SQUARE DANCING WITH PRIMES
Blog #4

Here is another refinement of square dancing that waltzes right into some pretty deep mathematics (see also SQUARE DANCING ON SQUARE TILES).

Carl Friedrich Gauss (1777-1855), arguably the greatest mathematician of all times, was intrigued by the identity $a^2 + b^2 = (a + ib)(a - ib) = c^2$, for integral values of a, b, implying that there is a one-to-one correspondence between Pythagorean triples (a, b, c) and complex numbers whose real and imaginary parts a, b as well as absolute value c are integers. Then Gauss went on looking at non-Pythagorean triples of the type $(1, 2, \sqrt{5})$ where the last component is the square root of a prime number (that is, the square of the hypotenuse of the right triangle is a prime number). Gauss took a hard look at the list of prime numbers

2, 3, **5**, 7, 11, **13**, **17**, 23, **29**, 31, **37**, **41**, 43, 47, **53**, 59, **61**,…

and noticed that the odd primes fall into two classes according as they yield a remainder of 1 or 3 upon division by 4. In the list above this is indicated by printing them in red or black color, resp. Thus $3 = 4 \times 0 + 3$, $7 = 4 \times 1 + 3$, $11 = 4 \times 2 + 3$, $23 = 4 \times 5 + 3$,… and $\mathbf{5} = 4 \times 1 + 1$, $\mathbf{13} = 4 \times 3 + 1$, $\mathbf{17} = 4 \times 4 + 1$, $\mathbf{29} = 4 \times 5 + 1$,… Both classes have infinitely many primes (this is not obvious!) But the remarkable thing is that the black primes never split into the product of complex conjugate numbers. Conversely, all the red primes do, thus: $\mathbf{5} = (1 + 2i)(1 - 2i)$, $\mathbf{13} = (2+3i)(2- 3i)$, $\mathbf{17} = (1 + 4i)(1 - 4i)$, $\mathbf{29} = (2 + 5i)(2 - 5i)$, $\mathbf{37} = (1 + 6i)(1 - 6i)$, etc.

The only even prime number **2** forms a class by itself; it also splits into the product of complex conjugate numbers: $\mathbf{2} = (1 + i)(1 - i)$.

In honor of Gauss we call a complex number $a + ib$ a Gauss integer, if a, b are integers (the absolute value $\sqrt{a^2 + b^2}$ may or may not be). The arithmetic of Gauss integers is rather similar to that of rational integers, if we consider the latter as special Gauss integers. We can talk about their divisibility, and we can talk about Gauss primes. We even have the Fundamental Theorem of Arithmetic asserting that every non-zero Gauss integer can be uniquely decomposed into the product of Gauss primes (provided that another decomposition which differs only in the order of factors, or in which Gauss primes may have been replaced by their mutual divisor, is considered the same). Examples of Gauss primes are: $1+2i$, $2+3i$, $1+4i$, $2+5i$, $1+6i$, $4+5i$; and also $1–2i$, $2–3i$, $1–4i$, $2–5i$, $1+6i$, $4–5i$. The interesting thing is that the squares of the absolute value of these complex numbers are just the red primes: **5**, **13**, **17**, **29**, **37**, **41**. We can see that the red primes are not Gauss primes; in contrast with the black primes, which are. Of course, **2** is not a Gauss prime either, but its factors $1 + i$ and $1 - i$ are.

Let us call a right triangle whose legs are integers and the square of the hypotenuse is a prime number, an instance of „square dancing with primes”. It follows from the foregoing that all such can be obtained from the factorization of the colored primes into Gauss primes.

This suggests that a survey of all possible instances of square dancing with primes is exactly the same as the survey of all Gauss primes with non-zero real and imaginary parts.

When it comes to prime factorization in **Z,** we do not make a distinction between the prime numbers 2 and – 2, 3 and – 3, etc. We treat them as if they were one and the same. In more details, we introduce an equivalence relation by calling two different integers equivalent if they are mutual divisors. This is the case if, and only if, either one is the negative of the other. Then we take the quotient set. Elements of the quotient set are equivalence classes or, as we shall call them, molecules consisting of an integer and its negative, called atoms. Thus all molecules have two atoms, with the exception of the zero molecule which has only one.

The Fundamental Theorem of Arithmetic refers to the quotient set consisting of molecules of integers. (Quotient sets of numbers were introduced in my blog MAIMING THE MIND.) The Fundamental Theorem may be stated as saying that, apart from order, a non-zero molecule of integers can be uniquely decomposed into the product of prime molecules.

Now we want to make the same distinction for the Gauss integer. We call two Gauss integers equivalent if they are mutual divisors. An example is $3 + 4i$ and $4 – 3i$. The first is a divisor of the second because $4 – 3i = (– i)(3 + 4i)$, and the second is a divisor of the first because $3 + 4i = i(4 – 3i)$. But $3 + 4i$ has two other mutual divisors as well: $– 3 – 4i$ and $– 4 + 3i$. As there are no others, the four Gauss integers $(3+4i, –3–4i, 4–3i, –4+3i)$ form a molecule. In the complex number plane the four atoms of a molecule are simmetrically located, in fact, they are the four vertices of a square the center of which is 0.

The simplest molecule of four atoms is the unit molecule $(1, –1, i, –i)$. The atoms of the unit molecule, $1, –1, i, –i$, are called units. The product of any two units, and the reciprocal of any unit is also a unit. The rule to get the various atoms of any given molecule is to multiply one of the atoms by the units. The 0-molecule, of course, has only one atom. The Fundamental Theorem of Arithmetic refers to the quotient set consisting of the molecules of Gauss integers. It can be stated as saying that, apart from order, every non-zero molecule of Gauss integers uniquely splits into the product of prime molecules.

Another molecule that occurs frequently is $(1+i, 1–i, –1+i, –1–i)$, the atoms of which are the Gauss prime divisors of 2. This is the only case where the complex conjugate of a Gauss prime belongs to the same molecule. In all other cases the complex conjugate of a Gauss prime with nonzero real and imaginary parts is a different Gauss prime.

There is a relation between Pythagorean triples and Gauss integers. Given a primitive Pythagorean triple (a, b, c), we can write the square of the hypotenuse as a product of complex conjugate Gauss integers: $c^2 = a^2 + b^2 = (a + ib)(a – ib)$. There is a theorem asserting that either factor is the square of a Gauss integer.

For example, for $(3+4i)(3–4i) = 3^2 + 4^2 = 5^2$ we have $3+4i = (2+i)^2$ and $3–4i = (2–i)^2$; for $(5 + 12i)(5 – 12i) = 5^2 + 12^2 = 13^2$ we have $5 + 12i = (3 + 2i)^2$ and $5 – 12i = (3 – 2i)^2$. This can be proved using the unique prime factorization of Gauss integers, see: http://wikipedia.org/wiki/Pythagorean_triple

To recapitulate, square dancing in general involves an arbitrary right triangle. Square dancing on square tiles involves right triangles with integral legs whose hypotenuse is an integer as well. Square dancing with primes also involves right triangles with integral legs, but the hypotenuse here is not an integer but the square root of a colored prime number.

There are some remarkable open problems in connection with Gauss primes. The real and imaginary axes contain infinitely many Gauss primes, namely, 3, 7, 11, 23, 31, 43,… and $3i, 7i, 11i, 23i, 31i, 43i$,… Are there any other straight lines in the complex number plane which also do?

In particular, it is not known whether there are infinitely many Gauss primes on the line parallel to the imaginary axis a unit distance from it to the right.

In passing I mention a fascinating analogy between the extension of integers to Gauss integers, and the extension of the set $\mathbf{R}(x)$ of polynomials with real coefficients to the set $\mathbf{C}(x)$ of polynomials with complex numbers as coefficients. The latter resemble the number system of integers: we have divisibility; we have units, we have primes. The units of $\mathbf{R}(x)$ is the set of non-zero real numbers $\mathbf{R}^*$, those of $\mathbf{C}(x)$ is the set of non-zero complex numbers $\mathbf{C}^*$ called scalars. Thus a molecule of polynomials, other than the zero polynomial, has infinitely many atoms, namely, polynomials which are non-zero scalar multiples of one another. Corresponding to primes we have the irreducible polynomials. The Fundamental Theorem asserts that any non-zero molecule of polynomials can be uniquely decomposed as a product of molecules of irreducible polynomials (apart from order).

Just like in **Z** where there are black primes and red primes, in **R(*x*)** there are also two kinds of irreducible polynomials: linear and irreducible quadratic polynomials (those with a negative discriminant). When we pass to **C(*x*)**, irreducible quadratic polynomials split into the product of linear polynomials with complex coefficients, just like the red primes split into the product of Gauss integers.

EXERCISES.

(1) Write the following primes as the product of a pair of complex conjugate Gauss primes: **41**, **53**, **61**, **73**, **89**, **97**, **101**.

(2) True or false? (*a*) $9-3i$ is divisible by $1+i$; (*b*) $24+21i$ is divisible by $1+3i$; (*c*) $10-47i$ is divisible by $2+3i$.

(3) Find pairs of mutual divisors among the Gauss integers $4-3i$, $4+3i$, $3+4i$.

(4) Show that if $a + ib$ is a Gauss prime, then its complex conjugate $a - ib$ is a Gauss prime as well. Are they mutual divisors?

(5) Show that if $a + ib$ is a Gauss prime, then so is $b + ia$.

(6) Find all the divisors of the Gauss integers (*a*) $1 - 3i$; (*b*) $1 + 4i$

(7) How many divisors does a Gauss prime have?

ANSWERS.

(1) **41** = $(4+5i)(4-5i)$; **53** = $(2+7i)(2-7i)$; **61** = $(5+6i)(5-6i)$; **73** = $(3+8i)(3-8i)$;

89 = $(5+8i)(5-8i)$; **97** = $(4+9i)(4-9i)$; **101** = $(1+10i)(1-10i)$.

(2) (*a*) True. (*b*) False. (*c*) True.

(3) $4 - 3i$ and $3+ 4i$ are mutual divisors; $4 + 3i$ is not a mutual divisor of either one of the preceding ones.

(4) If $a + ib$ is a Gauss prime, then the square of its absolute value, $a^2 + b^2$ is a red prime. But the complex conjugate has the same absolute value, therefore it cannot help but be a Gauss prime itself. The complex conjugate of a Gauss prime is not a mutual divisor, hence they belong to different molecules. There is only one exception to that, namely $1+i$, $1-i$, the Gauss prime divisor of 2 which belong to the same molecule.

(5) This follows from (4) and from the fact that the product of a Gauss prime by a unit (in this case, by i) is also a Gauss prime (they belong to the same molecule).

(6) (*a*) 16; (*b*) 8.

(7) There are two kinds of Gauss primes: the black primes p, and the Gauss prime divisors $a + ib$ of the colored primes. In the first case the number of divisors is 4 (namely, p, $-p$, 1, –1); in the second case, 8 (namely, $a + ib$, $-a - ib$, $-b + ia$, $b - ia$, 1, –1, i, $-i$).

(Revised March 22, 2010)