Thus, $\{\varepsilon_n\}$ *is a periodic sequence*, with period 6 and

$$\varepsilon_1 = u_1 - v_1 = u_1 + u_2 - u_3,\ \varepsilon_2 = u_2 - v_2 = u_2 + u_3 - u_4,\ \varepsilon_3 = \varepsilon_2 - \varepsilon_1,$$
$$\varepsilon_4 = -\varepsilon_1, \qquad \varepsilon_5 = -\varepsilon_2, \qquad \varepsilon_6 = -\varepsilon_3.$$

3. Hence

$$u_n + v_n = F_n$$
$$u_n - v_n = \varepsilon_n = \varepsilon_{[n]} \quad \text{(where } [n] = n \text{ modulo } 6\text{)},$$

and

$$\boxed{u_n = \tfrac{1}{2}(F_n + \varepsilon_{[n]})} \qquad (n > 4).$$

Now F_n may be written in the form (using the Binet formula):

$$F_n = (u_1 - u_2 + u_3)N_{n-2} + (u_2 - u_3 + u_4)N_{n-1},$$

where N_n is the integer closest to

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n$$

(see, for instance, N. N. Vorob'ev, *Fibonacci Numbers*, Blaisdell Publishing Company, 1961, page 22).

Remarks: 1. The method used makes obvious the following relations:

$$u_n + u_{n+3} = \tfrac{1}{2}(F_n + F_{n+3}) = F_{n+2},$$
$$u_{n+6} - u_n = \tfrac{1}{2}(F_{n+6} - F_n) = 2F_{n+3}, \ \ldots\ .$$

2. Any sequence $\{\varepsilon_n\}$ and any Fibonacci sequence are solutions of the given recurrent equation (directly or by our formula).

*****

PRIMENESS FOR THE GAUSSIAN INTEGERS

RICHARD C. WEIMER
Frostburg State College, Frostburg, Maryland

Complex numbers of the form $a + bi$, where a and b are integers, are commonly called Gaussian Integers. It can be shown that the Gaussian Integers, denoted by G, along with addition and multiplication of complex numbers, form an integral domain. One might suspect that many properties about the integers, denoted by Z, carry over to G. This is indeed the case, and it is the purpose of this paper to examine the property of primeness in the Gaussian domain. The Fundamental Theorem of Arithmetic states that every integer is either a prime or can be uniquely factored into a product of primes, apart from the order in which the factors appear. This theorem also holds for G. It is also true that both G and Z are unique factorization domains. For Z, the units are 1 and -1, while the units for G are 1, -1, i, and $-i$. The job at hand, then, is to determine what elements of G are prime.

For each $\alpha \in G$, $\alpha \cdot \overline{\alpha}$, where $\overline{\alpha}$ is the conjugate of α, is called *the norm of* α and is denoted by $N(\alpha)$. Thus for $a,b \in Z$, $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. It also follows that for $\alpha,\beta \in G$, $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

Since G is a unique factorization domain, any $\alpha \in G$ can be factored into a product of primes. Therefore, suppose $\alpha = p_1 \cdot p_2 \cdot \ldots \cdot p_n$, where the p_i's ($i = 1, 2, \ldots, n$) are prime in G. We thus have $N(\alpha) = N(p_1) \cdot N(p_2) \cdot \ldots \cdot N(p_n)$. Hence, any factorization of $\alpha \in G$ leads to a corresponding factorization of $N(\alpha)$ in Z. As a result, α is prime in G if $N(\alpha)$ is prime in Z. As an illustration of these results, consider $\alpha = 3 + 7i$. Since $N(\alpha) = 9 + 49 = 58 = 2 \cdot 29$, $3 + 7i$ has at most two prime factors having norms 2 and 29. Those elements of G with norm 2 are $1 \pm i$. Selecting $1 + i$ and solving the equation $(3 + 7i) = (1 + i)(x + iy)$ for x and y, one discovers that $(3 + 7i) = (1 + i)(5 + 2i)$. If $1 - i$ were chosen, $3 + 7i = (1 - i)(-2 + 5i)$. This appears at first glance to be a different factorization, but observe that $(3 + 7i) = -i(1 - i)(5 + 2i)$ where $-i$ is a unit. Note also that $N(5 + 2i) = 29$. Hence, $(1 + i)(5 + 2i)$ is a prime factorization of $3 + 7i$.

We now have a procedure for determining whether a Gaussian integer of the form $a + bi$, $a,b \neq 0$, is prime in G. What remains is to find a method for determining whether or not

an integral prime ($a + bi$, $b = 0$) is prime in G. Then the same method would apply for $a + bi$ when $a = 0$, since i is a unit.

If an integral prime p does not remain prime in G, then p can be written in the form $p = x^2 + y^2$ where $x,y \in Z$. This can be seen by letting $p = \alpha \cdot \beta$ where α,β are not units and $\alpha = a + bi$. Then $N(p) = N(\alpha) \cdot N(\beta)$ implies $p^2 = N(\alpha) \cdot N(\beta)$. As a result, $p = N(\alpha)$, since p is prime in Z. Hence, $p = a^2 + b^2$. As a consequence of this result, note, for example, 2, 5, 13, and 29 are not prime in G and $2 = 1^2 + 1^2$, $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, and $29 = 5^2 + 2^2$. On the other hand, 3, for example, is prime in G and $3 \neq x^2 + y^2$ for any $x,y \in Z$.

A sufficient condition for $p \in Z$ to be prime in G is $p \equiv 3 \pmod 4$. To see why this is the case, let $p = 4n + 3$ for some $n \in Z$. Assume p is not prime in G. By the result just established above, $p = x^2 + y^2$. Thus $x^2 + y^2 = 4n + 3$ implies $x^2 + y^2 \equiv 3 \pmod 4$. Now if $x^2 + y^2 \equiv 3 \pmod 4$, x and y cannot both be even or odd. Therefore, without loss of generality, let $x = 2m + 1$ be odd and $y = 2r$ be even. Then $(2m + 1)^2 + (2r)^2 \equiv 3 \pmod 4$. But this implies $2(m^2 + m + r^2) \equiv 1 \pmod 2$, which is absurd. Hence, p is prime in G. As examples, note 3, 7, 11, and 19 are all congruent to 3 (mod 4) and 3, 7, 11, and 19 are primes in Z that are also prime in G.

It turns out that $p \equiv 3 \pmod 4$ is also a necessary condition for an integral prime to be prime in G. If p is an integral prime and either $p \equiv 1 \pmod 4$ or $p \equiv 2 \pmod 4$, then p is not prime in G. For if $p \equiv 2 \pmod 4$, then p is even and equals 2. But $2 = (1 + i)(1 - i)$ and hence is not prime in G. In order to establish the remaining case, the result "If $p \equiv 1 \pmod 4$, then there exists an $x \in Z$ such that $x^2 \equiv -1 \pmod p$" will be used without proof (see Schockley, p. 139). Let p be an integral prime and $p \equiv 1 \pmod 4$. Therefore, there exists an $x \in Z$ such that $x^2 + 1 \equiv 0 \pmod p$. But this implies that $p \mid (x + i)(x - i)$. Moreover, if p is prime in G, then either $p \mid (x + i)$ or $p \mid (x - i)$. In either case, $p = \pm 1$, a contradiction. Hence p is not prime in G. As a consequence of this result, integral primes such as 5, 13, and 29 are not prime in G since 5, 13, and 29 are all congruent to 1 (mod 4).

If p is prime in Z and $p \equiv 1 \pmod 4$, then p is not prime in G and $p = x^2 + y^2$; this being a consequence of the above remarks. Now $x + iy$ is prime in G since $N(x + iy) = x^2 + y^2 = p$, which is prime in Z. Therefore, to determine a factorization of an integral prime p in G, one needs only obtain the perfect squares contained in p and test pairwise sums of squares. For example, consider 29, which is not prime in G. The perfect squares contained in 29 are 1, 4, 9, 16, and 25. Since $29 = 4 + 25$, $29 = (2 + 5i)(2 - 5i)$.

REFERENCE

James E. Shockley. *Introduction to Number Theory*. New York: Holt, Rinehart, and Winston, Inc., 1967.

*****

A NOTE ON ORDERING THE COMPLEX NUMBERS

RICHARD C. WEIMER
Frostburg State College, Frostburg, Maryland

Many order relations can be defined on C. One of the most common orderings is the dictionary or lexicographical ordering. This order behaves in much the same way that the words are arranged in the dictionary. If the symbol "$\textcircled{<}$" is used to denote this order ("$\textcircled{<}$" is read "less than"), then $(a,b) \textcircled{<} (c,d)$ iff $a < c$, or $a = c$ and $b < d$. One can easily verify that $\textcircled{<}$ satisfies the definition of an order relation on C. Thus, $0 \textcircled{<} i$, $2 + 3i \textcircled{<} 3 + 16i$, $2 + 7i \textcircled{<} 2 + 10i$, $-3 - i \textcircled{<} 4$, etc.

Another ordering of C closely related to the dictionary ordering is the antilexicographical ordering. This ordering ($\boxed{<}$) is defined as: $(a,b) \boxed{<} (c,d)$ iff $b < d$ or $b = d$ and $a < c$. It is also an easy matter to verify that $\boxed{<}$ is an order relation on C.

As another illustration, one can show that Δ defined by $(a,b) \Delta (c,d)$ iff $\sqrt{a^2 + b^2} < \sqrt{c^2 + d^2}$, or $\sqrt{a^2 + b^2} = \sqrt{c^2 + d^2}$ and $\tan^{-1}(b/a) < \tan^{-1}(d/c)$ is an ordering of C. Thus $(1,2) \Delta (2,3)$ since $\sqrt{1^2 + 2^2} < \sqrt{2^2 + 3^2}$, and $(\sqrt{3},1) \Delta (\sqrt{2},\sqrt{2})$ since $\sqrt{(\sqrt{3})^2 + 1^2} = \sqrt{(\sqrt{2})^2 + (\sqrt{2})^2}$ and $\tan^{-1}(1/\sqrt{3}) = \pi/6$ $\tan^{-1}(\sqrt{2}/\sqrt{2}) = \pi/4$.

As a final illustration, any one-to-one correspondence between C and the members of an ordered set can be used to establish an order relation on C or any infinite subset of C, such as $G^+ = \{(a,b) \in Z \times Z \mid a,b > 0\}$. For example, consider the natural numbers with the usual ordering and the following list: