Gauss and Primes

Tom White

December 30, 2001

1 Introduction

1.1 Summary

Gauss' empirical discovery of PNT.

Motivations for Gaussian primes - unique factorization. Applications.

End by asking: how are Gaussian primes distributed?

1.2 The Conjecture

In 1792, when he was only 15 years old[1], Carl Friedrich Gauss noticed a striking connection between the distribution of the prime numbers and the logarithmic function. Gauss had a table of prime numbers that had been compiled by Johann Lambert[2], and he was examining the number of prime numbers less than or equal to a given integer x. It is now customary to denote this function as $\pi(x)$. Based purely on numerical evidence Gauss wrote

> Primzahlen unter a $(= \infty)$ $a/\mathrm{l}a$.[3]

In today's notation we would write $\pi(x) \sim x/\log x$, that is, as x tends to infinity the ratio between $\pi(x)$ and $x/\log x$ tends to 1. Gauss never proved his conjecture, indeed it remained unproven for just over one hundred years until Hadamard and de la Vallée-Poussin independently proved in 1896 what became known as the Prime Number Theorem.

1.3 Gaussian Primes

[Gauss and Number Theory - King and Queen?]

While investigating the properties of biquadratic reciprocity (which we shan't go into) Gauss introduced a generalisation of the integers, now known as *Gaussian integers.*[4] These are the complex numbers $a + bi$, where a and b are both ordinary (rational) integers. It turns out that these numbers behave in a manner which is analogous to rational integers. For example, it is easy to check that the sums and products of Gaussian integers are themselves Gaussian integers:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

[1] check, see Dunham pp78-79, Maor 184-185

[2] ref?

[3] find a more original source than Maor

[4] [2] p188 note 12.1

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$$

Gauss proved that all Gaussian integers can be uniquely factored into prime Gaussian integers. This is of course true of rational integers and Gauss was actually the first to explicitly state the theorem for rational integers[5], athough the result was used by earlier mathematicians. But however familiar the property of unique factorisation there are number systems that do not have this property. For instance, for the numbers $a+b\sqrt{-5}$, where a and b are both rational integers

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

and it can be shown that 2, 3, $1+\sqrt{-5}$, and $1-\sqrt{-5}$ are all prime.[6]

Having defined the Gaussian integers it is natural to ask: which Gaussian integers are prime? How do the Gaussian primes relate to the rational primes? And in light of Gauss' discovery of the distribution of the rational primes, how are the Gaussian primes distributed?

2 What are Gaussian Primes?

2.1 Summary

Characterisation of Gaussian primes. Relation to rational primes. Examples for small primes.

2.2 Characterisation

We first look at some definitions and simple results concerning Gaussian primes. This treatment follows that in Hardy and Wright [2].

A *Gaussian integer* is a complex number $a+bi$, where a and b are both (rational) integers. A *unity* is a power of i, and we say a Gaussian integer g is *associated* with ϵg where ϵ is any unity. In other words the *associates* of g are g, ig, $-g$, $-ig$.

The *norm* of a Gaussian integer $a+bi$ is defined to be $N(a+bi) = a^2+b^2$. The norm of a unity is always 1.

A *Gaussian prime* is a Gaussian integer, not 0 or a unity, divisible only by numbers associated with itself or 1.

Let's now consider the rational primes - are they prime when considered as Gaussian integers? 2 is not prime since it equals $(1+i)(1-i)$ - these factors are not associated with itself or 1. 3 is still prime, this can be seen by trial division by all Gaussian integers with norm less than or equal to 3 that are not 0 or a unity, that is: $1+i$ (ignoring associates).

$$\frac{3}{1+i} = \frac{3(1-i)}{(1+i)(1-i)} = \frac{3(1-i)}{1^2+1^2} = \frac{3}{2} - \frac{i}{2}$$

and since $\frac{3}{2} - \frac{i}{2}$ is not a Gaussian integer 3 is a Gaussian prime. Continuing in this way we can create a little table indicating when a rational prime p is divisible by a Gaussian prime $a+bi$:

[5] DA, see ref in [2] p10, note 1.3

[6] do it!

p	a	b
2	1	1
3		
5	2	1
7		
11		
13	3	2
17	4	1
19		
23		
29	5	2
31		
37	6	1
41	5	4
43		
47		

It seems that only rational primes of the form $4n+3$ are also Gaussian primes. We can see this by supposing that $\pi\lambda = p$ where π is a Gaussian prime. Then

$$N\pi N\lambda = p^2.$$

Therefore either $N\lambda = 1$, in which case λ is a unity and π is an associate of p, or

$$N\pi = a^2 + b^2 = p. \tag{1}$$

Now a square is equal to 0 or 1 (mod 4), so (1) cannot be satisfied. Therefore the alternative case must occur: π is an associate of p, so p is a Gaussian prime.

There is a nice proof that rational primes of the form $4n+1$ are *never* Gaussian primes. It starts from Wilson's test for primality: p is prime if and only if p divides $(p-1)!+1$. Now $p = 4n+1$, so it divides

$$
\begin{aligned}
(4n)!+1 &= (1\cdot 2\cdot \ldots \cdot 2n \cdot (2n+1)\cdot(2n+2)\cdot \ldots \cdot 4n)+1 && (2)\\
&\equiv (1\cdot 2\cdot \ldots \cdot 2n \cdot (-2n)\cdot(-(2n-1))\cdot \ldots \cdot (-1))+1 \pmod p && (3)\\
&= ((2n)!)^2+1 && (4)\\
&= ((2n)!+i)((2n)!-i) && (5)
\end{aligned}
$$

But p divides neither factor so p must have a Gaussian prime factor.

We can go further: if $a+bi$ is a (positive[7]) prime divisor of p then so is $a-bi$:

$$\frac{p}{a\pm bi} = \frac{p(a\mp bi)}{(a\pm bi)(a\mp bi)} = \frac{p(a\mp bi)}{a^2+b^2} = \frac{pa}{a^2+b^2} \mp \frac{pbi}{a^2+b^2}$$

Since $a \neq b$, $a+bi$ and $a-bi$ are not associates, they are distinct primes, so their product $(a+bi)(a-bi) = a^2+b^2$ divides p. But p is a rational prime, so p must equal a^2+b^2. This establishes...[8].

[7] define

[8] Fermat

2.3 Proofs

(Need Theorem 250 of [2]...)

Let $\pi = a + bi$ be a Gaussian prime. If

$$\pi \mid p, \pi\lambda = p,$$

then

$$N\pi N\lambda = p^2.$$

Therefore either $N\lambda = 1$, in which case λ is a unity (prove it!) and π is an associate of p, or

$$N\pi = a^2 + b^2 = p. \tag{6}$$

We now look at different types of prime p.

1. If $p = 2$, then
$$p = 1^2 + 1^2.$$
So $1 + i$ and its associates are Gaussian primes.

2. If $p = 4n + 3$, then (6) cannot be satisfied since a square is equal to 0 or 1 (mod 4). Hence ... (?)

3. If $p = 4n + 1$, then ...?

Gaussian primes may be fully characterised by the following:

1. $1 + i$ and its associates ($-1 + i$, $-1 - i$, $1 - i$)

2. the rational primes $4n + 3$ and their associates

3. the factors $a + bi$ of the rational primes $4n + 1$

This characterisation makes it easy to plot the distribution of Gaussian primes. It is sufficient to consider only $a + bi$ where a is positive, and b lies between 0 and a. In fact, $1 + i$ is the only such prime whose real part and imaginary part are equal. For the rest there are two cases:

1. If $b = 0$, $a + bi$ is prime if a is a prime of the form $4n + 3$.

2. If $b \neq 0$, $a + bi$ is prime if $a^2 + b^2$ is prime.

These cases are easily checked using a list of (rational) prime numbers. My program draws the distribution of Gaussian primes bounded by a prescribed circle in the complex plane. It uses a table of primes generated using the sieve of Eratosthenes.

3 The Prime Number Theorem

3.1 Summary

Table of x, $\pi(x)$, etc.

Discussion of empirical results Gauss etc.

Description of the proof of PNT - historical. Number of different types of proofs.

Q: is $\pi_{4,1} > \pi_{4,3}$ always - current status. (Mention change of sign of $Li(x) - \pi(x)$)

Density result for Gaussian primes - deviration. Nice esult linking primes, e and π.

Visualisation discussion - Christmas tree, Op Art, scaling r to even out the distribution - the city skyline plot.

3.2 Empirical observations

x	$\pi(x)$	$\lfloor x/logx \rfloor$	$\pi_{4,1}(x)$	$\pi_{4,3}(x)$	$\lfloor x/2logx \rfloor$
10^1	4	4	1	2	2
10^2	25	21	?	?	
10^3	168				
10^4	$1,229$				
10^5	$9,592$				
10^6	$78,498$				
10^7	$664,579$				
10^8	$5,761,455$				
10^9	$50,847,534$				
10^{10}	$455,052,511$	$434,294,481$			

References

[1] Conway, John H. and Guy, Richard K., (1996), *The Book of Numbers*, Springer Verlag.

[2] Hardy, G. H. and Wright, E. M. (1938), *The Theory of Numbers*, Oxford University Press, pp177-186, pp218-219.

[3] Ribenboim, Paulo, (1989), *The Book of Prime Number Records*, Springer Verlag.

[4] Rose, H.E., (1988), *A Course in Number Theory*, Oxford University Press, p92.