Quadratic Prime-Generating Polynomials Over the Gaussian Integers

Frank Fuentes* Monta Meirose† Erik R. Tou‡§

March 23, 2017

1 Introduction

In 1772 [2], the Swiss mathematician Leonhard Euler discovered that the polynomial $x^2 - x + 41$ is prime for $x = 0, 1, \ldots, 40$. For this reason, it is called a prime-generating polynomial. Since then, much attention has been devoted to the problem of finding other such polynomials. In 1995, Boston and Greenwood [1] used a computer to find several quadratic polynomials that are frequently prime for $x = 0, 1, \ldots, 99$. Their best ones were $(x - 65)^2 + (x - 65) + 41$, $4(x - 40)^2 + 2(x - 40) + 41$, $2(x - 117)^2 - 199$, which produce 95, 88, and 85 primes, respectively, on this interval.[1] (Euler's own polynomial produces a respectable 86 primes.) Their paper also included an explanation of which polynomials are more likely to be prime-generating, and details on how to carry out a computer search to find them.

In this paper, we carry out a similar search for polynomials of the form $f(z) = \alpha z^2 + \beta z + \gamma$, where the coefficients α, β, γ and variable z are Gaussian integers (numbers of the form $a + bi$, where a and b are integers and $i = \sqrt{-1}$). The key geometric difference is that the integers $\mathbb{Z}$ have a natural linear ordering, while the Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ form a square array in the complex plane $\mathbb{C}$ and have no such ordering. Rather, they are divided into *quadrants* in the same way as the Euclidean plane; in particular, the first quadrant is defined as those Gaussian integers $\alpha = a + bi$ with $a > 0$ and $b \geq 0$. A Gaussian integer $\alpha = a + bi$ also possesses a *norm* $N(\alpha) = a^2 + b^2$ (the square of its magnitude in $\mathbb{C}$) and a *complex conjugate* $\overline{\alpha} = a - bi$ (its reflection over the real axis).

Other features of the integers can be translated into the realm of Gaussian integers with some small changes. For example, an integer n with $|n| > 1$ is

*Seattle University
†Morningside College
‡University of Washington, Tacoma
§This work was supported by NSF grant DMS-1460537.
[1]Some values from the table on p. 596 of [1] are incorrect, and the values given here have been recomputed.

prime if it is only divisible by ± 1 and $\pm n$, while a Gaussian integer α with $N(\alpha) > 1$ is prime if it is only divisible by ± 1, $\pm i$, $\pm\alpha$, and $\pm i\alpha$. (The number of possible variants is governed by the fact that there are four Gaussian integers with multiplicative inverses in $\mathbb{Z}[i]$, namely 1, -1, i, and $-i$. We call these the Gaussian *units*.) Additionally, while an even integer is one that is divisible by the smallest prime integer, 2, an even Gaussian integer is divisible by the smallest prime Gaussian integer, $1 + i$. The same parity relations exist for Gaussian integers as exist for integers: an odd plus an odd is even, an even plus an odd is odd, etc.

In what follows, we modify Boston and Greenwood's work in [1] to identify the most likely prime-generating polynomials with Gaussian integer coefficients and design computer search for the Gaussian polynomials that are best at generating primes. We conclude with a theoretical result on prime-generating efficiency that does not depend on probabilities or computations.

2 Gaussian Integer Polynomials

The methods for finding prime-generating integer polynomials generalize easily to the Gaussian integer case. First, the *discriminant* of an integer quadratic polynomial $f(x) = ax^2 + bx + c$ is $D_f = b^2 - 4ac$. (Readers will be most familiar with the discriminant as the expression appearing under the square root in the quadratic formula.) Alternatively, one can define $D_f = a^2(r_1 - r_2)^2$, where r_1 and r_2 are the roots of $f(x)$. Because of the quadratic formula, an integer quadratic polynomial with square discriminant will factor nontrivially over $\mathbb{Z}$. It is easy to see that a factorable polynomial is less likely to generate prime outputs.

Taking this idea a bit further, Boston and Greenwood [1] examined discriminants of integer polynomials and found that polynomials were more likely to be prime-generating when their discriminants were not squares modulo p, for many odd small primes p. To see how the discriminant's status as a modular square can hamper the polynomial's efficiency, consider the polynomials $f(x) = x^2 - x + 41$ and $g(x) = x^2 + x - 39$. Their discriminants are $D_f = -163$ and $D_g = 157$. As noted above, $f(x)$ is prime for 86 values of x in $[0, 99]$. However, $g(x)$ is prime for only 23 values of x in this interval. This is because D_f is not a square for any odd primes up to 37, while D_g is (in particular) a square modulo 3. Thus, $g(x)$ will factor modulo 3: $x^2 + x - 39 \equiv x^2 + x \equiv x(x + 1) \pmod 3$, so that $g(x)$ will be divisible by 3 whenever x or $x + 1$ is divisible by 3, which happens for 67 of the values in the test space. Since this clearly makes it more difficult for the polynomial to produce prime outputs, one criterion for a polynomial $f(x)$ to be prime-generating is that D_f not be a square for any of the primes in a predetermined set.

The language of divisibility and modular arithmetic can also be applied to the Gaussian integers; we choose to follow the approach given by Rosen [5], including the following form of the division algorithm.

Theorem 1 *For α, $\mu \in \mathbb{Z}[i]$ with $\mu \neq 0$, there exist κ, $\rho \in \mathbb{Z}[i]$ so that $\alpha = \kappa\mu + \rho$ and $N(\rho) < N(\mu)$.*

The key difference with the integer case is that the quotient κ and remainder ρ are not unique. For example, suppose we wish to divide $\alpha = 8+7i$ by $\mu = 2+3i$. One possible solution is $8+7i = (2-i)(2+3i)+(1+3i)$ (and it's easy to see that $N(1+3i) < N(2+3i)$). However, we could also take $8+7i = (3-i)(2+3i)+(-1)$, which is equally valid. In general, there are always four possible remainders that lie in the square in the complex plane whose midpoints are at $\pm\mu$ and $\pm i\mu$. If this square is subdivided into 4 smaller squares, each subsquare will contain exactly one of the four remainders. We will call the remainder lying in the subsquare with opposite corners at μ and $i\mu$ the *standard* remainder ρ. In the above example, the four remainders are -1, $2-2i$, $3+i$ and $1+3i$, with $3+i$ being the standard one (see Figure 1 below).

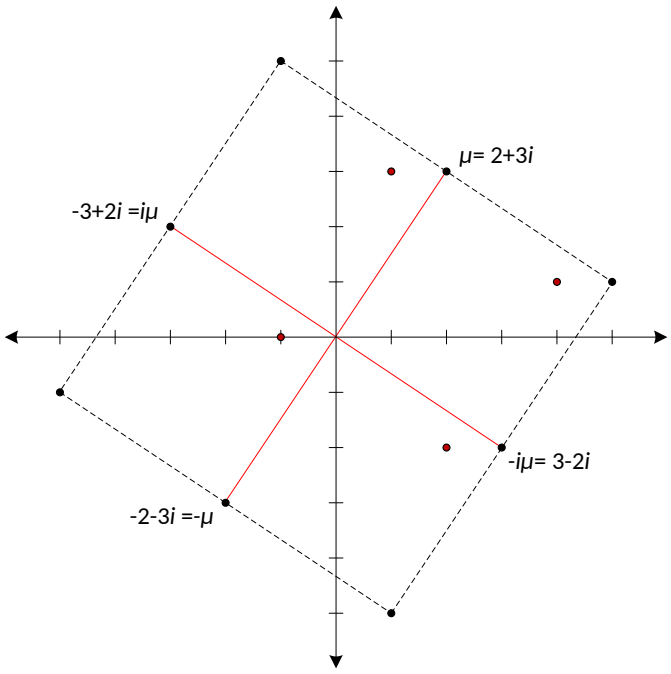

Figure 1: Remainders obtained from dividing $\alpha = 8+7i$ by $\mu = 2+3i$. The four possible remainders (-1, $2-2i$, $3+i$ and $1+3i$) all lie in a square with $\pm(2+3i)$ and $\pm i(2+3i)$ at the midpoints. The standard remainder, $1+3i$, lies in the upper left quadrant of the square.

Modular arithmetic may now be defined in the same way as in the integers, with the set of all possible standard remainders making up the residues modulo μ. Last of all, we define the *efficiency* of a polynomial $f(z)$ with Gaussian integer coefficients as the proportion of prime outputs for z values in the test space $\mathcal{T} = \{z = a + bi \in \mathbb{Z}[i] \mid -10 < a, b < 10\}$.

Taking all of this into account, we return to the discriminant-based approach described above. Define the following set $\mathcal{S}$ of small Gaussian primes as, listed in order of increasing norm:

$$\begin{aligned}\mathcal{S} \;=\; &\{2+i, 1+2i, 3, 3+2i, 2+3i, 4+i, 1+4i, 5+2i, 2+5i,\\ &\quad 6+i, 1+6i, 5+4i, 4+5i, 7, 7+2i, 2+7i, 6+5i, 5+6i\}.\end{aligned}$$

Further define $\mathcal{S}_n$ to be the subset containing the first n elements from $\mathcal{S}$. Next, following [1], we say that a Gaussian quadratic polynomial $f(z) = \alpha z^2 + \beta z + \gamma$ is *worthy* of testing if it meets two conditions:

1. *Parity condition.* $\alpha + \beta$ is even and γ is odd.
2. *Discriminant condition.* The discriminant $D_f = \beta^2 - 4\alpha\gamma$ is not a square modulo μ, for any $\mu \in \mathcal{S}_n$ (for some $n \geq 1$).

Note that the parity condition guarantees that every output value $f(z)$ will be odd. Sometimes we will indicate the value of n in the discriminant condition, as "n-worthy" (e.g., $f(z)$ is 11-worthy if it meets the discriminant condition for all primes in $\mathcal{S}_{11}$). When n is not specified it is assumed that the statement in question refers to a general n.

3 Searching Efficiently

Since the Gaussian integers form a square array in the complex plane, the symmetries of the array give rise to families of equivalent polynomials. This is similar to the integer case [1], in which two polynomials $f(x)$ and $g(x)$ are equivalent if $f(x) = g(n \pm x)$ for some integer n. Here, we say that two Gaussian polynomials $f(z)$ and $g(z)$ are equivalent if $g(z)$ can be obtained from $f(z)$ by a combination of the following moves:

- *Conjugation.* Given $f(z) = \alpha z^2 + \beta z + \gamma$, define $\overline{f}(z) = \overline{\alpha} z^2 + \overline{\beta} z + \overline{\gamma}$.
- *Post-multiplication by a unit.* Take $u \cdot f(z) = (u\alpha)z^2 + (u\beta)z + u\gamma$, where u is any unit.
- *Pre-multiplication by a unit.* Take $f(u \cdot z) = (\alpha u^2)z^2 + (u\beta)z + \gamma$, where u is any unit.
- *Translation.* Take $f(z - t) = \alpha(z-t)^2 + \beta(z-t) + \gamma = \alpha z^2 + (-2\alpha t + \beta)z + (\alpha t^2 - \beta t + \gamma)$, where t is any Gaussian integer.

As an example, consider the polynomial $f(z) = z^2 + (7 + 4i)z + (5 + 4i)$. In Figure 2, we see why $if(z)$, $f(iz)$, and $\overline{f}(z)$ give different expressions of the same situation, at least as it pertains to prime-generating efficiency. In the first case, multiplying the output by i does not change primality or compositeness, so the primality plots for $if(z)$ and $f(z)$ are the same. The polynomial $f(iz)$ rotates the domain, while $\overline{f}(z)$ reflects it, providing related plots with the same efficiency as $f(z)$.

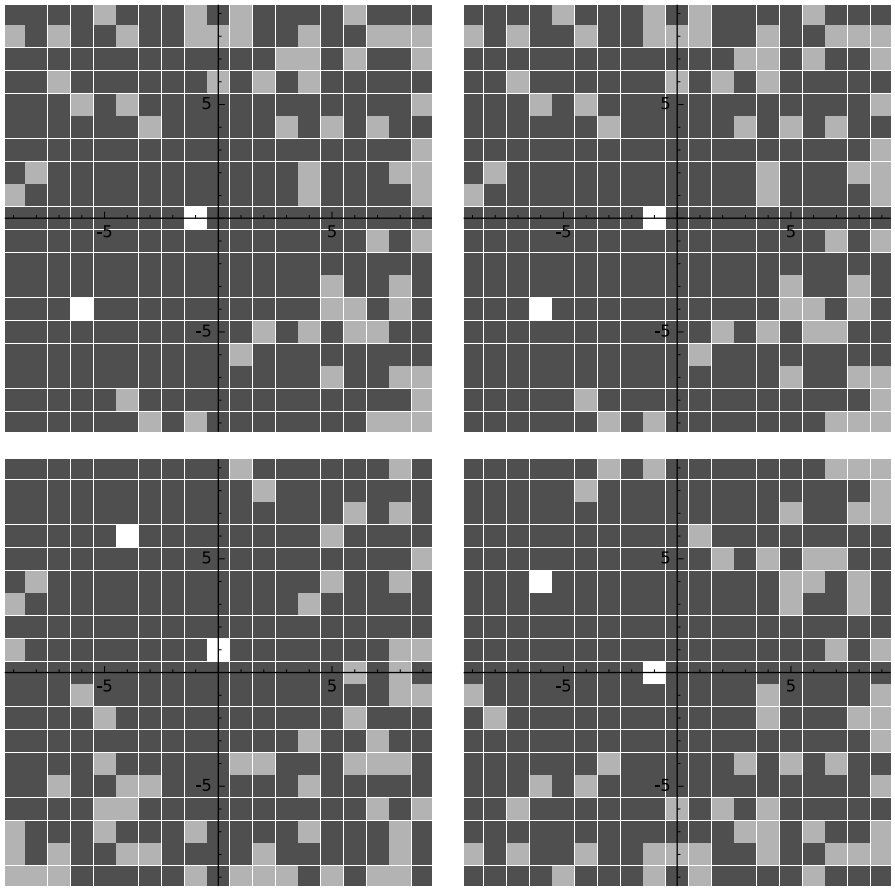

Figure 2: Primality plots for four related polynomials. Gaussian integers that produce prime outputs are dark gray, composite outputs are light gray, and units are shown in white. Clockwise from upper left: $f(z) = z^2 + (7 + 4i)z + (5 + 4i)$, $if(z)$, $f(iz)$, and $\overline{f}(z)$.

We now use these ideas to design an efficient search algorithm. First, it is easy to see that since post-multiplication by a unit will only rotate the domain,

we need only consider Gaussian quadratic polynomials $f(z) = \alpha z^2 + \beta z + \gamma$ for which α is in the first quadrant. Moreover, if $\alpha = a + bi$ is in the first quadrant, then $i\overline{\alpha}$ is in the first octant (so that $a \geq b$). From this point onward we restrict ourselves to polynomials where the first coefficient is in the first octant.

Second, note that all moves will preserve the worthiness of a polynomial; only translation is nontrivial to show. Given $f(z) = \alpha z^2 + \beta z + \gamma$ and $f(z-t) = \alpha z^2 + (-2t\alpha + \beta)z + (\alpha t^2 - \beta t + \gamma)$, we note first that $(\alpha + \beta) - (\alpha - 2t\alpha + \beta) = 2t\alpha$ is always even, so that $\alpha + \beta$ is even if and only if $\alpha + (-2t\alpha + \beta)$ is even. A similar argument will show that $\alpha t^2 - \beta t + \gamma$ is odd if and only if γ is odd, so the parity condition will be satisfied simultaneously for these two polynomials. Next, we use the discriminant formula $D_f = \alpha^2(r_1 - r_2)^2$, where r_1 and r_2 are the complex roots of $f(z)$. The translation $f(z-t)$ will have roots at $r_1 + t$ and $r_2 + t$, so that its discriminant is given by $\alpha^2((r_1 + t) - (r_2 + t))^2 = \alpha^2(r_1 - r_2)^2 = D_f$. Since the two polynomials have the same discriminant, they will both satisfy the discriminant condition simultaneously.

Last, we reduce the size of the search space by placing a restriction on the second coefficient. Given a polynomial $f(z) = \alpha z^2 + \beta z + \gamma$, Theorem 1 guarantees that there exist unique κ and ρ such that $\beta = \kappa \cdot 2\alpha + \rho$ and ρ is a standard residue modulo 2α. So, translate $f(z)$ by κ to obtain $f(z - \kappa) = \alpha z^2 + (\beta - 2\kappa\alpha)z + (\alpha\kappa^2 - \beta\kappa + \gamma)$. It is easy to see that the second coefficient is equal to ρ, the residue obtained from dividing β by 2α.

As an example of this reduction, consider the polynomial $f(z) = (1-2i)z^2 + (8+5i)z + (3-2i)$. Multiply by i to get the polynomial $if(z) = (2+i)z^2 + (-5+8i)z + (2+3i)$, so the first coefficient now lies in the first octant. Next, divide $-5+8i$ by $2(2+i)$ to get a quotient of $-1+2i$ with standard remainder $3+2i$, thus resulting in $g(z) = if(z - (-1+2i)) = (2+i)z^2 + (3+2i)z + (11+10i)$. So, we need only search for worthy quadratic polynomials $f(z) = \alpha z^2 + \beta z + \gamma$ with α in the first octant and β in the residue set for 2α. Since there are $N(2\alpha)$ such residues, our search space will be considerably reduced. This leads to our first polynomial search algorithm.

Algorithm 1 *Given α in the first octant with $Re(\alpha) \leq k$, and an odd Gaussian integer γ chosen so that $|Re(\gamma)|, |Im(\gamma)| \leq k$, search for prime-generating polynomials as follows.*

1. *Compute the set of standard residues modulo 2α.*
2. *For each β in this residue set, check whether or not the polynomial $\alpha z^2 + \beta z + \gamma$ is n-worthy (for some predetermined n).*
3. *If so, compute its efficiency over the test space $\mathcal{T}$.*
4. *Return the list of polynomials with efficiency $\geq 70\%$.*

The value of k restricts the size of α and γ, and will depend on the processing power or patience available to the user.

We implemented this algorithm in Sage [3], using $n = 11$ and $k = 10$. Here are the results. (Primality plots for the top three polynomials are shown in Figure 3.)

Coefficients	**Efficiency**
$[1, 6+5i, 6+5i]$	84.5%
$[1, 7, 9+10i]$	84.5%
$[1, 7+4i, 5+4i]$	83.1%
$[2, 1+3i, 9+4i]$	78.7%
$[1+i, 1+i, 8-5i]$	78.7%
$[2, 3+i, -9+4i]$	75.9%
$[3+i, 2+4i, -4-5i]$	75.1%
$[3+i, 2+4i, 3+8i]$	74.8%
$[2+2i, 2+4i, -5-6i]$	70.6%
$[2+2i, 2i, 5+8i]$	70.4%

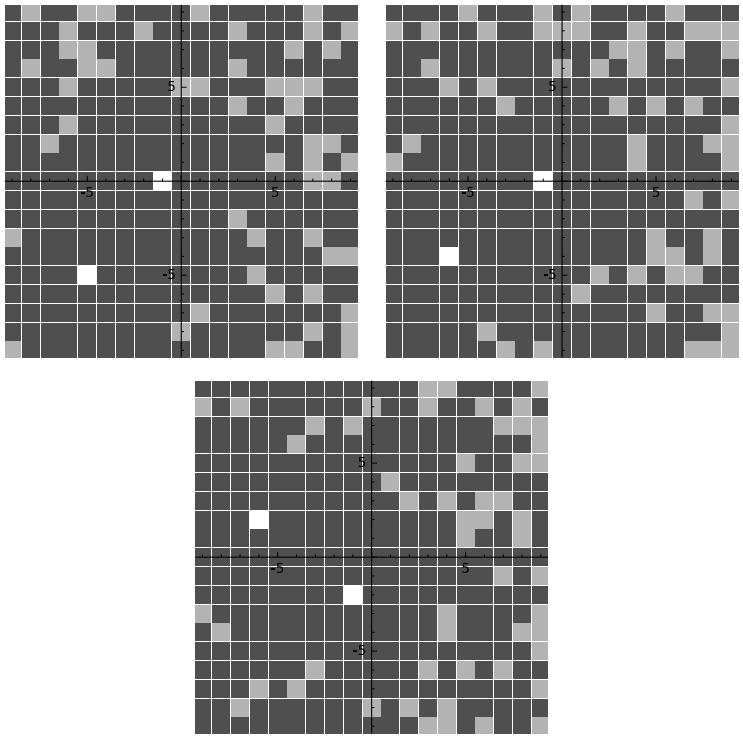

Figure 3: Primality plots for $z^2+(6+5i)z+(6+5i)$, $z^2+(7+4i)z+(5+4i)$, and $z^2+7z+(9+10i)$, respectively. Gaussian integers that produce prime outputs are dark gray, composite outputs are light gray, and units are shown in white.

Clearly, it is not so difficult for a Gaussian polynomial to generate primes. However, the search space is still quite large, and the results above took a long time to find. A less time-consuming search can be implemented by restricting to a special form of polynomial. In this case, we took the "Eulerian form" $f(z) = z^2 + z + \pi$, where π is a Gaussian prime. This way, one can search over a single set of Gaussian primes, rather than combinations of three coefficients.

Algorithm 2 *Choose a Gaussian prime π with $|Re(\pi)|, |Im(\pi)| \leq k$. Then search for Eulerian prime-generating polynomials as follows.*

1. *Check whether or not the polynomial $z^2 + z + \pi$ is n-worthy (for some predetermined n).*
2. *If so, compute its efficiency over the test space $\mathcal{T}$.*
3. *Return the list of polynomials with efficiency $\geq 66\%$.*

The value of k restricts the size of π, and again depends on the processing power or patience available to the user.

Since there are fewer parameters required in this search, the value of k can be quite large. We searched for Eulerian polynomials with $n = 11$ and $k = 150$; here are the results.

π	**Efficiency**
$-3 + 10i$	86.1%
$-94 + 25i$	71.5%
$-46 + 29i$	69.8%
$-29 + 90i$	69.8%
$2 + 115i$	68.1%
$-106 + 139i$	68.1%

Clearly, the most efficient prime-generating polynomial computed so far is $f(z) = z^2 + z + (-3 + 10i)$, which nearly matches the efficiency of Euler's own integer polynomial, $x^2 - x + 41$, on the interval $[0, 99]$. Its primality plot is shown in Figure 4.

4 The Prime Production Radius

We conclude with a result that applies to quadratic Gaussian polynomials in general, without the need for computer searches. While studying prime-generating polynomials over the integers, Mollin [4] defined the *prime-production length* of a polynomial. As an example, the polynomial $f(x) = x^2 - x + 41$ has a prime-production length of 41 since $f(x)$ is prime for the first 41 values in $x = 0, 1, 2, \ldots$. In the Gaussian case, this idea may be generalized by looking at a disk centered at 0. Specifically, we define the *prime-production radius* of a Gaussian polynomial $f(z)$ to be the largest norm, r, for which

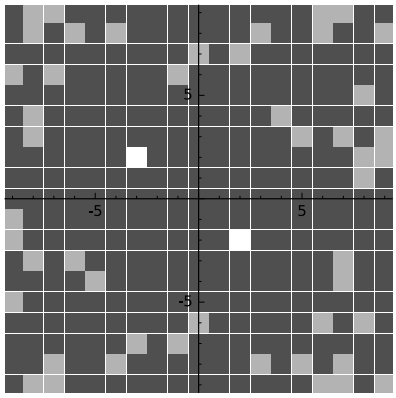

Figure 4: Primality plot for $z^2+z+(-3+10i)$. Gaussian integers that produce prime outputs are dark gray, composite outputs are light gray, and units are shown in white.

all values of z with $N(z) < r$ produce prime outputs $f(z)$. For example, the polynomial $f(z) = z^2 + z + (-3 + 10i)$ described in the previous section (again, see Figure 4) has a prime production radius of 32 since $z = 4 + 4i$ is the Gaussian integer closest to zero for which $f(z)$ is composite, specifically, $f(4 + 4i) = 1 + 46i = (2 + 5i)(8 + 3i)$.

Mollin restricted his initial attention to polynomials of the Eulerian form; we make the same restriction here. Recall from the comments following Theorem 1 that the standard residues modulo a Gaussian integer μ lie in a square with μ and $i\mu$ on opposite corners. However, we may translate this square so that it is centered on the origin; under this modification, the residue set is contained in the square $\mathcal{R}_\mu$ with midpoints at $\frac{1}{2}\mu$ and $\frac{1}{2}i\mu$.

We now proceed to the main result of this section.

Theorem 2 *Let $f(z) = z^2 + z + \pi$ with π prime, and let μ be a minimal prime (by norm) for which D_f is a square modulo μ. Then, the prime-production radius r is bounded above by $\frac{5}{4}N(\mu)$.*

PROOF: We begin by examining the possible residue sets modulo μ. Since $\mathcal{R}_\mu$ contains a full set of residues modulo μ, all other sets of congruent residues may be constructed by tiling the plane with this square, a partial representation of which appears in Figure 5.

Since D_f is a square modulo μ, we know that $f(z)$ factors modulo μ. So, there are exactly two residues in $\mathcal{R}_\mu$ that solve the equation $f(z) \equiv 0 \pmod{\mu}$. Since there are four prime multiples of μ (i.e., $\pm\mu$ and $\pm i\mu$), a disk centered at 0 need not contain a composite multiple of μ until it covers three residue squares.

At first glance, the circle in Figure 5 contains only one complete residue square. However, the circle also contains over half of the residue squares centered

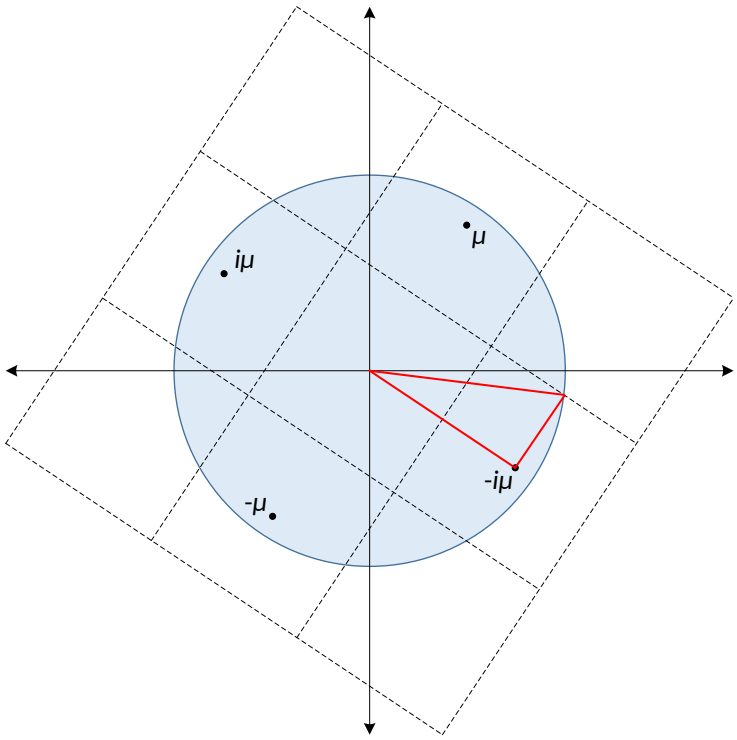

Figure 5: Nine central residue squares for divisor μ. The disk contains three complete residue squares modulo μ.

on μ and $-\mu$, in such a way that translating one to square to the other will give a complete residue square contained in the circle. In other words, if a solution to $f(z) \equiv 0 \pmod{\mu}$ lies in one of these squares, but is *outside* the circle, the corresponding solution in the other square will lie *inside* the circle. This works similarly for the residue squares centered on $i\mu$ and $-\mu$, so the circle in Figure 5 does indeed contain three complete residue squares.

The radius of the circle can be computed easily from the Pythagorean theorem (using the triangle in the figure). Specifically, $(|\mu|)^2 + \left(\frac{1}{2}|\mu|\right)^2 = \frac{5}{4}|\mu|^2 = \frac{5}{4}N(\mu)$. Since the circle of radius $\frac{5}{4}N(\mu)$ contains at least one composite multiple of μ, we must have $r < \frac{5}{4}N(\mu)$. QED

We note that, in general, this is not a sharp upper bound on the prime-production radius. For example, the polynomial $f(z) = z^2 + z + (-3 + 10i)$ has a prime-production radius of $r = 32$, while the theorem only specifies that $r < 136.25$. In the integer case, Mollin found sharper bounds to be a difficult problem, and we see no reason to doubt that the same is true for Gaussian polynomials.

5 Conclusion

Clearly, this is a subject ripe for further research. As can be seen from Figure 3, there appears to be a "pool" of prime outputs centered on those Gaussian integers that produce units as output values. Since unit outputs always occur near the roots of a polynomial, it is likely more accurate to say that this pool of prime outputs will occur near the midpoint of the roots. So, it's natural to expect that polynomials with roots centered at zero will have a high efficiency. (Incidentally, these are precisely those polynomials with β near zero, which describes all those found by Algorithm 2.) It would be valuable to find computational estimates for the size of this pool and then identify a sharper upper bound on the prime production radius, at least in some special cases. Additionally, it would be interesting to extend these results to include non-quadratic Gaussian polynomials.

6 Acknowledgments

We are very grateful to Drs. Steven Klee and Allison Henrich for their assistance in this endeavor. This research was performed as part of the 2015 SUMmER REU at Seattle University, which was supported from NSF grant DMS-1460537.

References

[1] Boston, N. and Greenwood, M. L., *Quadratics representing primes,* American Mathematical Monthly, Vol. 102, No. 7, pp. 595-599, 1995.

[2] Euler, Leonhard, *Extrait d'une lettre de M. Euler le père à M. Bernoulli concernant le memoire imprime parmi ceux de 1771,* Nouveaux Mémoires de l'Académie des Sciences de Berlin, p. 381, 1772.

[3] Stein, W. A., *Sage mathematics software (version 6.8)* Available online at `https://cloud.sagemath.com/`.

[4] Mollin, R. A., *Prime-producing quadratics,* American Mathematical Monthly, Vol. 104, No. 6, pp. 529-544, 1997.

[5] Rosen, K., "Elementary Number Theory and Its Applications", 6th ed., Addison-Wesley, 2011.