The Empyrean Realm

A paper presented by

Robert Word, VII°

to the

Masonic Societas Rosicruciana in Civitatibus Foederatus

Golden State College

The Mystery Tradition of the ancient Rosicrucians informs us of the various levels of existence, in a chain of being extending from the transient perceptions of sense experience, through finer gradations, and leading to the true ground of being, or the ultimate nature of things.

The astral is a realm of hallucination and delusion, and the lower magics lead to no true reality. But the neoplatonists showed that by pure thought alone one might ascend to the empyrean realm, wherein true knowledge of the reality prevails.

Thus, the philosopher Plotinus wrote:

"But how are we related to the Intellect? I mean by 'Intellect' not that state of the soul, which is one of the things which derive from Intellect, but Intellect itself. We possess this too, as something that transcends us. We have it either as common to all or particular to ourselves, or both common and particular; common because it is without parts and one and everywhere the same, and particular to ourselves because each has the whole of it in the primary part of his soul. So we also possess the forms in two ways, in our soul, in a manner of speaking unfolded and separated, in Intellect all together.

"But how do we possess God? He rides mounted on the nature of Intellect and true reality -- that is how we possess him ..."

The theories of the numerologists will not lead to the empyrean realm, nor even the gematria speculations of the latter day kabbalists, for these things are also full of vanity and self-deception.

Pure mathematics alone is shorn of the vanity and foolishness of the human kingdom. Euclid alone has looked on beauty bare. The Square and Compass of the Brotherhood are emblematic of Geometry.

Above the portal to the philosophic academy of Plato was written the admonition: "Let no man ignorant of mathematics enter herein."

Let us therefore look at a bit of number magic. Consider the real odd prime numbers (so we shall leave alone the exception of 2 here). An odd prime number can be written either in the form p=4n+1 or p=4n+3.

In the case that p=4n+1, then p can be written in one and only one way as the sum of two squares. This leads to the famous Pythagorean triplets $c^2=a^2+b^2$. For example, if p=5, then $5 = 2^2 + 1^2$, so 5 = (2+i)*(2-i); squaring this latter, we obtain $5^2 = 3^2 + 4^2$. That is, squaring the equation results in two factors of (2+i): $(2+i)*(2+i) = (2^2 - 1^2) + 2*2*i = 3 + 4i$, and in two factors of 2-i:
$(2-i)*(2-i) = (2^2 - 1^2) - 2*2*i = 3 - 4i$; therefore, $5^2 = (3+4i)(3-4i) = 3^2 + 4^2$.

Now we shall interject some ancient speculation at this point. The 3-4-5 triangle was a basis of ancient Egyptian science and engineering, as well as sacred theology. For it exemplified according to the ancient theologians the sacred trinity of Father-Mother-Son; of Osiris-Isis-Horus. The descending arm of three units was Osiris; the basal arm of 4 units was Isis, and the hypotenuse of 5 units was Horus.

Likewise, $13 = 3^2 + 2^2$, and squaring once again, we obtain the Pythagorean triplet $13^2 = 12^2 + 5^2$. (Here again, we group the two factors of 3+2i):
$(3+2i)(3+2i) = (3^2 - 2^2) + 2*3*2i = 5 + 12i$,
and $(3-2i)(3-2i) = (3^2 - 2^2) - 2*3*2i = 5 - 12i$. Thus, $13^2 = (5-12i)(5+12i) = 12^2 + 5^2$

Now showing that a real prime number of the form $p = 4n + 1$ can be expressed as the sum of two squares in one and only one way will take some doing, and hence, I shall exhibit the broad outlines of a proof only, so that this fact itself will then be crystal clear.

The reader who is unfamiliar with elementary number theoretic concepts will find some of the basic definitions in the Appendix to this paper.

The proof hinges on three primary facets:

1) The fundamental theorem of arithmetic is true in the complex integral domain as well as the real integral domain. (Any integer may be reduced to the product of unique prime factors.) For example, the number 5 is prime in the real integral domain, but in the complex domain, it may be factored uniquely into prime complex integer factors: $5 = (2+i)(2-i)$. Thus 2+i is prime in the domain of complex integers, since it cannot be factored further; also, there is no other factorization of 5 in the domain of complex integers. Therefore we see that although 5 is prime in the real integral domain, yet it is not prime in the complex integral domain.

2) The Fermat Theorem in the real domain. Let p be a prime number, and let a be any real integer not congruent to 0 in the modulus p. Then $a^{(p-1)}$ is congruent to 1 in the modulus of p. (See the appendix for definitions of congruence and modulus). For example, in the modulus of the real prime 5, $2^4 = 16 = 1 \pmod 5$; $3^4 = 81 = 1 \pmod 5$; $4^4 = 256 = 1 \pmod 5$, etc.

3) The theory of equations in a field for which every element has a multiplicative inverse except zero. Then a polynomial of degree n has at most n roots, and unity has at most n roots of order n. Thus, for example, in a prime modulus, -1 can have at most two square roots.

Additionally, note that in a prime modulus p, every element not equal to zero in the modulus p has a multiplicative inverse. Therefore, facet 3) must apply in this case. As we have seen, it is possible that p may be prime in the real integral domain, but not in the complex integral domain. In this eventuality, there may be non-zero elements which have no multiplicative inverse in the modulus of p in the complex domain, even though every non-zero element must have a multiplicative inverse in the modulus of p in the real domain.

Consider, for example, the case of 5. Then 2*3 = 6 = 1(mod 5), and 4*4 = 16 = 1 (mod 5). (That is 1, 2, 3, and 4 have multiplicative inverses in the modulus of 5). But in the complex integral domain, 5 is not a prime, (i.e., 5 = (2+i)(2-i)) and it is not true that for complex integers every non-zero element has a multiplicative inverse in the modulus of 5. For example, 2+i has no multiplicative inverse in the modulus of 5. In fact, we see that (2+i)(2-i) = 5 = 0 (mod 5), so clearly, (2+i) can have no multiplicative inverse in this modulus. Additionally, in the real integral domain modulus 5, -1 has precisely two square roots; i.e., $3^2 = 9 = -1$ (mod 5); and also $2^2 = 4 = -1$ (mod 5). This is the maximum allowed number of square roots, according to facet 3) above. However, in the complex integral domain, we also have $i^2 = -1$ (mod 5) and $(-i)^2 = -1$ (mod 5), so that -1 has *four* distinct square roots in the complex integral domain modulus 5: i.e., 3, 4, i, and -i. This circumstance does not contradict facet 3), since in the complex domain, there are non-zero elements that have no multiplicative inverse in the modulus of 5 (for example, 2+i).

First, we show that a real prime of the form p = 4n+1 cannot be expressed as the sum of two squares in more than one way. For suppose it could. Then there would be (p,a,b,c,d) for which $p=a^2+b^2$ and $p=c^2+d^2$ would both be true. But going to the complex integral domain, p = (a+bi)(a-bi) and p=(c+di)(c-di) are both true. The fundamental theorem of arithmetic in the complex domain requires that the factorization into prime factors must be unique; therefore, the two different factorizations would require that p = (a+bi)(a-bi) can be further factored into ultimate prime factors, so p must be expressed as the product of at least four complex factors. Then by grouping these factors in two (element and complex conjugate), one obtains a factorization of p in the real domain, contrary to the assumption that it is a real prime. Hence, a real prime of the form 4n+1 cannot be expressed in more than one way as the sum of two squares; this fact follows directly from the fundamental theorem of arithmetic in the complex domain.

Next, it remains to show that a real prime of the form p=4n+1 can be expressed as the sum of two squares in at least one way. This is equivelent to the statement that p may be factored in the complex domain. This is shown as follows.

In the real domain, by the Fermat theorem, $a^{(4n)} = 1$ in the modulus of p, for all a not zero in the modulus of p. Therefore $(a^{(2n)})^2 = 1$ (mod p). Thus, $a^{(2n)}$ is a square root of 1 for each non-zero a in the modulus p in the real domain. Now 1 has two square roots in the modulus of p: i.e., +1 and -1. (That is 1*1 = 1 (mod p), and (-1)*(-1) = 1 (mod p).) By facet 3) there can only be two distinct square roots of 1 in the modulus of p in the real domain; thus, $a^{(2n)}$ must be one or the other of these two values (i.e., 1 or -1) for each non-zero a in the modulus of p in the real domain. Hence, $a^{(2n)} = 1$ (mod p) or $a^{(2n)} = -1$ (mod p). But 1 has at most 2n roots of order 2n, and -1 has at most 2n roots of order 2n; however, the modulus p has p - 1 = 4n distinct non-zero elements (see appendix). If only the case $a^{(2n)} = 1 \pmod p$ occurs, then by facet 3), the modulus of p could only have 2n non zero elements. But it has 4n distinct non-zero elements. Thus, the case $a^{(2n)} = -1 \pmod p$ must also occur; in fact, 2n distinct cases of a for which $a^{(2n)} = -1 \pmod p$ must occur. Then for any one of these cases, $(a^n)^2 = -1 \pmod p$; also $((-a)^n))^2 = -1 \pmod p$. Therefore, the modular prime domain p contains at least two distinct real square roots of -1. By facet 3), it cannot contain more than two distinct real square roots of -1. Thus, a modular prime domain p where p=4n+1 must always contain exactly two real square roots of -1. But now let us go to the complex integral domain. Then i and -i are also square roots of -1. Therefore, in the complex domain, -1 has at least four distinct square roots in the modulus of p. But by the theory of equations, if p is prime in the complex domain, then every non-zero element has a multiplicative inverse, and therefore -1 could at most have two square roots. The existance of four distinct square roots, two real, and also i and -i, therefore means that p cannot be prime in the complex domain. Therefore, it can be factored in the complex domain, which means that p can be expressed as the sum of two squares in the real domain. Hence, it is seen that a real prime p of the form p = 4n + 1 can always be expressed as the sum of two squares in at least one way.

Thus, a real prime number of the form p = 4n + 1 can always be expressed as the sum of two squares in one and only one way, as was to be shown.

Where is the empyrean realm? It cannot be grasped in the transitory realm of sensory experience. But is there a portal of intellectual rigor, exemplified by pure mathematics? Perhaps therein one might catch a glimpse of the empyrean realm, wherein resides an eternal and unchanging verity.

APPENDIX

I. Real integers and complex integers.

Real integers comprise the infinite set of counting numbers and their negatives, including zero: { . . ., -3, -2, -1, 0, 1, 2, 3 . . .}

Complex integers consist of all numbers of the form a + bi, where a and b are any real integers.

Note that a real integer a is also a complex integer, since it may be written a = a + 0i .

II. Definition of modulus.

Let a and b be two real integers, and p a third integer. Then in the real domain, we say that

$a = b \pmod p$

iff

(a - b)/p is a real integer.

We also say that a is equal to b in the modulus of p.

For example, consider the case that p = 5. Then we see that 6 = 1 (mod 5) since (6-1)/5 = 1, which is an integer.

This relationship defines an equivalence class which we shall informally call "the modulus of p in the real integral domain." The modulus of p in the real domain has p distinct elements {0, 1, 2, ... p - 1}, where p - 1 = -1 (mod p).

Let a and be be two complex integers, and p a third complex integer. Then we say that

a = b (mod p)

iff

(a-b)/p is a complex integer.

We also say that a is equal to b in the modulus of p.

This relationship defines an equivalence class which we shall informally call "the modulus of p in the complex integral domain."

For example, suppose that p = 5. Then

$(3^2 - (-1))/5 = 10/5 = 2$, which is a complex integer, so $3^2 = -1$ (mod 5).

$(2^2 - (-1))/5 = 5/5 = 1$, which is a complex integer, so $2^2 = -1$ (mod 5).

$(i^2 - (-1))/5 = 0/5 = 0$, which is a complex integer, so $i^2 = -1$ (mod 5).

$((-i)^2 - (-1))/5 = 0/5 = 0$, which is a complex integer, so $(-i)^2 = -1$ (mod 5).

However, it is not the case that 3 = 2 (mod 5), since (3-2)/5 = 1/5, which is not a complex integer. Likewise, it is not the case the 3=i (mod 5), since (3-i)/5 = (3/5) - (1/5)i, which is not a complex integer.

III. Complex prime integers.

A complex prime integer is an integer p which has no factors except itself, 1, -1, i, -i, or -p, ip, or -ip. Thus, for example, the integer 2 + i is a complex prime integer. However, the number 5 is not a complex prime integer, since it can be factored:

5 = (2 + i)(2 - i).

In the real domain, 5 is prime, but in the complex domain, it is a composite number.

IV. Fundamental theorem of arithmetic in the complex domain.

Every integer p can be uniquely factored into complex primes (except for factors of 1, -1, i, or -i).

Thus, for example, we can write

$5 = (2 + i)(2-i)$, or equivalently, $5 = (1 -2i)(1+2i)$; (it is an equivalent factorisation, since $-i(2-i) = 1 - 2i$, etc.)

As noted before, the number 5 is a composite number in the complex domain, and its prime factors are (1-2i) and (1+2i).

V. Factorization in the complex domain

If a + bi is a prime factor of the real integer p in the complex domain, then a-bi is also a prime factor of the real integer p in the complex domain. This fact is seen by noting that the complex conjugate of p is itself; taking the complex conjugate of the factorization will yield the factor a - bi in the unique factorization of p. Therefore, the prime factor a - bi must also occur.

For example, in the factorization of 5, the prime factor 2 + i occurs. Therefore, the complex conjugate of 2 + i, i.e., 2 -i, must also occur. In fact, as previously noted,

$5 = (2 + i)(2-i)$.