THE RATIONAL ZERO THEOREM EXTENDED

Leonard L. Palmer

Southeast Missouri State University

Introduction. In college algebra classes the students are taught how to find zeros of polynomials such as $P(x) = x^4 - 4x^3 + 6x^2 - 4x + 5$. Normally the Rational Zero Theorem is applied to find the possible rational zeros to be ± 1 or ± 5. A quick check will reveal that none of these possibilities are zeros of $P(x)$. Since $P(x) = (x-1)^4 + 4 \geq 4$, $P(x)$ does not have real zeros. So the question is, how do we find the four complex zeros? A complex zero of the form $\alpha = a + bi$, where a and b are integers is usually given. The fact that the conjugate of α, denoted by $\overline{\alpha} = a - bi$ is also a zero is used to finish finding all the zeros.

Consider the fact that $5 = 2^2 + 1^2 = (2+i)(2-i)$. It would seem that $2+i$ and $2-i$ are divisors of 5. We can calculate $P(x) \div (x - (2+i))$ by synthetic division. We have

$$\begin{array}{r|rrrrr} 2+i & 1 & -4 & 6 & -4 & 5 \\ & & 2+i & -5 & 2+i & -5 \\ \hline & 1 & -2+i & 1 & -2+i & 0 \end{array}$$

so that $2+i$ is a zero of $P(x)$. Therefore, $\overline{2+i} = 2-i$, the other divisor of 5, is a zero and we have

$$\begin{array}{r|rrrr} 2-i & 1 & -2+i & 1 & -2+i \\ & & 2-i & 0 & 2-i \\ \hline & 1 & 0 & 1 & 0 \end{array}$$

Finally, $P(x) = (x-2-i)(x-2+i)(x^2+1) = (x-2-i)(x-2+i)(x+i)(x-i)$.

The purpose of this paper is to generalize the Rational Zero Theorem to complex numbers of the form $\alpha = a + bi$, where a and b are integers. The set G of all numbers of this type are called Gaussian Integers. This set with the ordinary operations of addition and multiplication is an Integral Domain without order. We can define the notion of a divisor in the same way it is done for the set of integers. Denote the set of integers by I.

Some Number Theory in G.

Definition 1. If $\alpha = \beta\gamma$, $(\beta \neq 0)$ where α, β, $\gamma \in G$ then we say that β is a divisor (factor) of α and write $\beta | \alpha$.

Using this definition the divisibility properties of G are, by and large, the same as they are for the integers and are proven in the same manner. The notion of a prime in G is more general than the definition of a prime in I.

Definition 2. A unit in G is an element in G that has a multiplicative inverse in G.

Example 1. Because $(i)(-i) = 1$, $(-1)(-1) = 1$ and $1 \cdot 1 = 1$, we have 1, -1, i and $-i$ are units in G.

Definition 3. An element π in G is a prime in G if every factorization of $\pi = \alpha\beta$ in G requires α or β to be a unit.

Example 2. Note that $5 = (2+i)(2-i)$ where neither $2+i$ or $2-i$ are units. So 5 is not a prime in G.

What is needed now is a method to determine primes in G. For the same reason 5 is not a prime in G we have $13 = (2^2 + 3^2) = (2+3i)(2-3i)$ is not a prime in G.

Definition 4. The norm of $\alpha \in G$ is $\alpha\overline{\alpha}$ and we write $N(\alpha) = \alpha\overline{\alpha}$. Notice that the norm is a nonnegative integer. The following theorem gives the main properties of $N(\alpha)$.

Theorem 1. For α, $\beta \in G$,

(i) $N(\alpha) = 0$ if and only if $\alpha = 0$,
(ii) $N(\alpha\beta) = N(\alpha)N(\beta)$,
(iii) $N(\alpha) = 1$ if and only if α is a unit, and
(iv) 1, -1, i, $-i$ are the units of G.

Using the norm, N, of a Gaussian integer in G we can gain some knowledge of the primes in G. Recall that the positive odd primes in I have the form $4k+1$ or $4k+3$. Further, if p is a prime of the form $4k+1$, then $p = a^2 + b^2$ for some $a, b \in I$.

Theorem 2. If p is a positive odd prime in I and $p = 4k+1$, then p is not a prime in G.

Proof. Suppose $p = 4k+1$. Then $p = a^2 + b^2 = (a+bi)(a-bi)$. Since $N(a+bi) = N(a-bi) = a^2 + b^2 > 1$, neither of $a+bi$ or $a-bi$ can be units. Therefore p is not a prime in G.

Theorem 3. If p is a positive odd prime in I and $p = 4k+3$ then p is a prime in G.

Proof. Suppose $p = \alpha\beta$ in G. Then $p^2 = N(p) = N(\alpha)N(\beta)$. Because the factors of p^2 are 1, p and p^2 either $N(\alpha) = 1$, $N(\alpha) = p$ or $N(\alpha) = p^2$. For $N(\alpha) = 1$ we have α is a unit and p is a prime. If $N(\alpha) = p$ then $p = N(\alpha) = N(a+bi) = a^2 + b^2$. But this implies p is a sum of two squares in I, which can't be, since p is of the form $4k+3$. Now $N(\alpha) = p^2$ gives $N(\beta) = 1$ and β is a unit. Thus, p is a prime in G.

Theorem 4. If $\alpha = a + bi$ where $N(\alpha) = a^2 + b^2 = p$, a prime in I, then α is a prime in G.

Proof. Suppose $\alpha = \beta \cdot \gamma$ then $N(\beta)N(\gamma) = N(\alpha) = p$, and $N(\beta) = 1$ or $N(\gamma) = 1$ so one of β or γ is a unit.

With Theorems 1 through 4 we can factor elements of I in the set G. We see that the primes $2, 5, 13, 17, 29$, and all primes of the form $4k+1$ in I are not primes in G. All the odd primes of the form $4k+3$ in I, such as $3, 7, 11, 19$ and 23 remain primes in G. Any element $\alpha = a + bi$ in G, such that $N(\alpha) = a^2 + b^2$ is a prime in I, is a prime in G.

Example 3. Consider the integer 35. In the set I, $35 = 5 \cdot 7$, which is the prime factorization in this set. But 5 has the form $4k+1$ so it can be factored in G as $35 = 5 \cdot 7 = (1^2 + 2^2) \cdot 7 = (-i)(i)(1+2i)(1-2i) \cdot 7$.

Example 4. The integer $42 = 2 \cdot 3 \cdot 7 = (-i)(i)(1+i)(1-i)(3)(7)$ in G.

Example 5. The Gaussian integer $\alpha = 3 + 5i$ is not a prime in G. To see this notice that

$$\begin{aligned} \alpha\overline{\alpha} &= N(3+5i) = 9 + 25 = 34 = 2 \cdot 17 = N(1+i)N(1+4i) \\ &= N(1+i)N(4+i) = N(1-i)N(4-i) = N(1-i)N(1-4i). \end{aligned}$$

By considering this equation we notice that $3 + 5i = (1+i)(4+i)$.

Notice that $35 = (2^2 + 1^2) \cdot 7 = (2+i)(2-i) \cdot 7$ also. A question arises here. What is the relationship between the factors $1 + 2i$, $1 = 2i$, $2 + i$, and $2 - i$? The connection here is $1 + 2i = i(2-i)$ and $1 - 2i = -i(2+i)$ where i and $-i$ are units. This is the same relationship in G as 5 and -5 are related in I. We have $-5 = (-1)(5)$ where -1 is a unit in I. Abstractly speaking we consider $1 + 2i$, $(-1)(1+2i)$, $i(1+2i)$, and $(-i)(1+2i)$ as the same prime in G.

Some Examples.

This brings us back to the purpose of this paper, which is to find the zeros of a polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \text{ where } a_i \in I \text{ for } 0 \le i \le n. \tag{1}$$

Example 6. To find the zeros of $f(x) = x^4 - 2x^3 + 4x - 4$ we see that ± 1, ± 2, and ± 4 are the possible rational zeros. None of these are actual zeros of $f(x)$. By factoring 4 in G we see that $\pm i$, $\pm 2i$, $\pm 4i$, $\pm(1+i)$, $\pm(1-i)$, $\pm 2(1+i)$, $\pm 2(1-i)$, $\pm 2i(1+i)$, $\pm 2i(1-i)$ are possible zeros. By synthetic division we see that $1 + i$ and $1 - i$ are zeros so that

$$f(x) = (x-1-i)(x-1+i)(x^2-2) = (x-1-i)(x-1+i)(x-\sqrt{2})(x+\sqrt{2}).$$

In Example 6, if we had used some method of approximating the irrational real roots, as is usually the case, we would have approximations to $\pm\sqrt{2}$. But how often can we recognize the surds that we are approximating? It would not have been easy to find the other quadratic factor $x^2 - 2x + 2$ of $f(x)$.

Example 7. Find the zeros of $f(x) = x^6 + 3x^5 - 3x^4 + 6x^3 - 9x^2 + 3x - 5$. If we do not know what the zeros are we would look at $5 = 1 \cdot 5 = (-i)(i)(5) = (-i)(i)(1+2i)(1-2i)$ the prime factorization of 5 in G and conclude that the possible zeros are ± 1, ± 5, $\pm i$, $\pm 5i$, $\pm(1+2i)$, $\pm(1-2i)$, $\pm i(1+2i)$, and $\pm i(1-2i)$. Checking these in the order they are written we find that,

$$\begin{aligned} f(x) &= (x+i)^2(x-i)^2(x^2+3x-5) \\ &= (x+i)^2(x-i)^2\left(x + \frac{3-\sqrt{29}}{2}\right)\left(x + \frac{3+\sqrt{29}}{2}\right), \end{aligned}$$

with zeros,

$$i, i, -i, -i, \frac{-3+\sqrt{29}}{2} \text{ and } \frac{-3-\sqrt{29}}{2}.$$

Example 8. Find the zeros of $f(x) = 4x^3 + 23x^2 + 34x - 10$. We need to factor the leading coefficient and constant term into units and primes. We have $10 = 2 \cdot 5 = (-1)(-1)(1)(-i)(i)(1-i)(1+i)(1-2i)(1+2i)$ and $4 = (-1)(-1)(1)(-i)(i)(1-i)^2(1+i)^2$. The possible zeros are α/β where α is a divisor of 10 and β is a divisor of 4. For this example the zeros are $-3+i$, $-3-i$ and $1/4$. Note that $-3+i = (1+i)(-1+2i) = (-1)(-1-i)(1-2i)$ where each of the factors of $-3+i$ is a divisor of 10.

Conclusion.

The previous discussion gives methods for solving polynomials such as those given in (1). This discussion can be extended to polynomials such as $f(x) = x^3 + ix^2 - (7-i)x + (6-6i)$. Here we have $6 - 6i = 6(1-i) = 2 \cdot 3 \cdot (1-i) = (1+i)(1-i)^2 \cdot 3$, the prime factorization of $6-6i$ in G. Again by synthetic division one finds that $1-i$ is a zero. This leads to $f(x) = (x-1+i)(x^2+x+6) = (x-1+i)(x+3)(x-2)$, so the zeros are 1, $-i$, 2 and -3.

Of course a generalized version of the Rational Zero Theorem could be stated for polynomials of the form (1) where the coefficients are Gaussian Integers. This generalized theorem would give possible zeros of the form $s+ti$ where s and t are rational numbers. Zeros of this form would be in the quotient field of G.