4. SUMS OF SQUARES

§4.1. Gaussian Integers

The German mathematician Carl Friedrich Gauss [1777 – 1855] is considered to be one of the greatest mathematicians of all time and he contributed to many branches of mathematics.

A **Gaussian integer** is a complex number of the form $a + b$i where $a, b \in \mathbb{Z}$. The set of Gaussian integers is denoted by $\mathbb{Z}$[i]. This set is clearly closed under addition and multiplication.

The **norm** of a Gaussian integer $z = a + b$i is $||\mathbf{z}|| = a^2 + b^2$. It is the square of the modulus, but has the advantage over the modulus of being an integer. Clearly the norm of a product is the product of the norms.

Example 1: $||3 + 2i|| = 13$.

A **unit** in $\mathbb{Z}$[i] is a complex number that has an inverse under multiplication. If u is a unit then $||u||.||u^{-1}|| = ||1|| = 1$ and, being

positive integers, we must have $||u|| = ||u^{-1}|| = 1$. It follows that the units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

The norm plays a similar role to the absolute value for integers. In particular, we can divide one Gaussian integer by another to get a quotient and a remainder, where the remainder has smaller norm than the number we're dividing by.

Theorem 1 (REMAINDER THEOREM): If $a + bi$ and $c + di$ are Gaussian integers,
with $c + di \neq 0$, then $a + bi = (c + di)(p + qi) + (r + si)$ for some Gaussian integers $p + qi$ and
$r + si$ where $||r + si|| < ||c + di||$.

Proof: Let $\dfrac{a + bi}{c + di} = x + yi$ where $x, y \in \mathbb{Q}$.

Let p, q be the closest integers to x, y respectively. (If x or y is exactly half-way between two integers, either will do.)

Then $|x - \alpha| \leq ½$ and $|y - \beta| \leq ½$.

Therefore $= |(x + yi) - (p + qi)|$

$$= |(x - p) + (y - q)i|$$
$$= \sqrt{(x - p)^2 + (y - q)^2}$$
$$\leq \sqrt{¼ + ¼}$$
$$\leq \frac{1}{\sqrt{2}}$$

$< 1.$

Hence $|(a + b\mathrm{i}) - (c + d\mathrm{i})(p + q\mathrm{i})| < |c + d\mathrm{i}|$.

Because of this the theory of greatest common divisors and prime numbers, as well as results built upon these, can be extended from integers to Gaussian integers. In particular we have the following theorem. Full details are given in Chapter 2 of my Ring Theory notes.)

Theorem 2: Every non-zero Gaussian integer can be factorised uniquely into primes, up to rearrangement of factors and multiplication by units.

Example 2: $16 + 2\mathrm{i} = (2 - \mathrm{i})(3 + 2\mathrm{i})(1 + \mathrm{i})(1 - \mathrm{i})$ is a factorisation into primes.

So is $16 + 2\mathrm{i} = (-1 - \mathrm{i})(1 + 2\mathrm{i})\ (2 - 3\mathrm{i})(-1 + \mathrm{i})$.

Note that $2 - \mathrm{i} = (1 + 2\mathrm{i})(-\mathrm{i})$,

$3 + 2\mathrm{i} = (2 - 3\mathrm{i})\ \mathrm{i}$,

$1 + \mathrm{i} = (-1 - \mathrm{i})(-1)$,

$1 - \mathrm{i} = (-1 + \mathrm{i})(-1)$.

How do we know that these factors are all prime? The answer is “because their norms are all prime integers”.

Theorem 3: If $||a + b\mathrm{i}||$ is a prime integer then $a + b\mathrm{i}$ is a prime Gaussian integer.

Proof: Suppose that $\|a + b\mathrm{i}\|$ is prime and suppose that $a + b\mathrm{i} = (c + d\mathrm{i})(e + f\mathrm{i})$ where neither factor is a unit. Then $\|a + b\mathrm{i}\| = \|c + d\mathrm{i}\|.\|e + f\mathrm{i}\|$ is a proper factorisation, a contradiction.

Some prime integers are prime Gaussian integers, but others are not. For example, 2 is prime in $\mathbb{Z}$ but factorises as $(1 + \mathrm{i})(1 - \mathrm{i})$ in $\mathbb{Z}]\mathrm{i}]$. On the other hand 3 is both a prime integer and a prime Gaussian integer.

Why is 3 a prime Gaussian integer, even though its norm, 9 is not prime? The answer is because if $3 = uv$ where $u, v \in \mathbb{Z}[\mathrm{i}]$, neither being a unit, then $9 = \|u\|.\|v\|$ and so
$\|u\| = \|v\| = 3$. But 3 cannot be expressed as a sum of square integers and so cannot be the norm of any Gaussian integer.

Theorem 4: If $a + b\mathrm{i}$ is prime and $a, b \neq 0$ then $\|a + b\mathrm{i}\|$ is prime.
Proof: Suppose that $a + b\mathrm{i}$ is prime in $\mathbb{Z}[\mathrm{i}]$. Then $a - b\mathrm{i}$ is also prime because the factors of
$a - b\mathrm{i}$ are conjugates of factors of $a + b\mathrm{i}$.
The associates of $a + b\mathrm{i}$ are $\pm (a + b\mathrm{i})$ and $\pm (-b + a\mathrm{i})$.
Suppose that $a + b\mathrm{i}$ and $a - b\mathrm{i}$ are associates.
Then $a = \pm b$, in which case $a, b = \pm 1$ and $\|a + b\mathrm{i}\| = 2$, which is prime.
So suppose that $a + b\mathrm{i}$ and $a - b\mathrm{i}$ are not associates.

Being prime they must be coprime.

Suppose that $\|a + bi\| = mn$ where $m, n \in \mathbb{Z}[i]$.
Since $\|a + bi\| = (a + bi)(a - bi)$, we conclude that $a + bi$ divides mn in $\mathbb{Z}[i]$, and being prime, $a + bi$ divides m or n.
Suppose, without loss of generality, that $a + bi$ divides m.
Since m is real, $a - bi \mid m$.
Since $a + bi$ and $a - bi$ are coprime it follows that $\|a + bi\|$ divides m.
Hence $n = 1$, a contradiction.

Theorem 5: Let p be prime in $\mathbb{Z}$. Then p is prime in $\mathbb{Z}[i]$ if and only if $p \equiv 3 (\text{mod } 4)$.
Proof: Suppose p is prime in $\mathbb{Z}[i]$. Since $2 = (1 + i)(1 - i)$, $p > 2$.
Hence $p \equiv 1 (\text{mod } 4)$ or $p \equiv 3 (\text{mod } 4)$.

Case 1: Suppose that $p \equiv 1 (\text{mod } 4)$.
Then, by the theory of quadratic residues, $(-1 \mid p) = 0$, that is, $x^2 \equiv -1 (\text{mod } p)$ has a solution. Regarding x now as an integer, $x^2 + 1 = kp$ for some integer k.
Hence $p \mid (x + i)(x - i)$, and being prime in $\mathbb{Z}[i]$, $p \mid x + i$ or $p \mid x - i$.
If $p \mid x + i$ then $x + i = p(c + di)$ for some $c + di \in \mathbb{Z}[i]$, and so $pd = 1$, a contradiction.

Similarly we get a contradiction if $p \mid x - \mathrm{i}$.
Hence $p \equiv 3 (\mathrm{mod}\ 4)$.

Case 2: Suppose that $p \equiv 3 (\mathrm{mod}\ 4)$.
Suppose that p is composite in $\mathbb{Z}[\mathrm{i}]$.
Let $p = (a + b\mathrm{i})(c + d\mathrm{i})$ be a proper factorisation, that is with neither factor being a unit.

Conjugating, we get $p = (a - b\mathrm{i})(c - d\mathrm{i})$ and so $a - b\mathrm{i} \mid p$.
If $a + b\mathrm{i}$ and $a - b\mathrm{i}$ are associates then $a = \pm b = \pm 1$, in which case $p = 2$, a contradiction.

Hence $a + b\mathrm{i}$ and $a - b\mathrm{i}$ are coprime and so

$$||a + b\mathrm{i}|| = (a + b\mathrm{i})(a - b\mathrm{i}) \text{ divides } p.$$

Thus $p = a^2 + b^2$.

Hence $x^2 \equiv -1 (\mathrm{mod}\ p)$ has a solution and so $(-1 \mid p) = 0$.
Hence $p \equiv 1 (\mathrm{mod}\ 4)$, a contradiction and so p is prime in $\mathbb{Z}[\mathrm{i}]$.

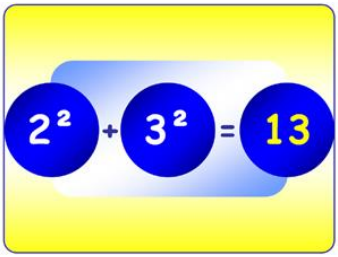
Example 3: The prime integers 2, 5, 13, 17, 29 are composite Gaussian integers.
The prime integers 3, 7, 11, 19, 23, 31 are prime Gaussian integers.

Example 4: The prime Gaussian integers with norm at most 10 are:

norm	Gaussian integers
2	1 + i, 1 – i, –1 + i, –1 – i
3	None
4	2, –2i, –2, – 2i
5	1 + 2i, 1 – 2i, –1 + 2i, –1 – 2i, 2 + i, 2 – i, –2 + i, –2 – i
6	None
7	None
8	none
9	3, 3i, –3, –3i
10	None

§4.2. Sums of Two Squares

Which positive integers can be expressed in the form $a^2 + b^2$? Let $\boldsymbol{\Sigma_n}$ denote the set of positive integers that are sum of n squares of integers. Clearly $\Sigma_m \leq \Sigma_n$ if $m < n$.



Example 5: 1, 2, 4, 5, 8, 9, 10, ... all belong to Σ_2.

Clearly Σ_2 is the set of possible norms for Gaussian integers. Hence it's closed under multiplication. The product of two sums of 2 squares is a sum of two squares, since $\|u\|.\|v\| = \|uv\|$. Of course Σ_1, the set of squares, is also closed under multiplication.

Theorem 6: Suppose $a, b \neq 0$. If $a + b$i divides the positive prime p then $p = a^2 + b^2$.
Proof: Case 1: $a = b = 1$: $p = (1 + \text{i})(c + d\text{i}) = (c - d) + (c + d)\text{i}$ for some $c, d \in \mathbb{Z}$.
Hence $c = -d$ and so $p = 2c$. Hence $c = 1$ and $p = 2$.
Case 2 (the general case): Since $a + b\text{i} \mid p$ and $a - b\text{i} \mid p$.
If $a + b$i and $a - b$i are associates then $a = \pm b$ and so $1 + \text{i}$ divides p, which is case 1. Otherwise $a + b$i and $a - b$i are coprime and so $(a + b\text{i})(a - b\text{i}) \mid p$, that is $a^2 + b^2 \mid p$.
Hence $p = a^2 + b^2$.

Theorem 7: The positive integer prime p is a sum of two squares if and only if $p = 2$ or $p \equiv 1 (\text{mod } 4)$.
Proof: Clearly $2 = 1^2 + 1^2 \in \Sigma_2$.
Suppose $p \equiv 1 (\text{mod } 4)$.
Then by Theorem 5, p is composite in $\mathbb{Z}[\text{i}]$.
Let $a + b$i be a prime divisor of p. Then, by Theorem 6, $p \in \Sigma_2$.
Now suppose $p = a^2 + b^2 > 2$. Clearly $0 < a, b < p$.

Then $a^2 + b^2 \equiv 0 (\text{mod } p)$, so in $\mathbb{Z}_p$ the equation $x^2 = -1$ has a solution.
Thus from the theory of quadratic residues, $(-1|p) = 0$ and so $\frac{p-1}{2}$ is even.
Thus $p \equiv 1 (\text{mod } 4)$.

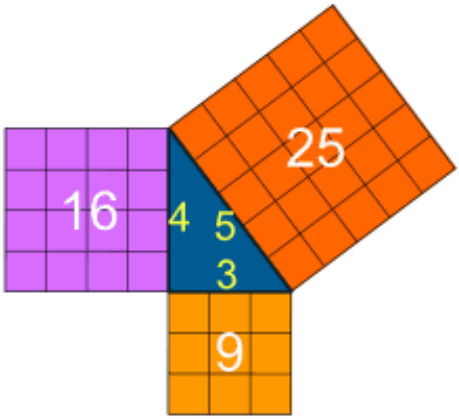
Theorem 8: The positive integer n is a sum of two squares if and only if $n = st^2$ where the odd prime divisors of s are congruent to 1 mod 4.
Proof: Suppose $n = a^2 + b^2$. We prove this by induction on n. It is vacuously true for $n = 1$.
If all the prime factors of n are congruent to 1 mod 4, the theorem holds with $n = s$ and $t = 1$.
Suppose $p \mid n$ where $p \equiv 3 (\text{mod } 4)$. Then by Theorem 5, p is a prime in $\mathbb{Z}[i]$.
Since $p \mid (a + bi)(a - bi)$ then $p \mid a + bi$ or $p \mid a - bi$. In either case p divides the conjugate.
Hence $p \mid 2a$ and $p \mid 2b$.
Since $p > 2$, $p \mid a$ and $p \mid b$.
So $a = pc$ and $b = pd$ for some $c, d \in \mathbb{Z}$.
Hence $n = p^2(c^2 + d^2)$.
By induction, $c^2 + d^2$ has the required form, and therefore so does n.

The converse is clearly true, for if $n = st^2$ where the odd prime divisors of s are congruent to 1 mod 4, the

prime divisors of s are in Σ_2 and $t^2 \in \Sigma_2$ and so by the closure of Σ_2 under multiplication, $n \in \Sigma_2$.

§4.3. Pythagorean Triples

The well-known theorem of Pythagoras states that if a, b, c are the lengths of the sides of a right-angled triangle, with c being the length of the hypotenuse.



A **Pythagorean triple** is a triple of positive integers (a, b, c) such that $a^2 + b^2 = c^2$. The most well-known examples are (3, 4, 5), and (5, 12, 13).

Of course any multiple of a Pythagorean triple is a Pythagorean triple, so that (6, 8, 10) and (300, 400, 500) are also Pythagorean triples.

We define a **primitive Pythagoran triple** to be one where the numbers are coprime. So far the only primitive Pythagorean triple we have exhibited are (3, 4, 5) and (5, 12, 13). Apart from swapping a, b in these examples, are there any others?

Firstly note that if (a, b, c) is a primitive Pythagorean triple then one of a, b is odd and the other is even. Being primitive they can't be both even. Suppose a, b are both odd. Then a^2 and b^2 are both congruent to 1 mod 4 and so $a^2 + b^2 \equiv 2 (\text{mod } 4)$, which is not possible for the square of an integer.

We will quote primitive Pythagorean triples by giving the odd number first.
So a primitive Pythagorean triple will always be given as (ODD, EVEN, ODD).

Theorem 9: The primitive Pythagorean triple are the triple $(u^2 - v^2, 2uv, u^2 + v^2)$ where u, v are coprime positive integers of opposite parity.

Proof: The easy part is to observe that $(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2$.

Now, suppose that (a, b, c) is a primitive Pythagorean triple.

Since $b^2 = (a - c)(a + c)$,

$$\frac{b}{a+c} = \frac{a-c}{b}.$$

Let the common value be $\frac{m}{n}$ where m, n are coprime.

Hence $\frac{a}{b} = \frac{m^2 - n^2}{2mn}$ and


Arithmeticorum Lib. II. 85

QVÆSTIO VIII

QVÆSTIO IX

$\frac{c}{b} = \frac{m^2 + n^2}{2mn}$.

Clearly m, n are not both even and if m, n are both odd then $m^2 + n^2 \equiv 2 (\text{mod } 4)$.

Hence dividing numerator and denominator by 2 we get a rational number of the form $\frac{\text{odd}}{\text{odd}}$. However b is even and c is odd, a contradiction.

Hence m, n have opposite parity and so $m^2 + n^2$ is odd.

So 2 is not a common divisor of $m^2 + n^2$ and $2mn$.

But nor is any odd prime because if $p > 2$ divides $2mn$ it divides m or n.

But since it divides $m^2 + n^2$, if it divides one of m, n it must divide them both, a contradiction.

So $\frac{m^2 + n^2}{2mn}$ is reduced to lowest term, as is $\frac{c}{b}$.

Hence $c = m^2 + n^2$ and $b = 2mn$.

It follows from $a^2 + b^2 = c^2$ that $a = m^2 - n^2$.

As a result of theorem 9 there are infinitely many primitive solutions to the equation $a^2 + b^2 = c^2$. It's natural to ask about solutions to the equation $a^n + b^n = c^n$ in general. Fermat proved that there are no non-trivial solutions for $n = 4$ and wrote in the margin of a book (in Latin) that he had a most wondrous proof that there are no non-trivial solutions to $a^n + b^n = c^n$ for any integer $n > 2$.

It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.

It's unlikely that Fermat really had such a proof, because no general proof was found during the next four centuries despite an enormous amount of effort despite many special cases being proved. The general result is known as Fermat's Last Theorem and it was finally proved in 1995 by Andrew Wiles using techniques from algebraic geometry.

Theorem 10 (FERMAT/WILES): There is no positive integer solution to

$$a^n + b^n = c^n \text{ for } n > 2.$$

§4.4. The Number of Ways of Expressing a Number as a Sum of Two Squares

We've obtained a criterion for a number to be expressible as a sum of squares. Here we ask a stronger question. In how many ways can n be expressed as a sum of squares? We could count trivial variations but we'd be more interested in counting essentially different ways.

Example 6: There are 8 ways of writing 13 as a sum of squares:

$2^2 + 3^2$	$(-2)^2 + 3^2$	$2^2 + (-3)^2$	$(-2)^2 + (-3)^2$
$3^2 + 2^2$	$(-3)^2 + 2^2$	$3^2 + (-2)^2$	$(-3)^2 + (-2)^2$

But we will consider these to be essentially the same.

Now 65, being a product of two primes, each of the form $4n + 1$, is expressible as a sum of squares. In fact it can be written two different ways: $65 = 8^2 + 1^2 = 7^2 + 4^2$. If we include the trivial variations we'd get 16 different ways. The following is an analysis of why we could predict that there are 2 essentially different ways of expressing 65 as a sum of squares, and no more.

Example 7: Find all the, essentially different, ways of expressing 65 as a sum of two squares.

Solution: $65 = 5 \times 13$. Both prime factors are congruent to 1 modulo 4 and so both can be factorised further in the ring of Gaussian integers.

$5 = (2 + i)(2 - i)$ and $13 = (3 + 2i)(3 - 2i)$.

All these factors have prime modulus, and so are prime in $\mathbb{Z}[i]$.

Hence $65 = (2 + i)(2 - i)(3 + 2i)(3 - 2i)$.

Moreover this factorisation is unique, apart from rearrangement and multiplication by units. The units of $Z[i]$ are ± 1 and $\pm i$.

Note that i(3 + 2i) = –2 + 3i and (–i)(2 – i) = –1 – 2i so 65 = (2 + i)(–1 – 2i)(–2 + 3i)(3 – 2i) is essentially the same factorisation.

Suppose $65 = a^2 + b^2$ for integers a, b.
Then $65 = (a + bi)(a – bi)$.
Now each of a + bi and a – bi must be, apart from units, a product of Gaussian primes chosen from the four choices

2 + i	2 – i	3 + 2i	3 – 2i

Since $a + bi$ and $a – bi$ are conjugates each must have the same number of Gaussian prime factors. Moreover each must include one of each conjugate pair.

So there are only two choices:
- $a + bi = (2 + i)(3 + 2i) = 4 + 7i$ and $a – bi = (2 – i)(3 – 2i) = 4 – 7i$ and
- $a + bi = (2 + i)(3 – 2i) = 8 – i$ and $a – bi = (2 + i)(3 – 2i) = 8 + i$.

In the first case we have $a = 4$ and $b = 7$, giving $65 = 4^2 + 7^2$
and in the second case we have $65 = 8^2 + 1^2$.

Theorem 10: If p is a prime of the form $4n + 1$ then p is a sum of squares in only one way (apart from trivial variations).

Proof: p is not a Gaussian prime and so factorises as a product of two Gaussian primes
$a + b\text{i}$ and $a - b\text{i}$.
Apart from rearrangement and multiplication by units this factorisation is unique.
So if $p = m^2 + n^2 = (m + n\text{i})(m - n\text{i})$ then, apart from unit factors, one factor must be $a + b\text{i}$ and the other $a - b\text{i}$, giving $a^2 + b^2$ as the only way of expressing p as a sum of squares, apart from trivial variations.

Example 8: Apart from trivial variations 113 can only be expressed as a sum of two squares as $113 = 8^2 + 7^2$.

Theorem 11: A product of k distinct primes, all of the form $4n + 1$ can be expressed as a sum of two squares in precisely 2^{k-1} ways.
Proof: Let $N = p_1 p_2 \ldots p_k$ where each p_i is a prime of the form $4n + 1$.
Then, for each i, $p_i = (a_i + b_i)(a_i - b_i)$ where $a_i, b_i \in \mathbb{Z}$.

Hence $N = \prod_{i=1}^{k} (a_i + b_i)(a_i - b_i)$.

If $N = m^2 + n^2 = (m + n\text{i})(m - n\text{i})$ then, apart from multiplication by units, $m + n\text{i}$ is a product of k Gaussian primes, one chosen from each conjugate pair and $m - n\text{i}$ is the product of all the remaining factors. There are 2^k such choices. Since $m^2 + n^2 = (m - n\text{i})(m + n\text{i})$ half these

choices will be the same as the other half, with $m + n$i and $m - n$i.

Without loss of generality we may assume that $a_1 + b_i$ is a factor of $m + n$i and $a_1 - b_1$i is a factor of $m - n$i. We may choose the remaining factors in 2^{k-1} ways, leading to 2^{k-1} ways of expressing N as a sum of two squares.

Example 9: Express 1105 as a sum of two squares in as many ways as possible.

Solution: $1105 = 5 \times 13 \times 17$

$= (2 + i)(2 - i)(3 + 2i)(3 - 2i)(4 + i)(4 - i)$

If $1105 = m^2 + n^2$ then $m + n$i is one of the following (remember we are assuming that $m + n$i has $2 + i$ as a factor and $m - n$i has $2 - i$ as a factor so the choice only begins with the second conjugate pair):

$m + n$i $= (2 + i)(3 + 2i)(4 + i) = 9 + 32i$, giving $1105 = 32^2 + 9^2$.

$m + n$i $= (2 + i)(3 + 2i)(4 - i) = 23 + 24i$, giving $1105 = 24^2 + 23^2$.

$m + n$i $= (2 + i)(3 - 2i)(4 + i) = 33 + 4i$, giving $1105 = 33^2 + 4^2$.

$m + n$i $= (2 + i)(3 - 2i)(4 - i) = 31 - 12i$, giving $1105 = 31^2 + 12^2$.

Example 10: Express 625 as a sum of two squares in as many ways as possible.

Solution: $625 = 5^4 = (2 + i)^4(2 – i)^4$.
Suppose $625 = m^2 + n^2 = (m + ni)(m – ni)$.
Then $m + ni$ and $m – ni$ must each be a product of four Gaussian primes chosen from the 8.
The choices are:
$m + ni = (2 + i)^4 = –7 + 24i$, giving $625 = 24^2 + 7^2$.
$m + ni = (2 + i)^3(2 – i) = 5(2 + i)^2 = 15 + 20i$, giving $625 = 20^2 + 15^2$.
$m + ni = (2 + i)^2(2 – i)^2 = 25$, giving $625 = 25^2 + 0^2$.

Example 11: Express 128 as a sum of two squares in as many ways as possible.
Solution: $128 = 2^7 = (1 + i)^7(1 – i)^7$. Now $1 – i = (–i)(1 + i)$ so $128 = (–i)(1 + i)^{14}$.
Suppose $128 = m^2 + n^2 = (m + ni)(m – ni)$.
Then $m + ni$ and $m – ni$ must each be a product of seven Gaussian primes.
Apart from units, the only choice for $m + ni$ is $(1 + i)^7 = 8 – 8i$, giving $128 = 8^2 + 8^2$ as the only way of expressing 128 as a sum of two squares.

§4.5. Overpowering Numbers

In the early 1970's I published a small book, *Numbers, Their Personalities and Properties*, aimed at A Level students in England. It was in John Murray's *Exploring Mathematics on Your Own* series and was

designed for the enthusiastic student who wanted to go beyond the syllabus.

Each chapter discussed some aspect of Number Theory that was connected with the chapter number. For example, chapter 2 was on Quadratic Congruences, chapter 3 discussed primes, chapter 4 was on squares etc. My intention was to go as far as chapter 10, but I was faced with trying to find something interesting to say about the number ten, apart from the fact that we have ten fingers and so adopted base 10 for our number system. Is there anything special about the number ten?

I then came up with the fact that 10 is the only composite number all of whose positive divisors have the form $n^2 + 1$. The chapter occupied itself with proving this useless, but somewhat interesting fact. What other number, apart from 0 and 1, is unique in some natural way. Plenty of numbers are the *smallest* number with a certain property, such as 1729 which is the smallest number which can be expressed as a sum of two cubes in more than one way. Of course 2 is the only even prime, but is that so very special? That's like saying that 97 is the only prime that's a multiple of 97.

When I decided to include this proof in these notes I went to my copy of the book, and to my horror, it only went up to chapter 8! I then remembered cutting out chapters 9 and 10 to keep the book short. I looked for my original typescript and then remembered throwing it out, thinking it was all there in the printed

book. I tried unsuccessfully to reproduce my proof, if indeed it *was* a proof. I dreamt of having come with 'Cooper's Last Theorem', for which I claimed to have had a proof but which was lost, and would take 300 years before it was finally proved, was short lived!

I asked a colleague, Gerry Myerson with whom I had taught at Macquarie University and, to my delight, he came up with a proof within a day. It wasn't the one I'd come up with, but I was beginning to feel that my 'proof' may not have been a valid one after all.

I define an **overpowering number** to be one that is one over a power, or more precisely, has the form $n^k + 1$ for some $k \geq 2$. The first few overpowering numbers are 1, 2, 5, 9, 10, 17, 26, 33, 37, 50. The **overpowering primes** up to 101 are 2, 5, 17, 37, 101.

A **complete overpowering number** is a composite number all of whose divisors are overpowering. The claim is that 10 is the only such number.

Theorem 1: An overpowering prime must have the form $n^2 + 1$.
Proof: Suppose that $p = n^k + 1$ is prime.
If k is odd then $n + 1$ divides p, a contradiction.
So $k = 2h$ is even. Hence $p = (n^h)^2 + 1$. ☺

Theorem 2 (Myerson): The number 10 is the only complete overpowering number.

Proof: Let N be a complete overpowering number.

Clearly any composite divisor of N must also be a complete overpowering number.

N can't be a prime power because $p^2 = n^2 + 1$ is impossible, as the next square beyond n^2 is $(n + 1)^2$ which is greater than p.

Suppose N = pq where p, q are distinct primes and where $p = a^2 + 1$ and $q = b^2 + 1$ for some integers a, b.

It's known that if each of two odd primes p, q is a sum of two squares then pq is a sum of two squares in exactly two different ways (e.g., 5 x 13 = 65 = $8^2 + 1^2 = 7^2 + 4^2$). In our case, $pq = (a^2 + 1)(b^2 + 1) = (ab - 1)^2 + (a + b)^2 = (ab + 1)^2 + (a - b)^2$ gives us the two ways, so in order to have $pq = n^2 + 1$, one of the numbers $ab - 1$, $a + b$, $ab + 1$, $a - b$ must be 1.

Case 1: $ab - 1 = 1$ leads to the number 10 that we already know about.

Case 2: $a + b = 1$ and $ab + 1 = 1$ lead nowhere.

Case 4: $a - b = 1$: One of the two numbers a, b must be odd, so its square is odd, so when you add 1 the result is even, but it's supposed to be a prime, and the only even prime is 2, and so we're back to the number 10.

The only case left to consider is when one of p, q is 2.

Then pq has exactly one representation as a sum of two squares; if, say, $a = 1$, then it's $2(b^2 + 1) = (b + 1)^2 + (b - 1)^2$, so we must have $b + 1 = 1$ or $b - 1 = 1$. Again $b + 1 = 1$ is useless, and $b - 1 = 1$ leads back to 10.

So, 10 is the only composite number with the required property. ✋☺

§4.6. Sums of Three or Four Squares

Every positive integer is the sum of four squares and so $\Sigma_4 = \mathbb{Z}^+$. Hence $\Sigma_4 = \Sigma_5 = ...$
Σ_1 and Σ_2 are closed under multiplication. So too is Σ_4.

Theorem 12: Σ_4 is closed under multiplication.
Proof: $(a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2)$
$= (a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2)^2 + (a_1b_2 - a_2b_1 + c_1d_2 - c_2d_1)^2$
$+ (a_1c_2 - a_2c_1 + b_2d_1 - b_1d_2)^2$
$+ (a_1d_2 - a_2d_1 + b_1c_2 - b_2c_1)^2$.

So, to prove that $\Sigma_4 = \mathbb{Z}^+$ it is sufficient to prove that every prime is the sum of 4 squares. I omit this proof.

Theorem 13 (LAGRANGE): Every positive integer is the sum of four squares.

The case of Σ_3 is a little more difficult, because it's not closed under multiplication. For example 3, 5 $\in$ Σ_3 but 15 is not. That is why the analysis of Σ_3 involves different methods to the others.

Theorem 14: $n \in \Sigma_3$ if and only if n is not of the form $4^m(8k + 7)$.

Proof: I prove that if $n = 4^m(8k + 7)$ then $n \notin \Sigma_3$.

The square of an integer is congruent to 0, 1 or 4 modulo 8. Hence the sum of 3 squares cannot be congruent to 7 modulo 8. So the theorem is true for $m = 1$.

Suppose that $4^m(8k + 7)$ is a sum of 3 squares and suppose that m is the least for which such an integer is a sum of 3 squares.

We've shown that $m \geq 1$.

Suppose that $4^m(8k + 7) = x^2 + y^2 + z^2$.

This is congruent to 0 modulo 4, while a square is congruent to 0 or 1 mod 4.

This can only be if x^2, y^2, z^2 are all congruent to 0 modulo 4, that is, if x, y, z are all even.

Let $x = 2x_1$, $y = 2y_1$ and $z = 2z_1$.

Then

$$4^m(8k + 7) = 4(x_1^2 + y_1^2 + z_1^2) \text{ whence}$$

$$4^{m-1}(8k + 7) = x_1^2 + y_1^2 + z_1^2, \text{ contradicting the minimality of } m.$$

It remains to prove that if n is not of the form $4^m(8k + 7)$ then it is the sum of 3 squares.
This is somewhat more difficult and I omit this proof.

§4.7. Waring's Problem

Now let's move beyond sums of squares to sums of higher powers. If k is a positive integer define $\omega(k)$ to be the smallest number n, if one exists, such that every positive integer is a sum of n non-negative k'th powers. Clearly $\omega(1) = 1$ and we announced in the previous section that $\omega(2) = 4$.

Waring's problem was to determine whether $\omega(k)$ exists for all k. Hilbert has solved this problem by showing that $\omega(k)$ does, indeed, exist for all k. The problem then becomes to find the value of $\omega(k)$, or at least upper and lower bounds for it.

It has been shown that $\omega(3) = 9$. However only 23 and 239 require 9 cubes and only a further 15 integers require 8 cubes. Apart from these 17 exceptions, every positive integer can be represented as a sum of 7 cubes.

So a more meaningful constant is $\Omega(k)$, the smallest number n, such that all but a finite number of positive integers can be expressed as a sum of n non-negative k-th powers. From what we've just said it follows that $\Omega(3) \leq 7$.

For 4^{th} powers, all that's known is that $4 \leq \Omega(4) \leq 7$. It's conjectured that $\Omega(4) = 4$.