$ 24	$[2 + 5i]$ 24	$[2 + 6i]$ 6	$[2 + 7i]$ 8	$[2 + 8i]$ 24
	$[3 + i]$ 12	$[3 + 2i]$ 12		$[3 + 4i]$ 12	$[3 + 5i]$ 12		$[3 + 7i]$ 12	$[3 + 8i]$ 12
$[4]$ 3	$[4 + i]$ 24	$[4 + 2i]$ 24	$[4 + 3i]$ 3	$[4 + 4i]$ 24	$[4 + 5i]$ 24	$[4 + 6i]$ 3	$[4 + 7i]$ 24	$[4 + 8i]$ 24
$[5]$ 6	$[5 + i]$ 24	$[5 + 2i]$ 24	$[5 + 3i]$ 6	$[5 + 4i]$ 24	$[5 + 5i]$ 24	$[5 + 6i]$ 6	$[5 + 7i]$ 24	$[5 + 8i]$ 24
	$[6 + i]$ 12	$[6 + 2i]$ 12		$[6 + 4i]$ 12	$[6 + 5i]$ 12		$[6 + 7i]$ 12	$[6 + 8i]$ 12
$[7]$ 3	$[7 + i]$ 24	$[7 + 2i]$ 8	$[7 + 3i]$ 3	$[7 + 4i]$ 24	$[7 + 5i]$ 24	$[7 + 6i]$ 3	$[7 + 7i]$ 8	$[7 + 8i]$ 24
$[8]$ 2	$[8 + i]$ 24	$[8 + 2i]$ 24	$[8 + 3i]$ 6	$[8 + 4i]$ 24	$[8 + 5i]$ 24	$[8 + 6i]$ 6	$[8 + 7i]$ 24	$[8 + 8i]$ 24

FIG. 1.
The elements of $\Phi_G(3^2)$ and their orders.

In the table, for which the computations were done by computer, square brackets denote equivalence classes while the numbers without brackets indicate orders. For example, the order of $[4 + 7i]$ is 24, the order of $[5]$ is 6, and the order of $[1 + 3i]$ is 3. These orders are easy to determine though the calculations are tedious. For example, the order of $[1 + 3i]$ is 3 because

$$(1 + 3i)^3 = 1 + 9i + 27i^2 + 27i^3 \equiv 1 \pmod 9,$$

while

$$(1 + 3i)^2 = 1 + 6i + 9i^2 \not\equiv 1 \pmod 9.$$

Since the highest order observed in the table is 24, it is clear that there exist odd primes for which the answer to question 1 is no. (We will show in Example 7 below that $\Phi_G(3^2) \simeq Z_3 \times Z_3 \times Z_8$.)

Our objective in this paper is to answer questions 3 and 4, obtaining Crowe's answer to question 2 as a by-product. Our methods are direct and constructive:

(i). We identify the primes in G. Fortunately, we have to consider only three types.
(ii). For β a prime in G, we find equivalence class representatives of $G/(\beta^n)$ and its units group, $\Phi_G(\beta^n)$.
(iii). For a power of each type of prime, we determine the structure of the corresponding units group, answering question 3.
(iv). We show that Φ_G is multiplicative. The answer to question 4 will then be at hand.

2. The Primes in G. Our principal goal in this section is to identify the primes in G; in conjunction with this program we also give some relevant facts concerning the Gaussian Integers. The reader can find these topics discussed in [**1**, pp. 82–112] or [**3**, pp. 246–260]:

For $\beta = a + bi$ in G, the norm $N(\beta)$ of β is defined by $N(\beta) = (a + bi)(a - bi) = a^2 + b^2$. Note that $N(\beta)$ is in Z. The norm of a product equals the product of the norms. If β divides γ in G, then $N(\beta)$ divides $N(\gamma)$ in Z.

If μ is in G, then μ is a unit if and only if $N(\mu) = 1$. It follows that the units in G are 1, -1, i, and $-i$.

If q is a positive prime in Z and $q \equiv 1 \pmod 4$, then $q = \pi\bar{\pi}$ for some π in G, where $\bar{\pi}$ is the complex conjugate of π. Here π and $\bar{\pi}$ are prime in G and they are not associates. (Members β and γ in G are *associates*, which we denote by $\beta \sim \gamma$, if $\beta = \mu\gamma$ for some unit μ in G.)

EXAMPLE 1. In G, $5 = (1 + 2i)(1 - 2i)$. If, for example, $1 + 2i = \beta\gamma$ in G, then $N(1 + 2i) = 5 = N(\beta)\ N(\gamma)$ in Z. Then $N(\beta) = 1$ or $N(\gamma) = 1$, so that one of the factors is a unit and the factorization is trivial. Thus $1 + 2i$ is prime; similarly, so is $1 - 2i$. To see that they are not associates, we need only try to get from one to the other by means of the four units.

If p is a positive prime in Z and $p \equiv 3 \pmod 4$, then p is prime in G.

EXAMPLE 2. Let $p = 3$. If $3 = \beta\gamma$ in G, then $N(3) = 9 = N(\beta)\ N(\gamma)$ in Z. Then either $N(\beta) = N(\gamma) = 3$ or the norm of one of the factors is 1. Since $a^2 + b^2 = 3$ is not solvable in Z, the first alternative must be discarded. Then one of β and γ is a unit, the factorization of 3 is trivial, and 3 is prime in G.

In G, $2 = (1 + i)(1 - i)$, where these factors are primes. However, they are associates since $1 - i = -i(1 + i)$. Then $2 = \mu(1 + i)^2$, where μ is a unit in G, and we see that 2 is a power of a prime in G. If α denotes $1 + i$, then $\alpha^2 \sim 2$, $\alpha^3 \sim 2\alpha$, $\alpha^4 \sim 4, \dots, \alpha^{2m} \sim 2^m$, and $\alpha^{2m+1} \sim 2^m\alpha$.

The primes described above (α and primes of the types π and p) are, together with their associates, the only primes in G.

Factorization into primes in G is unique in the following sense: two factorizations may look different, but we can get from one to the other by multiplying by units. For example, as we saw above, $2 = \alpha\bar{\alpha} = -i\alpha^2$. This phenomenon also occurs in Z: $6 = (3)(2) = (-3)(-2)$.

3. The Equivalence Classes in $G/(\beta^n)$ and $\Phi_G(\beta^n)$, Where β Is Prime in G. Now that we have identified the primes in G, we want to be able to raise them to powers and find representatives for the equivalence classes of the corresponding quotient rings and units groups. Theorems 1 and 2 below address this problem. Following the theorems we consider some examples.

In the remainder of the paper we will continue with the following notation: q and p will denote positive primes in Z satisfying $q \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$, π will denote a *prime factor of q in G*, and α will denote $1 + i$.

THEOREM 1. *The equivalence classes of G* modulo *a power of a prime are given as follows*:

1. $G/(\pi^n) = \{[a]\colon 0 \leqslant a \leqslant q^n - 1\}$,
2. $G/(p^n) = \{[a + bi]\colon 0 \leqslant a \leqslant p^n - 1 \text{ and } 0 \leqslant b \leqslant p^n - 1\}$,
3. $G/(\alpha^{2m}) = \{[a + bi]\colon 0 \leqslant a \leqslant 2^m - 1 \text{ and } 0 \leqslant b \leqslant 2^m - 1\}$,
4. $G/(\alpha^{2m+1}) = \{[a + bi]\colon 0 \leqslant a \leqslant 2^{m+1} - 1 \text{ and } 0 \leqslant b \leqslant 2^m - 1\}$.

In the statements of this theorem, as well as in the examples to be considered below, we intend to imply that the given sets of representatives are complete and nonrepeating.

Proof. First we observe that $G/(\alpha^{2m}) = G/(2^m)$ and $G/(\alpha^{2m+1}) = G/(2^m\alpha)$ because $\alpha^{2m} \sim 2^m$. Now if $a + bi \equiv c + di \pmod{\alpha^{2m}}$, then 2^m divides both $a - c$ and $b - d$, so that the classes of (3) are distinct. A similar argument applies to the classes in (2). If $[a] = [b]$ in $G/(\pi^n)$, then π^n divides $a - b$. Let $\pi^n\gamma = a - b$ for some γ in G. Then taking complex conjugates, we get $\bar{\pi}^n = \overline{a - b} = a - b$, so that $\bar{\pi}^n$ also divides $a - b$. Since π and $\bar{\pi}$ are not associates, $\pi^n\bar{\pi}^n = q^n$

divides $a - b$ implying that the classes in (1) are distinct. If $[a + bi] = [c + di]$ in $G/(\alpha^{2m+1}) = G/(2^m\alpha)$, then $2^m\alpha$ divides $a - c + (b - d)i$. Then 2^m divides $b - d$; since each is less than 2^m, $b = d$. Then $2^m\alpha$ divides $a - c$. Let $a - c = 2^m k$, where k is in Z because the only rational members of G are integers. Then α divides k so that $N(\alpha) = 2$ divides $N(k) = k^2$. Then 2 divides k, so that 2^{m+1} divides $a - c$ and the classes in (4) are distinct.

Now let $\beta = x + yi$ be in G. Reducing x and y by multiples of 2^m gets β in one of the classes in (3). Reducing by multiples of p^n, we get β in one of the classes of (2). Reducing by multiples of 2^{m+1} yields $\beta \equiv c + di \pmod{2^{m+1}}$, where each of c and d is nonnegative and less than 2^{m+1}. If $d < 2^m$, we have β in one of the classes of (4). If $d \geqslant 2^m$, then we subtract and add $2^m\alpha$, getting

$$c + di = (c - 2^m) + (d - 2^m)i + 2^m\alpha.$$

Then

$$\beta \equiv (c - 2^m) + (d - 2^m)i \pmod{\alpha^{2m+1}},$$

where $0 \leqslant d - 2^m < 2^m$. Then $c - 2^m$ can be reduced by multiples of 2^{m+1}, getting β in one of the classes in (4). Now we show that i belongs to one of the classes in (1). Let $\pi^n = a - bi$, so that $bi \equiv a \pmod{\pi^n}$. Now q is prime to b, for if q divides b, then both π and $\bar{\pi}$ divide b. Then π divides a. But this implies that q divides a. Then q divides π^n; this is absurd because $q = \pi\bar{\pi}$. Thus $(q, b) = 1$ and the congruence, $zb \equiv 1 \pmod{q^n}$ is solvable in Z. Then the congruence, $bi \equiv a \pmod{q^n}$, yields $i \equiv za \pmod{\pi^n}$. Then za can be reduced by multiples of p^n to find i in one of the given classes. Since each of x, y, and i belongs to one of the classes of (1), then so does $\beta = x + yi$. □

This theorem implies that $G/(\pi^n)$ has q^n members, $G/(p^n)$ has p^{2n} members, and $G/(\alpha^n)$ has 2^n members. These facts are special cases of the well-known result [**4**, page 54] that the order of $G/(\beta)$ is $N(\beta)$.

Now we are ready to identify the units of the rings whose members are specified in Theorem 1.

Theorem 2. *Let $[a]$ be in $G/(\pi^n)$. Then $[a]$ is a unit if and only if $(q, a) = 1$. Let $[a + bi]$ be in $G/(p^n)$. Then $[a + bi]$ is a unit if and only if at least one of a and b is prime to p. Let $[a + bi]$ be in $G/(\alpha^n)$. Then $[a + bi]$ is a unit if and only if $a \not\equiv b$* (mod 2).

Proof. Let β and γ be in G. Then $[\beta]$ is a unit in $G/(\gamma)$ if and only if $[\beta][\delta] = [1]$ in $G/(\gamma)$, for some δ in G. Then $[\beta]$ is a unit if and only if $\beta\delta \equiv 1 \pmod{\gamma}$; that is, if and only if $\beta\delta + \eta\gamma = 1$ for some η in G. Thus $[\beta]$ is a unit in $G/(\gamma)$ if and only if β is prime to γ. It follows that $[a]$ in $G/(\pi^n)$ is a unit if and only if π does not divide a, but π does not divide a if and only if q does not divide a. Next, $[a + bi]$ in $G/(p^n)$ is a unit if and only if p does not divide $a + bi$; p does not divide $a + bi$ if and only if p is prime to at least one of a and b. Finally, $[a + bi]$ in $G/(\alpha^n)$ is a unit if and only if α does not divide $a + bi$. But

$$(a + bi)/\alpha = (a + bi)/(1 + i) = (a + b)/2 + i(b - a)/2.$$

This quotient is a Gaussian integer if and only if $a \equiv b$ (mod 2). Thus α does not divide $a + bi$ if and only if $a \not\equiv b$ (mod 2). □

Example 3. Let $\pi = 1 + 2i$. We know that π is prime and $\pi\bar{\pi} = 5$. Theorems 1 and 2 assert that

$$G/(\pi^2) = \{[0], [1], [2], \ldots, [24]\}$$

and $[a]$ in $G/(\pi^2)$ is a unit if and only if 5 does not divide a. It may be instructive to find the class to which i belongs. Now $\pi^2 = -3 + 4i$, so that $4i \equiv 3 \pmod{\pi^2}$. Multiplying this congruence through by 19, we get $76i \equiv 57 \pmod{\pi^2}$. But since π^2 divides 25, this congruence reduces to $i \equiv 7 \pmod{\pi^2}$. We can check this result directly: $(7 - i)/(-3 + 4i) = -1 - i$, so that π^2 divides $7 - i$ in G. Thus $i \equiv 7 \pmod{\pi^2}$, and i belongs to [7].

In this example the reader should convince himself that $\Phi_G((1 + 2i)^2)$ is isomorphic to $\Phi_Z(25)$.

Since $\Phi_Z(25)$ is cyclic, $(1+2i)^2 = -3+4i$ has primitive roots. In fact, 2 serves as such a root.

EXAMPLE 4. By Theorems 1 and 2, $\Phi_G(3^2) = \Phi_G(9) =$

$$\{[a+bi]: 0 \leqslant a \leqslant 8, 0 \leqslant b \leqslant 8, \text{and 3 is prime to at least one of } a \text{ and } b\}.$$

Note that $\Phi_Z(9)$ is included isomorphically in $\Phi_G(9)$. Thus $\Phi_Z(9) = \{[1], [2], [4], [5], [7], [8]\}$ can be identified in an obvious way with $\{[1], [2], [4], [5], [7], [8]\}$ in $\Phi_G(9)$.

EXAMPLE 5. By Theorems 1 and 2,

$$\begin{aligned}\Phi_G(\alpha^5) &= \Phi_G(4\alpha)\\ &= \{[1],[3],[5],[7],[i],[2+i],[4+i],[6+i],[1+2i],[3+2i],\\ &\qquad [5+2i],[7+2i],[3i],[2+3i],[4+3i],[6+3i]\}.\end{aligned}$$

Note that $\Phi_Z(8) = \{[1], [3], [5], [7]\}$ is included isomorphically in $\Phi_G(\alpha^5)$. Since $\Phi_Z(8)$ is not cyclic and since any subgroup of a cyclic group is cyclic, α^5 has no primitive root.

Let us be more ambitious and find the structure of $\Phi_G(\alpha^5)$. Let H denote the subgroup generated by $[1+2i]$, and let K and I denote the subgroups generated by $[5]$ and $[i]$, respectively. Then

$$H = \{[1],[1+2i]\}, \quad K = \{[1],[5]\},$$

and

$$I = \{[1],[i],[-1],[-i]\} = \{[1],[i],[7],[4+3i]\}.$$

Now $H \times K = \{[1], [5], [1+2i], [5+2i]\}$. Since $H \times K$ intersects I only at the identity and since each of $H \times K$ and I has order 4, the order of $H \times K \times I$ is $16 = \phi_G(\alpha^5)$. Then

$$\Phi_G(\alpha^5) = H \times K \times I \simeq Z_2 \times Z_2 \times Z_4.$$

Now, using Theorems 1 and 2, we can count the members of the units groups and find the following results:

$$\begin{aligned}\phi_G(\pi^n) &= \phi_Z(q^n) = q^n - q^{n-1} = q^{n-1}(q-1),\\ \phi_G(p^n) &= p^{2n} - p^{2n-2} = p^{2n-2}(p^2-1),\\ \phi_G(\alpha^n) &= 2^n - 2^{n-1} = 2^{n-1}.\end{aligned}$$

The reader is invited to verify these results in Examples 3–5.

In our program outlined in (i)–(iv) of Section 1, we have now reached (iii). We are ready to find the structures of the units groups that we have been discussing.

4. The Structure of $\Phi_G(\pi^n)$. We show that Example 3 is typical; that is, $\Phi_G(\pi^n)$ is cyclic.

THEOREM 3. $\Phi_G(\pi^n) \simeq Z_{q^n - q^{n-1}}$.

Proof. By Theorem 2,

$$\Phi_G(\pi^n) = \{[a];\ 1 \leqslant a < q^n \text{ and } (q,a) = 1\}.$$

Formally, $\Phi_G(\pi^n)$ looks like $\Phi_Z(q^n)$, and, in fact, the map

$$[a] \text{ in } \Phi_Z(q^n) \to [a] \text{ in } \Phi_G(\pi^n)$$

is an isomorphism onto $\Phi_G(\pi^n)$. Thus, $\Phi_G(\pi^n)$ behaves algebraically like $\Phi_Z(q^n)$. Since $\Phi_Z(q^n) \simeq Z_{q^n - q^{n-1}}$, the proof is complete. While this theorem may be pleasing, it is not very exciting. Fortunately we encounter more interesting ones below.

5. Some Preliminary Ideas Concerning $\Phi_G(\alpha^n)$ and $\Phi_G(p^n)$. We dealt in Section 4 with one type of prime in G. The units groups corresponding to the other two types are generally not cyclic as we saw in the Introduction and in Example 5. We showed in Example 5 that $\Phi_G(\alpha^5) = H \times K \times I$. Let us see whether we may expect a similar structure when α is raised to an even power.

EXAMPLE 6. By Theorems 1 and 2,

$$\Phi_G(\alpha^6) = \Phi_G(8) = \{[a + bi]: 0 \leqslant a \leqslant 7, 0 \leqslant b \leqslant 7, \text{and } a \not\equiv b \pmod 2\}.$$

Again let H, K, and I be generated by $[1 + 2i]$, $[5]$, and $[i]$, respectively. Then

$$H = \{[1], [1 + 2i], [5 + 4i], [5 + 6i]\},$$
$$K = \{[1], [5]\}, \text{and } I = \{[1], [i], [7], [7i]\}.$$

Then $K \times I = \{[1], [i], [7], [7i], [5], [5i], [3], [3i]\}$, so that $(K \times I) \cap H = \{[1]\}$. Then the order of $H \times K \times I$ is $32 = \phi_G(\alpha^6)$. Then again $\Phi_G(\alpha^6) = H \times K \times I$.

Examples 5 and 6 lead us to conjecture that $\Phi_G(\alpha^n) = H \times K \times I$, where these subgroups are generated by $[1 + 2i]$, $[5]$, and $[i]$, respectively. We delay checking out this conjecture in order to motivate another one concerning $\Phi_G(p^n)$. This conjecture involves a subgroup generated by $[1 + pi]$, and we shall study this subgroup and the subgroup H simultaneously.

Now $\phi_G(3^2) = 72$, $\phi_G(3^3) = 648$, and $\phi_G(7^2) = 2352$; it is clear that ideas concerning the structure of $\Phi_G(p^n)$ cannot be gotten by displaying multiplication tables. However, we can write a computer program to find the orders of the members of some of these groups and hope to observe something significant. The results of this effort are summarized below, where we have tabulated the highest orders observed and the order of $[1 + pi]$:

Group	Order	Highest order of an element	Order of $[1 + pi]$
$\Phi_G(3^2)$	$72 = 3^2(3^2 - 1)$	$24 = 3(3^2 - 1)$	3
$\Phi_G(3^3)$	$648 = 3^4(3^2 - 1)$	$72 = 3^2(3^2 - 1)$	9
$\Phi_G(7^2)$	$2352 = 7^2(7^2 - 1)$	$336 = 7(7^2 - 1)$	7
$\Phi_G(7^3)$	$115248 = 7^4(7^2 - 1)$	$2352 = 7^2(7^2 - 1)$	49
$\Phi_G(11^2)$	$14520 = 11^2(11^2 - 1)$	$1320 = 11(11^2 - 1)$	11

Note that in each case the highest order observed is $p^{n-1}(p^2 - 1)$ and the product of this number with p^{n-1} gives $\phi_G(p^n)$. This is a short table; the evidence is skimpy, but we are led to conjecture that $\Phi_G(p^n) = L \times K$, where L has order $p^{n-1}(p^2 - 1)$ and K has order p^{n-1}. This would imply that $\Phi_G(p^n) = H \times K \times R$, where each of H and K has order p^{n-1} and R has order $p^2 - 1$. We note also that $[1 + pi]$ appears to have order p^{n-1}.

EXAMPLE 7. Referring to Fig. 1, we let H, K, and R be the subgroups of $\Phi_G(9)$ generated by $[1 + 3i]$, $[4]$, and $[7 + 2i]$, respectively. Then

$$H = \{[1], [1 + 3i], [1 + 6i]\}, \quad K = \{[1], [4], [7]\},$$

and

$$R = \{[1], [7 + 2i], [i], [7 + 7i], [8], [2 + 7i], [8i], [2 + 2i]\}.$$

Since $H \cap K = \{[1]\}$, $H \times K$ has order 9, and since 8 is prime to 9, $H \times K$ intersects R only at the identity. Then $H \times K \times R$ has order $72 = \phi_G(3^2)$. Then $\Phi_G(3^2) = H \times K \times R$.

Now we recapitulate. Examples 5–7 and our display of orders have led to two conjectures:

(i). $\Phi_G(\alpha^n) = H \times K \times I$, where H, K, and I are generated by $[1 + 2i]$, $[5]$, and $[i]$, respectively.

(ii). $\Phi_G(p^n) = H \times K \times R$, where H is generated by $[1 + pi]$, K has order p^{n-1}, and R has order $p^2 - 1$.

We prove these conjectures in the next two sections (one of them requires some qualification).

At this point we study the subgroups denoted by H in (i) and (ii). Our principal tool is the following lemma.

LEMMA 1. *Let k denote a positive integer. Then,*

(A) $(1 + pi)^{p^k} = 1 + p^{k+1}i + p^{k+2}\gamma$, *where γ is in G.*
(B) $(1 + 2i)^{2^k} = 1 + 2^{k+1}(a + i) + 2^{k+2}\gamma$, *where γ is in G and a is an odd integer.*

Proof. Let β be in G, let r denote a prime in Z, let k be a positive integer, and let σ denote $(1 + \beta r)^{r^k}$. The reader can readily convince himself that it is probably true that

$$\sigma = 1 + \beta r^{k+1} + (\beta^2/2)(r^k - 1)r^{k+2} + \gamma r^{k+2},$$

where γ is some member of G. A proof based on the Binomial Theorem is somewhat tedious but not difficult. We omit the details. Now,

$$\text{if } r \neq 2, \text{ then } \sigma \equiv 1 + \beta r^{k+1} \pmod{r^{k+2}}.$$

If $r = 2$, then

$$\begin{aligned} \sigma &\equiv 1 + 2^{k+1}\beta + \beta^2(2^k - 1)2^{k+1} \pmod{2^{k+2}} \\ &\equiv 1 + 2^{k+1}((2^k - 1)\beta^2 + \beta) \pmod{2^{k+2}}. \end{aligned}$$

The statements of the lemma follow from putting $\beta = i$ in these results. □

The following lemma gives the orders of the subgroups denoted by H in conjectures (i) and (ii).

LEMMA 2. *Let each of m and n be a positive integer greater than* 1. *Then*

A. *Let ρ denote $1 + pi$. The order of $[\rho]$ in $\Phi_G(p^n)$ is p^{n-1}.*
B. *Let δ denote $1 + 2i$. The order of $[\delta]$ in $\Phi_G(\alpha^{2m})$ and in $\Phi_G(\alpha^{2m+1})$ is 2^{m-1}.*

Proof. Put $k = n - 1$ in (A) and $k = m - 1$ in (B) of Lemma 1. Then

$$\rho^{p^{n-1}} \equiv 1 \pmod{p^n}$$

and

$$\delta^{2^{m-1}} \equiv 1 + 2^m(a + i) \pmod{2^{m+1}}.$$

But α divides $a + i$ since a is odd, and $\alpha^{2m} \sim 2^m$. Then

$$\delta^{2^{m-1}} \equiv 1 \pmod{\alpha^{2m+1}}.$$

Then the order of $[\rho]$ in $\Phi_G(p^n)$ is a divisor of p^{n-1}, and the order of $[\delta]$ in $\Phi_G(\alpha^{2m})$ and in $\Phi_G(\alpha^{2m+1})$ is a divisor of 2^{m-1}. It suffices to show now that $\rho^{p^{n-2}} \not\equiv 1 \pmod{p^n}$ and $\delta^{2^{m-2}} \not\equiv 1 \pmod{2^m}$. Put $k = n - 2$ in (A) and $k = m - 2$ in (B) of Lemma 1. Then

$$\rho^{p^{n-2}} \equiv 1 + p^{n-1}i \not\equiv 1 \pmod{p^n},$$

and

$$\delta^{2^{m-2}} \equiv 1 + 2^{m-1}(a + i) \quad \pmod{2^m}.$$

Since 2 does not divide $a + i$, $\delta^{2^{m-2}} \not\equiv 1 \pmod{2^m}$. □

As we implied in the conjectures, we intend to use the subgroups generated by $[1 + pi]$ and $[1 + 2i]$ and denoted by H as factors in direct products. For this purpose it will be necessary to have the following lemma which asserts that no member, except the identity, of these subgroups contains a real number or a pure imaginary number.

LEMMA 3. *Let each of m and n be a positive integer greater than* 1. *Let ρ denote $1 + pi$ and δ denote $1 + 2i$. No member, except* [1], *of the subgroup of $\Phi_G(p^n)$ generated by $[\rho]$ and no member, except* [1], *of the subgroup of $\Phi_G(\alpha^{2m})$ or of $\Phi_G(\alpha^{2m+1})$ generated by $[\delta]$ can be represented by a real number or a pure imaginary number.*

Proof. Let a complex number c be called *special* if c is in Z or $c = ic_1$ for some c_1 in Z. Suppose now that δ^b is congruent (mod 2^m) to a special number, for some b satisfying $0 < b < 2^{m-1}$. Let B denote the set of all such "bad" b. First, we show that 2^{m-2} is not in B. Put $k = m - 2$ in part (B) of Lemma 1. Then

$$\delta^{2^{m-2}} \equiv 1 + 2^{m-1}(a + i) \pmod{2^m}.$$

Now supposing $\delta^{2^{m-2}}$ congruent (mod 2^m) to a special number s, we have

$$1 + 2^{m-1}a - s + 2^{m-1}i \equiv 0 \pmod{2^m}.$$

If s is real, 2^m divides 2^{m-1}. If s is imaginary, 2^{m-1} divides 1. These contradictions guarantee that 2^{m-2} is not in B. Our technique for completing the proof is Fermat's "method of descent." Let L be the least member of B and let

$$2^{m-1} = Ld + r,$$

where $0 \leqslant r < L$. If $r = 0$, then $L = 2^t$ for some t satisfying $0 < t < m - 2$. (We showed $t \neq m - 2$.) Then

$$\delta^{2^{m-2}} = \delta^{L(2^{m-2-t})}.$$

Since L is in B, δ^L is congruent (mod 2^m) to a special number. It follows that $\delta^{L(2^{m-2-t})} = \delta^{2^{m-2}}$ is also congruent (mod 2^m) to such a number, which we proved impossible. Then $r \neq 0$. Since the order of $[\delta]$ is 2^{m-1},

$$(1) \qquad [1] = [\delta^{Ld}][\delta^r] = [s][\delta^r] \text{ in } \Phi_G(2^m),$$

for some special number s. Let $s = x$ or $s = ix$ for some x in Z. Since $[s]$ is in the units group, x is odd. Then let y in Z satisfy $[yx] = [1]$ in $\Phi_Z(2^m)$. Then 2^m divides $yx - 1$ in Z, implying that 2^m divides $yx - 1$ in G, so that $[yx] = [1]$ in $\Phi_G(2^m)$. From (1) we get

$$(2) \qquad [y] = [ys][\delta^r] \text{ in } \Phi_G(2^m).$$

If $s = x$, then $[\delta^r] = [y]$. If $s = ix$, we multiply (2) by $[-i]$, getting $[-iy] = [\delta^r]$. In either case, δ^r is congruent (mod 2^m) to a special number, contradicting the minimality of L. The set B is empty. This completes the proof of the lemma as it applies to α. Replacing 2 by p and m by n, we can use the same argument to prove the lemma as it applies to p. □

6. The Structure of $\Phi_G(p^n)$. We conjectured in Section 5 that $\Phi_G(p^n) = H \times K \times R$, where H is generated by $[1 + pi]$, K has order p^{n-1}, and R has order $p^2 - 1$. We established the useful properties of H. Now we go to work on K.

We saw in Example 4 that $\Phi_Z(9)$ is included in $\Phi_G(9)$ by an obvious isomorphism. More generally, the map,

$$[a] \text{ in } \Phi_Z(p^n) \to [a] \text{ in } \Phi_G(p^n),$$

is an isomorphism. We know that $\Phi_Z(p^n)$ is cyclic and that $\phi_Z(p^n) = p^{n-1}(p - 1)$. It follows that some [a] in $\Phi_Z(p^n)$ has order p^{n-1}. The isomorphism then implies that [a] has order p^{n-1} in $\Phi_G(p^n)$. We let K be the subgroup generated by [a]. Each member of K can be represented by a real number, so that $H \cap K = \{[1]\}$ and $H \times K$ has order p^{2n-2}.

Next, we turn to R. Since p is prime in G, $G/(p)$ is a field and $\Phi_G(p)$ is cyclic, being the multiplicative group of a finite field. The order of this group is $p^2 - 1$. Let $[\beta]$ generate $\Phi_G(p)$. Then $\beta^{p^2-1} \equiv 1 (\text{mod}\, p)$ so that $\beta^{p^2-1} = 1 + \gamma p$ for some γ in G. Then from the proof of Lemma 1,

$$\left(\beta^{p^2-1}\right)^{p^{n-1}} = 1 + \eta p^n$$

for some η in G. Hence,

$$\left(\beta^{p^{n-1}}\right)^{p^2-1} \equiv 1 \pmod{p^n},$$

so $[\beta^{p^{n-1}}]$ has order t, where t divides $p^2 - 1$. It follows that $\beta^{tp^{n-1}} \equiv 1 \pmod p$, whence $p^2 - 1$ divides tp^{n-1}. Then $p^2 - 1$ divides t, so that $t = p^2 - 1$ and $[\beta^{p^{n-1}}]$ has order $p^2 - 1$ in $\Phi_G(p^n)$. We let R denote the subgroup of $\Phi_G(p^n)$ generated by $[\beta^{p^{n-1}}]$.

Now since every member of $H \times K$ has order a power of p, $(H \times K) \cap R = \{[1]\}$, and the order of $H \times K \times R$ is $p^{2n-2}(p^2 - 1) = \phi_G(p^n)$. Our conjecture has checked out; $\Phi_G(p^n) = H \times K \times R$ and we have proved the following theorem:

THEOREM 4. $\Phi_G(p^n) \simeq Z_{p^{n-1}} \times Z_{p^{n-1}} \times Z_{p^2-1}$.

Our proof of this theorem is valid only for $n > 1$, but the theorem holds also for $n = 1$. In this case $Z_{p^{n-1}}$ is trivial.

REMARK. In Example 7 the subgroups K and R can be gotten without resort to Fig. 1: Just examine the 6 members of $\Phi_Z(9)$, finding that [4] has order 3, and let K be generated by [4] in $\Phi_G(9)$. Then write out the 8 members of $\Phi_G(3)$, getting $[1 + i]$ to be a generator. Then let R be generated by $[(1 + i)^3]$ in $\Phi_G(9)$.

7. The Structure of $\Phi_G(\alpha^n)$. We conjectured in Section 5 that $\Phi_G(\alpha^n) = H \times K \times I$, where H is generated by $[1 + 2i]$ while K and I are generated by [5] and $[i]$, respectively. However, in Lemmas 2 and 3 we assumed $m > 1$ so that for $n < 4$ we determine directly the structure of $\Phi_G(\alpha^n)$. Moreover, in $\Phi_G(\alpha^4) = \Phi_G(4)$, the subgroup generated by [5] is trivial. Therefore, we give the structure of $\Phi_G(\alpha^n)$ in two theorems, the first applicable for $n = 1, 2, 3$, or 4, while the second applies if $n \geqslant 5$.

THEOREM 5. *$\Phi_G(\alpha) \simeq Z_1$, $\Phi_G(\alpha^2) \simeq Z_2$, $\Phi_G(\alpha^3) \simeq Z_4$, and $\Phi_G(\alpha^4) \simeq Z_2 \times Z_4$.*

Proof. By Theorem 2,

$$\begin{aligned}\Phi_G(\alpha) &= \{[1]\},\\ \Phi_G(\alpha^2) &= \{[1],[i]\},\\ \Phi_G(\alpha^3) &= \{[1],[3],[i],[2+i]\},\\ \Phi_G(\alpha^4) &= \{[1],[3],[i],[3i],[1+2i],[2+i],[2+3i],[3+2i]\}.\end{aligned}$$

One can verify that $[i]$ generates $\Phi_G(\alpha^3)$ and that $\Phi_G(\alpha^4)$ is the direct product of the subgroups, $\{[1], [1 + 2i]\}$ and $\{[1], [i], [3], [3i]\}$. □

Now we assume $n \geqslant 5$ and prove conjecture (i) of Section 5. We investigated the subgroup H. The properties of K that are important for us are given in the following lemma.

LEMMA 4. *Let $n \geqslant 5$. The order of K is 2^{m-2} or 2^{m-1}, according as $n = 2m$ or $n = 2m + 1$. The member $[-1]$ of $\Phi_G(\alpha^n)$ is not in K.*

Proof. The maps

$$[a] \text{ in } \Phi_Z(2^m) \to [a] \text{ in } \Phi_G(\alpha^{2m})$$

and

$$[a] \text{ in } \Phi_Z(2^{m+1}) \to [a] \text{ in } \Phi_G(\alpha^{2m+1})$$

are isomorphisms. We noted one of them in Example 5. Now $\Phi_Z(2^m)$ and $\Phi_Z(2^{m+1})$ are direct products of the subgroups generated by $[-1]$ and [5]. (See [**1**, page 46].) The order of the subgroup generated by $[-1]$ is 2. Then the order of the subgroup generated by [5] is $\phi_Z(2^m)/2$ or $\phi_Z(2^{m+1})/2$; that is, 2^{m-2} in $\Phi_Z(2^m)$ and 2^{m-1} in $\Phi_Z(2^{m+1})$. Then the given isomorphisms establish the truth of the lemma. □

Now since $[-1]$ is not in K and since $[i]$ generates I, K intersects I only at the identity. Since each member of $K \times I$ can be represented by a real number or a pure imaginary number,

$H \cap (K \times I) = \{[1]\}$. The order of $H \times K \times I$ is, therefore,

$$2^{m-1+m-2+2} = 2^{n-1} = \phi_G(\alpha^n) \text{ if } n = 2m,$$

$$2^{m-1+m-1+2} = 2^{n-1} = \phi_G(\alpha^n) \text{ if } n = 2m+1.$$

Then $\Phi_G(\alpha^n) = H \times K \times I$, and we have proved the following theorem.

THEOREM 6. *Let $n \geqslant 5$. Then*

$$\Phi_G(\alpha^n) \simeq Z_{2^{m-1}} \times Z_{2^{m-2}} \times Z_4 \text{ if } n = 2m,$$

$$\Phi_G(\alpha^n) \simeq Z_{2^{m-1}} \times Z_{2^{m-1}} \times Z_4 \text{ if } n = 2m+1.$$

8. Φ_G Is Multiplicative. Question 3 of the Introduction has been answered by Theorems 3–6. We will show now that

$$\Phi_G(\beta_1\beta_2) \simeq \Phi_G(\beta_1) \times \Phi_G(\beta_2)$$

when β_1 is prime to β_2, thus answering question 4 in the affirmative. Now it is easy to modify a "Z" proof of a version of the Chinese Remainder Theorem so as to establish that if β_1, β_2, η_1, and η_2 are members of G with β_1 prime to β_2, then there exists X in G satisfying $X \equiv \eta_1 \pmod{\beta_1}$ and $X \equiv \eta_2 \pmod{\beta_2}$. Moreover, X is unique (mod $\beta_1\ \beta_2$). These facts are helpful in establishing the following theorem.

THEOREM 7. *Let β_1 and β_2 be in G with $(\beta_1, \beta_2) = 1$. Let f map $\Phi_G(\beta_1) \times \Phi_G(\beta_2)$ to $G/(\beta_1\beta_2)$ such that*

$$f(([\eta_1], [\eta_2])) = [\eta],$$

where $\eta \equiv \eta_i \pmod{\beta_i}$ for $i = 1$ or 2. Then the image of f is $\Phi_G(\beta_1\beta_2)$ and f is an isomorphism.

Proof. The Chinese Remainder Theorem implies that f is well defined. For $i = 1$ or 2, $(\eta, \beta_i) = (\eta_i, \beta_i) = 1$ since $\eta \equiv \eta_i \pmod{\beta_i}$ and η_i is prime to β_i, being a member of $\Phi_G(\beta_i)$. Thus η is prime to $\beta_1\beta_2$ and f maps to $\Phi_G(\beta_1\beta_2)$. A routine check verifies that f is an isomorphism onto $\Phi_G(\beta_1\beta_2)$. □

EXAMPLE 8. Assuming that it might be fun to see the function f in action, we apply f to $\Phi_G(3) \times \Phi_G(\alpha^3)$. We know that $\Phi_G(3)$ is cyclic with generator $[1+i]$. (See the Remark following Theorem 4.) From Theorem 5 we have that $\Phi_G(\alpha^3) = \Phi_G(2\alpha)$ is cyclic with generator $[i]$. In view of Examples 4 and 5 and Theorems 1 and 2, we might conjecture that $G/(6\alpha) =$

$$\{[a+bi] : 0 \leqslant a \leqslant 11 \text{ and } 0 \leqslant b \leqslant 5\}$$

and that $[a+bi]$ is a unit if $a \not\equiv b \pmod 2$ and $(3, a) = 1$ or $(3, b) = 1$. This conjecture does check out, and a systematic listing of a set of representatives of $\Phi_G(6\alpha)$ might go as follows: $i, 5i, 1, 1+2i, 1+4i, 2+i, \ldots, 11+4i$. This set has 32 members, checking that $\phi_G(6\alpha) = \phi_G(3)\phi_G(\alpha^3) = 8(4)$. Now using the notation of Theorem 7 with $\beta_1 = 3$ and $\beta_2 = 2\alpha$, we let

$$\eta = \eta_1 + (3+6i)(\eta_2 - \eta_1).$$

(One who works through a proof of the Chinese Remainder Theorem can see the motivation.) Then $\eta \equiv \eta_1 \pmod 3$ and $\eta \equiv \eta_2 \pmod{2\alpha}$. For example, to find $f(([1+i], [3]))$, we let $\eta_1 = 1+i$ and $\eta_2 = 3$. Then

$$\eta = 1+i+(3-6i)(2-i) = 1-14i \equiv 7+4i \pmod{6\alpha},$$

since $12i \equiv 0 \pmod{6\alpha}$ and $7+4i = 1-2i+6\alpha$. Thus $f(([1+i], [3]))$ is $[7+4i]$. Fig. 2 is a display of f in its entirety. In this display we omit the brackets that denote equivalence classes. In the upper left corner we isolate the subgroup $\Phi_G(3) \times \{[1]\}$, which is, of course, isomorphic to $\Phi_G(3)$; in the upper right we isolate $\{[1]\} \times \Phi_G(2\alpha)$. We denote the images of these subgroups by S and T. The reader who wishes to practice his computational skills is urged to show directly that

$[1+4i]$ in $\Phi_G(6\alpha)$ generates S and $[10+3i]$ generates T. It is clear that $S \cap T = \{[1]\}$, so that $\Phi_G(6\alpha) = S \times T$.

$$\Phi_G(3) \times \Phi_G(2\alpha) \xrightarrow{f} \Phi_G(6\alpha)$$

$(1,1)$	$\xrightarrow{f}$	1	S	$(1,1)$	$\xrightarrow{f}$	1	T
$(1+i,1)$		$1+4i$		$(1,i)$		$10+3i$	
$(2i,1)$		$3+2i$		$(1,3)$		7	
$(1+2i,1)$		$7+2i$		$(1,2+i)$		$4+3i$	
$(2,1)$		5					
$(2+2i,1)$		$11+2i$		$(2i,2+i)$		$6+5i$	
$(i,1)$		$9+4i$		$(1+i,3)$		$7+4i$	
$(2+i,1)$		$5+4i$		$(1+i,i)$		$4+i$	
				$(1+i,2+i)$		$10+i$	
$(2,3)$		11		$(1+2i,3)$		$1+2i$	
$(2,i)$		$2+3i$		$(1+2i,i)$		$4+5i$	
$(2,2+i)$		$8+3i$		$(1+2i,2+i)$		$10+5i$	
$(i,3)$		$3+4i$		$(2+i,3)$		$11+4i$	
(i,i)		i		$(2+i,i)$		$8+i$	
$(i,2+i)$		$6+i$		$(2+i,2+i)$		$2+i$	
$(2i,3)$		$9+2i$		$(2+2i,3)$		$5+2i$	
$(2i,i)$		$5i$		$(2+2i,i)$		$8+5i$	
				$(2+2i,2+i)$		$2+5i$	

FIG. 2.

9. Primitive Roots. Theorem 3 says that $\Phi_G(\pi^n)$ is cyclic, Theorem 4 implies that $\Phi_G(p^n)$ is cyclic only if $n = 1$, while Theorems 5 and 6 yield that $\Phi_G(\alpha^n)$ is cyclic only if $n \leqslant 3$. We summarize:

Group	Order	Cyclic?
$\Phi_G(\pi^n)$	$q^{n-1}(q-1)$	yes
$\Phi_G(p^n)$	$p^{2n-2}(p^2-1)$	only if $n = 1$
$\Phi_G(\alpha^n)$	2^{n-1}	only if $n \leqslant 3$

Thus α, α^2, α^3, π^n, and p have primitive roots. The product of cyclic groups is cyclic if and only if their orders are relatively prime. Then $\alpha\pi^n$ and αp also have primitive roots, but these are the only additional ones that we get in this manner. We therefore have the following theorem.

THEOREM 8. *The Gaussian integers α, α^2, α^3, π^n, p, $\alpha\pi^n$, and αp have primitive roots. These and their associates are the only Gaussian integers having primitive roots.*

As we mentioned in the Introduction, Crowe proves Theorem 8. Since his paper is unpublished, we comment on his methods. Versions of Theorems 1–3 appear in his work, so that he obtains that $\Phi_G(\pi^n)$ is cyclic. He then observes that $\Phi_Z(2^m)$ or $\Phi_Z(2^{m+1})$ is included isomorphically in $\Phi_G(\alpha^n)$, implying that α^n has no primitive root if $n > 3$. Finally, for $n > 1$, he finds two distinct subgroups of order p in $\Phi_G(p^n)$, implying that $\Phi_G(p^n)$ is not cyclic.

References

1. Ethan D. Bolker, Elementary Number Theory, W. A. Benjamin, New York, 1970.
2. Michael S. Crowe, An extension of the Euler ϕ-function to the Gaussian Integers, Senior Honors paper, 1974, unpublished. Available at the duPont Library, The University of the South.
3. Ivan Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, 4th ed., Wiley, New York, 1980.
4. Henry B. Mann, Introduction to Algebraic Number Theory, The Ohio State University Press, 1955.