CHAPTER XIII

COMPLEX INTEGERS

§ 1. Complex integers and their norm. Associated integers. The *complex* or *Gaussian integers* are the complex numbers $a+bi$, where a, b are integers.

The theory of complex integers is important for two reasons, firstly because it is interesting to see how far the properties of ordinary integers are susceptible to generalization, and secondly because various properties of ordinary integers themselves follow most simply from those of the wider class. The proofs of these properties obtained in another way turn out to be much more difficult.

An immediate consequence of the definition of arithmetical operations on complex numbers is that the sum the difference and the product of two or more complex integers is also a complex integer.

EXERCISES. **1.** Find all the possible representations of the number 0 as the sum of the squares of two complex integers.

Answer. $0 = (a+bi)^2+(\pm b\mp ai)^2$, where a, b are arbitrary rational integers, and either both upper or both lower signs are taken.

2. Find the complex integers $x+yi$ which are representable as sums of the squares of two complex integers.

Solution. In order that an integer $x+yi$ be the sum of the squares of two complex integers it is necessary and sufficient that y should be even and, in the case where x is of the form $4t+2$, y should be divisible by 4.

The condition is necessary because if

$$x+yi = (a+bi)^2+(c+di)^2,$$

then

$$x = a^2-b^2+c^2-d^2, \quad y = 2(ab+cd).$$

Hence, as one verifies directly, x is of the form $4t+2$ if at least one of the numbers a and b and at least one of the numbers c and d are even. But then the number $ab+cd$ is even, which shows that y is divisible by 4.

The condition is also sufficient because, if $x = 2t+1$ and $y = 2u$, then

$$x+yi = (t+1+ui)^2+(u-ti)^2.$$

If $x = 4t+2$ and $y = 4u$, then

$$x+yi = (t+u+1+(u-t)i)^2+(t-u+1+(t+u)i)^2.$$

If $x = 4t$ and $y = 4u$, then

$$x+yi = (t+1+ui)^2+(u+(1-t)i)^2,$$

finally, if $x = 4t$ and $y = 4u+2$, then

$$x+yi = (t+u+1+(u+1-t)i)^2+(t-u+(t+u)i)^2.$$

3. Prove that a complex integer $x+yi$ is representable as the sum of the squares of three complex integers if and only if y is even.

Hint. Use exercise 2 and the identity

$$4t+2+2ui = 4t+1+2ui+1^2.$$

4. Prove that a complex integer $a+bi\neq 0$ is the square of a complex integer if and only if

$$a^2+b^2 = c^2, \quad c+a = 2x^2 \quad \text{and} \quad c-a = 2y^2,$$

where c is a natural number and x, y are rational integers. Prove that then

$$a+bi = (\pm x\pm yi)^2,$$

where the signs should be identical if $b > 0$ and opposite if $b < 0$.

Remark. The theorem formulated in exercise 4 may be thought of as a test for verifying whether a given complex number is the square of a complex integer, and as a method of finding the complex integral square roots of a complex integer (in the case where such roots exist).

For a given complex number $z = a+bi$ we denote by z' its conjugate complex number, i.e. the number $z' = a-bi$.

As an immediate consequence of the definition of the arithmetical operations on complex numbers, we have

(1) if $z = t+u$, then $z' = t'+u'$,

(2) if $z = t-u$, then $z' = t'-u'$,

(3) if $z = tu$, then $z' = t'u'$.

Clearly, either the numbers z and z' are both complex integers or none of them is a complex integer. The number $(z')'$, the conjugate of z', is equal to z.

The product zz' of two conjugate numbers is called the *norm* of the number z and denoted by $N(z)$. We write

$$N(z) = zz'.$$

Consequently, if $z = a+bi$ (where a, b are real numbers), we have

$$N(z) = a^2+b^2.$$

Therefore the norm of a complex number is always real and non-negative, being equal to zero only if $a = b = 0$, i.e. if $z = 0$.

Moreover, the norm of a non-zero complex integer is a natural number.

The conjugates have the same norm. We say that a complex integer z is *divisible* by a number t if there exists a complex integer u such that

$$z = tu. \tag{4}$$

We then write $t \mid z$.

To establish whether a complex integer $a+bi$ is divisible by a complex number $c+di$, not equal to 0, one has to know whether certain divisibilities among rational integers hold. In fact, the formula

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\, i$$

implies that

$$c+di \mid a+bi$$

is valid if and only if

$$c^2+d^2 \mid ac+bd \quad \text{and} \quad c^2+d^2 \mid bc-ad.$$

For example,

$$3+5i \mid 21+i \quad \text{because} \quad 34 \mid 68 \quad \text{and} \quad 34 \mid -102,$$

$$1+i \mid 2 \quad \text{because} \quad 2 \mid 2 \quad \text{and} \quad 2 \mid -2;$$

on the other hand,

$$1-2i \nmid 1+2i \quad \text{because} \quad 5 \nmid -3.$$

It follows from (3) that, if $t \mid z$, then $t' \mid z'$ and if $z = tu$, then

$$zz' = tut'u' = tt'uu',$$

whence, by the definition of the norm of a complex number,

$$N(z) = N(t)N(u). \tag{5}$$

We express this by saying that the *norm of the product of two complex numbers is the product of their norms.*

This theorem is easily generalized to the product of any finite number of factors.

By (5) we also have $N(t) \mid N(z)$; consequently, *if a complex integer t is a divisor of a number z, then the norm of t is a divisor of the norm of z.*

The converse, however, is not true. For example, $N(1-2i) = N(1+2i)$ but $1-2i \nmid 1+2i$.

Two complex integers, both not 0, which divide each other are called *associated.*

Consequently, z and t are associated if and only if $t \mid z$ and $z \mid t$. We then have $N(t) \mid N(z)$ and $N(z) \mid N(t)$, which, in virtue of the fact that the norm of a non-zero complex integer is different from zero, gives $N(t) = N(z)$.

Thus *any two associated complex integers have equal norms* (the converse is false: the numbers $1-2i$ and $1+2i$ have equal norms but are not associated because, as we have learned, $1-2i \nmid 1+2i$).

Now we are going to find the associates of a given complex integer $z \neq 0$.

Let t be associated with z; then, for a complex integer u, we have $t = zu$, whence

$$N(t) = N(z)N(u). \tag{6}$$

But, since associates have equal norms, $N(z) = N(t)$ and $N(z) \neq 0$ because $z \neq 0$. Consequently, (6) proves that $N(u) = 1$.

Let $u = a+bi$, whence $a^2+b^2 = 1$. Therefore, either $a = \pm 1$ and $b = 0$, or, conversely, $a = 0$ and $b = \pm 1$. From this we conclude that u is one of the four numbers $1, -1, i, -i$, and so $t = zu$ is one of the four numbers

$$z, \quad -z, \quad iz, \quad -iz. \tag{7}$$

Thus we see that any associate of z is one of the numbers (7). Conversely, it is easy to see that each of the numbers (7) is associated with z. This is because $z = (-1)(-z) = (-i)iz = i(-iz)$. Thus we arrive at

THEOREM 1. *Any complex integer z, not equal to 0, has exactly four associates, namely, the numbers* (7).

It is clear that (since $z \neq 0$) all the four associates are different.

In problems concerning divisibility of complex integers, associated numbers can be replaced by one another. The reason is that, if z is divisible by t, then any associate of z is divisible by any associate of t.

It is also clear that if z is associated with t, then z' is associated with t'.

If two complex integers z_1 and z_2 are divisible by t, then their sum and their difference are divisible by t. In fact, if $z_1 = tu$ and $z_2 = tv$, then $z_1 \pm z_2 = t(u \pm v)$.

If a complex integer z is divisible by t and t is divisible by u, then z is divisible by u. In fact, if $z = tw$ and $t = uv$, then $z = uvw$.

This, in consequence, shows that, if t is a common divisor of complex integers $z_1, z_2, \ldots, z_n$ and if $u_1, u_2, \ldots, u_n$ are any complex integers, then $t \mid z_1u_1 + z_2u_2 + \ldots + z_nu_n$.

§ 2. Euclidean algorithm and the greatest common divisor of complex integers. We now prove

THEOREM 2. *If z and $t \neq 0$ are complex integers, then there exist complex integers c and r such that*

$$z = ct + r \tag{8}$$

and

$$N(r) \leqslant \tfrac{1}{2} N(t), \tag{9}$$

whence $N(r) < N(t)$.

Proof. Let

$$z/t = x + yi, \tag{10}$$

where x, y are rationals. Let ξ and η be the integers closest to x and y, respectively. Then we may write

$$x = \xi + x_1, \quad y = \eta + y_1, \tag{11}$$

where x_1 and y_1 are rational numbers such that

$$|x_1| \leqslant \tfrac{1}{2}, \quad |y_1| \leqslant \tfrac{1}{2}. \tag{12}$$

Let

$$c = \xi + \eta i, \quad r = z - ct. \tag{13}$$

It is clear that c, r are complex integers and that they satisfy (8). At the same time, by (10), (11), (13), we have

$$r = z - ct = (x + yi)t - (\xi + \eta i)t = (x_1 + y_1 i)t.$$

Since the norm of a product is equal to the product of the norms of the factors, we obtain by (12)

$$N(r) = N(x_1 + y_1 i) N(t) = (x_1^2 + y_1^2) N(t), \qquad x_1^2 + y_1^2 \leqslant \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}$$

which proves (9) and at the same time completes the proof of the theorem.

The theorem just proved provides an algorithm similar to the Euclidean algorithm proved for rational integers.

It embodies the ordinary process for finding the greatest common divisor of two given complex integers, z and $t \neq 0$. At first, by means of theorem 2, we find the numbers c, r. By (8), we infer that the numbers z and t have the same common divisors as the numbers t and r. Moreover, by (5), $N(r) < N(t)$. Thus in order to find the common divisors of the numbers z and t it is sufficient to find the common divisors of the numbers t and r, where $N(r) < N(t)$.

If $r = 0$, then the common divisors of the numbers z and t are precisely the divisors of the number t.

If $r \neq 0$, then we apply the above procedure with the numbers t, r in place of z, t. Thus to find the common divisors of the numbers t, r we have to find the common divisors of the numbers r, r_1, where $N(r_1) < N(r)$.

If $r_1 \neq 0$, we find another number r_2, and so on.

The sequence $r, r_1, r_2, \ldots$ cannot be infinite, because the corresponding sequence of norms is a strictly decreasing sequence of natural numbers. Therefore, for some n, $r_n = 0$. Then the common divisors of r_{n-1} and r_{n-2} are precisely the divisors of the number r_{-1}. Thus we reach the conclusion that there exists a complex integer ϱ whose divisors are precisely the common divisors of the numbers z and t.

This shows that two given complex integers different from zero have at least one common divisor that is divisible by any of their common divisors. It is a natural thing to call it the *greatest common divisor* of the given two complex integers.

Now we are going to establish the number of the greatest common divisors of two complex integers. Let d and δ be the greatest common divisors of complex integers z, t. The numbers d, δ are divisible each by the other, therefore they are associated complex integers. Hence, by theorem 2, we obtain the following

COROLLARY. *Any two complex integers different from 0 have precisely four greatest common divisors, these being accociated with each other.*

Actually, rational integers also have two greatest common divisors which differ in the sign. They are such that each of them is divisible by any common divisor of the given numbers. However, if we find the number of common divisors, we do not distinguish between the divisors that differ in the sign only. Similarly, in the case of complex integers we could consider only one greatest common divisor of any two complex integers identifying associated divisors. At any rate, either approach is nothing but a more or less convenient convention.

EXAMPLES. **1.** By means of the algorithm presented above we find the greatest common divisors of the numbers $6-17i$ and $18+i$. Using the successive steps of the algorithm, we find

$$\frac{6-17i}{18-i} = \frac{(6-17i)(18-i)}{18^2+1} = \frac{91-312i}{325} = -i + \frac{91+13i}{325},$$

$$6-17i = -i(18+i) + (5+i),$$

$$\frac{18+i}{5+i} = \frac{(18+i)(5-i)}{5^2+1} = \frac{91-13i}{26} = 3 + \frac{1-i}{2},$$

$$18+i = 3(5+i) + 3 - 2i,$$

$$\frac{5+i}{3-2i} = \frac{(5+i)(3+2i)}{3^2+2^2} = 1+i.$$

Therefore the greatest common divisors of the numbers $6-17i$ and $18+i$ are the number $3-2i$ and the numbers associated with it, i.e. $-3+2i$, $2+3i$, $-2-3i$.

2. We find the greatest common divisors of the numbers $2+3i$ and $2-3i$. We have

$$\frac{2+3i}{2-3i} = \frac{(2+3i)^2}{2^2+3^2} + \frac{5+12i}{13} = i + \frac{5-i}{13},$$

$$2+3i = i(2-3i)+i-1,$$

$$\frac{2+3i}{i-1} = \frac{-(2-3i)(i+1)}{2} = \frac{-5+i}{2} = -3+\frac{1+i}{2},$$

$$2-3i = -3(i-1)-1.$$

Therefore the greatest common divisors of the numbers $2+3i$ and $2-3i$ are the number 1 and its associates: -1, i and $-i$.

3. We find the greatest common divisors of the numbers $31+i$ and $5+i$. We have

$$\frac{31+i}{5+i} = \frac{31+i(5-i)}{5^2+1^2} = \frac{156-26i}{26} = 6-i.$$

Therefore the greatest common divisors of the complex integers $31+i$ and $5+i$ are the number $5+i$ and its associates: $-5-i$, $-1+5i$ and $1-5i$.

It is easy to see that the greatest common divisors have the greatest norm among all the common divisors of the numbers, the converse being also true. So the greatest common divisors could also be defined as the common divisors whose norms assume the greatest possible values. These, however, would make it more difficult to prove the most important property of the greatest common divisors, namely that they are divisible by any common divisor.

The theory of the greatest common divisors of two or more complex integers can easily be established by considering linear forms, just as has been done in the case of rational integers. In fact, let $a_1, a_2, \ldots, a_m$ be complex integers different from zero. Let Z be the set of non-zero numbers of the form

$$a_1z_1+a_2z_2+\ldots+a_mz_m,$$

where $z_1, z_2, \ldots, z_m$ are complex integers. Finally, let N be the set of the values of the norm of the numbers of Z. Clearly, N is the set of natural numbers. Let n be the least natural number of the set N. Therefore there exists a number ζ in Z such that $N(\zeta) = n$, which means that there exist complex integers $\zeta_1, \zeta_2, \ldots, \zeta_m$ such that

$$\zeta = a_1\zeta_1+a_2\zeta_2+\ldots+a_m\zeta_m. \tag{14}$$

We are going to show that each number of the set Z is divisible by ζ. In fact, let z be any number of the set Z. Then there exist complex integers $z_1, z_2, \ldots, z_m$ that

$$z = a_1z_1+a_2z_2+\ldots+a_mz_m. \tag{15}$$

Moreover, by theorem 2, there exist complex integers c and r such that

$$z = c\zeta+r \quad \text{and} \quad N(r) < N(\zeta). \tag{16}$$

If $r \neq 0$, then r belongs to Z because, by (14), (15) and (12),

$$r = z-c\zeta = a_1(z_1-c\zeta_1)+a_2(z_2-c\zeta_2)+\ldots+a_m(z_m-c\zeta_m),$$

and, moreover, the numbers $z_j-c\zeta_j$, $j = 1, 2, \ldots, m$, are complex integers. But then, by (16), r is a number whose norm is less than the norm n of ζ, contrary to the definition of n. Consequently $r = 0$, whence, by (16), $z = c\zeta$ and so $\zeta \mid z$.

It is clear that each of the numbers $a_1, a_2, \ldots, a_m$ belongs to the set Z. Therefore, in virtue of what we proved above, the complex integer ζ is a common divisor of the numbers $a_1, a_2, \ldots, a_m$.

Now let δ be any common divisor of these numbers. Then there exist complex integers $t_1, t_2, \ldots, t_m$ such that $a_j = t_j\delta$ for any $j = 1, 2, \ldots, m$. Hence, by (14),

$$\zeta = (t_1\zeta_1+t_2\zeta_2+\ldots+t_m\zeta_m)\delta,$$

which shows that $\delta \mid \zeta$. From this we conclude that ζ is a common divisor of the numbers $a_1, a_2, \ldots, a_m$ which is such that any common divisor of these numbers divides it. At the same time we have proved that ζ is representable in form (14), where $\zeta_1, \zeta_2, \ldots, \zeta_m$ are complex integers.

Any two complex integers a, b have at least four common divisors, 1, -1, i, $-i$.

If the complex integers a, b have no more than these four divisors, they are called *relatively prime*. We then write $(a, b) = 1$.

It is easy to see that then there exist complex integers x, y which satisfy the equation

$$ax+by = 1. \tag{17}$$

In fact, if $(a, b) = 1$, the number ζ defined by (14) with $a = a_1$, $b = a_2$, $m = 2$ must be one of the numbers 1, -1, i, $-i$. Consequently, one of the numbers ζ, $-\zeta$, $i\zeta$, $-i\zeta$ must be equal to 1 and this implies that for an appropriate choice of complex integers x, y (17) holds.

On the other hand, (17) implies that any common divisor of the numbers a, b is a divisor of the number 1, therefore the numbers a, b

cannot possibly have any common divisor different from 1, -1, i, $-i$, this being equivalent to saying that $(a, b) = 1$.

THEOREM 3. *Two complex integers a, b are relatively prime if and only if there exist complex integers x, y such that $ax+by = 1$.*

Now we consider three complex integers a, b, c, about which we assume that $(a, b) = 1$ and $b \mid ac$. We prove that then $b \mid c$.

In fact, since $(a, b) = 1$, by theorem 3 there exist complex integers x, y which satisfy equation (17). This, multiplied by c, gives

$$acx + bcy = c. \tag{18}$$

By assumption, $b \mid ac$ and, clearly, $b \mid bc$ for any b. Therefore (18) implies that $b \mid c$, which was to be proved. Thus we have obtained

THEOREM 4. *For any complex integers a, b, c the relations $(a, b) = 1$ and $b \mid ac$ imply $b \mid c$.*

Another consequence of theorem 3 is

THEOREM 5. *If $(a, b) = 1$ and $(a, c) = 1$, then $(a, bc) = 1$.*

Proof. If $(a, b) = 1$ and $(a, c) = 1$, then there exist complex integers x, y, u, v such that $ax+by = 1$ and $au+cv = 1$. Multiplying together these equalities we obtain $a\big(x(au+cv)+buy\big)+bcyv = 1$, whence $(a, bc) = 1$.

§ 3. The least common multiply of complex integers. Let $a_1, a_2, \ldots, a_m$ be complex integers different from zero. There are of course various common multiples of these numbers, e.g. the one obtained by multiplying by one another. Among them we select those for which the norm is the least, i.e. not greater than the norm of any common multiple of these numbers. Let ν be such a common multiple of $a_1, a_2, \ldots, a_m$. We prove that any common multiple of the numbers $a_1, a_2, \ldots, a_m$ is divisible by ν.

In fact, let z be any common multiple of these numbers. By theorem 2 there exist complex integers c, r such that $z = c\nu + r$ and $N(r) < N(\nu)$. If r were equal to zero, then r, being a common multiple of $a_1, a_2, \ldots, a_m$, would have a norm less than ν, contrary to the definition of the number ν. Consequently $r = 0$, and this means that there exists at least one common multiple of the numbers $a_1, a_2, \ldots, a_m$ which is such that any common multiple of these numbers is divisible by it.

The norm of any common multiple with this property is, in fact, not greater than the norm of any common multiple of the numbers $a_1, a_2, \ldots, a_m$. We call it the *least common multiple* of the numbers $a_1, a_2, \ldots, a_m$.

It is easy to see that all the least common multiples of the numbers $a_1, a_2, \ldots, a_m$ are associated and that their norm is the least among the norms of common multiples of these numbers.

EXERCISE. Find the solution of the equations

$$x+y+z = xyz = 1$$

in complex integers.

Solution. Since $xyz = 1$, the numbers x, y, z must be divisors of unity, i.e. they must be numbers of the sequence $1, -1, i, -i$. Again from $xyz = 1$ it follows that they cannot all be imaginary; on the other hand, the equality $x+y+z = 1$ shows that if the three of them are real, then two are equal to 1, the third being equal to -1, but this contradicts the $xyz = 1$. Therefore at least one of the numbers x, y, z is imaginary, but then, by $x+y+z = 1$, at least two of them are imaginary. Thus we arrive at the final conclusion that one of the numbers x, y, z must be i, the others being $-i$ and 1. We see that the only solutions of our system of equations are $x = 1$, $y = i$, $z = -i$ and those which can be obtained from them by permuting the numbers $1, i, -i$. The number of solutions is thus equal to 6.

Remark. As is proved by J. W. S. Cassels [4], the system of equations $x+y+z = xyz = 1$ has no solutions in ordinary rational numbers x, y, z (see also Sansone and Cassels [1]).

§ 4. Complex primes. Since any complex integer has at least the four divisors $1, -1, i, -i$ and, moreover, any complex integer z, not an associate of 1, has other four divisors, namely $z, -z, iz, -iz$, we see that any such complex integer has at least eight different divisors.

The complex integers which have precisely the 8 divisors are called *primes*.

In other words, a complex integer is prime if it has no divisors except its associates, and the associates of 1, and moreover, if it is not associated with 1.

It is clear that this definition is equivalent to the following one:

A complex integer is a prime if its norm is greater than 1 and if it is not representable as the product of complex integers with norms greater than 1.

In fact, if ζ is a complex integer, $N(\zeta) > 1$ and $\zeta = \mu\nu$, where $N(\mu) > 1$ and $N(\nu) > 1$, then the number μ cannot be associated either with 1, because, if it could, $N(\mu) = 1$, nor with ζ, because then $N(\mu) = N(\zeta)$, whence, by $N(\zeta) = N(\mu)\times N(\nu)$, it would follow that $N(\nu) = 1$, contrary to the assumption. Consequently, ζ has a divisor μ which is not associated with 1 or with ζ, and so it is not a prime.

On the other hand, if ζ is a complex integer with $N(\zeta) > 1$ and if it is not a prime, then, by definition, it has a divisor μ which is not associated either with 1 or with ζ. We then have $\zeta = \mu\nu$, where ν is a complex integer.

If $N(\mu) = 1$, then μ is associated with 1, contrary to the assumption (in fact, if for a complex integer $a+bi$ we have $N(a+bi) = 1$, then $a^2+b^2 = 1$, whence, since a, b are rational integers, either $a = \pm 1$ and $b = 0$, or $a = 0$ and $b = \pm 1$).

If $N(\nu) = 1$, then the number ν is associated with 1, whence, by $\zeta = \mu\nu$, the number μ is associated with ζ, contrary to the assumption. Consequently, $N(\mu) > 1$ and $N(\nu) > 1$, and so the number ζ is the product of two complex integers with norms greater than 1.

It is clear that *any complex integer which is associated or conjugated with a prime complex integer is a prime complex integer.*

THEOREM 6. *Any complex integer whose norm is greater than* 1 *is representable as the product of finitely many prime complex integers.*

Proof. Suppose to the contrary that there is a complex integer with a norm n greater than 1 which is not representable as the product of finitely many prime complex numbers. Let M be the set of the values of the norm of all the complex integers with this property. Thus M is a non-void set of natural numbers. Let m be the least number belonging to M. Accordingly, there exists a complex integer z with norm m which is not representable as the product of finitely many prime complex integers. By assumption, z is not a prime and its norm is $m > 1$. Consequently, it is the product of two complex integers, μ and ν, with norms greater than 1. Moreover, $m = N(z) = N(\mu\nu) = N(\mu)N(\nu)$, whence it follows that $N(\mu) < m$ and $N(\nu) < m$. From the definition of m we infer that each of the numbers μ, ν is representable as the product of finitely prime complex integers. But this shows that also the number $z = \mu\nu$ is representable in such a form, contrary to the definition of z. The theorem is thus proved.

By definition any complex integer π has precisely the eight divisors

$$1, \quad -1, \quad i, \quad -i, \quad \pi, \quad -\pi, \quad i\pi, \quad -i\pi.$$

From this we infer that, *if a complex integer λ is not divisible by a prime complex integer π, then* $(\lambda, \pi) = 1$.

A natural number which is a prime complex integer is of course a prime (in the ordinary sense). The converse, however, is not true: there are primes which are not prime complex integers. For example,

$$2 = (1+i)(1-i) \quad \text{and} \quad N(1+i) = N(1-i) = 2 > 1.$$

The numbers $1+i$ and $1-i$ are prime complex integers. This follows from the fact that, if $1 \pm i = \mu\nu$, then

$$N(\mu)N(\nu) = N(\mu\nu) = N(1 \pm i) = 2;$$

so (in virtue of the fact that the norm of a complex integer is a natural number) we must have $N(\mu) = 1$ or $N(\nu) = 1$, which proves that either μ or ν is associated with 1.

The numbers $1+i$ and $1-i$ are associated because $1-i = -i(1+i)$. Thus we see that the number 2 is associated with the square of a prime complex integer.

Using theorem 4 one can easily prove that the representation of a complex integer as a product of prime complex integers is unique apart from the order of the primes and ambiguities of associated primes.

In this connection, we are going to characterize the prime complex integers in the set of all complex integers.

We start with determining the natural numbers which, regarded as complex integers, are prime. Clearly, they must be ordinary primes, and, moreover, they should be odd, since the number two has been shown not to be of this sort. Thus we have to consider the primes of the form $4k+1$ and $4k+3$, where k is a natural number.

Let p be a prime of the form $4k+1$. By theorem 9, Chapter V, there exist natural numbers a, b such that $p = a^2+b^2$, whence $p = (a+bi)(a-bi)$ and, moreover, $N(a \pm bi) = a^2+b^2 = p > 1$. Thus p is not a prime complex integer.

The factors $a+bi$ and $a-bi$, however, are prime complex integers. In fact, if $a+bi = \mu\nu$, where

$$(19) \qquad N(\mu) > 1 \quad \text{and} \quad N(\nu) > 1,$$

then $p = N(a+bi) = N(\mu)N(\nu)$, which is impossible, since p is a prime.

From this we conclude that *the complex factors of primes of the form* $4k+1$, *where k is a natural number, are prime complex numbers.*

It is easy to see that these factors are not associated with each other. In fact, the identity $a+bi = a-bi$ is impossible, since it implies $b = 0$ and $p = a^2$. The identity $a+bi = -(a-bi)$ is also impossible because it implies $a = 0$, $p = b^2$. If $a+bi = i(a-bi)$, then $a = b$ and so $p = 2a^2$, which is impossible. Finally, if $a+bi = -i(a-bi)$, then $a = -b$ and so $p = 2a^2$, which is impossible.

As for the *primes of the form* $4k+3$, *where k is a non-negative rational integer*, we show that they *are prime when regarded as complex integers.*

In fact, if a prime $p = 4k+3$ were a product of two complex integers with norms greater than 1, then

$$p = (a+bi)(c+di),$$

whence, passing to the norms,

$$p^2 = (a^2+b^2)(c^2+d^2),$$

where $a^2+b^2 > 1$ and $c^2+d^2 > 1$. Since p is a prime, this would give $p = a^2+b^2$, but this is impossible for any prime of the form $4k+3$.

Thus we see that among the primes precisely the primes of the form $4k+3$ are prime complex integers. Other prime complex integers are the number $1+i$ and the conjugate complex factors of the primes of the form $4k+1$.

In virtue of what we proved above, any natural number >1 is a product of prime complex integers of one of the sorts we have just listed or of their associates.

It is clear that there cannot be any other complex prime integers because, if π were such a prime, then, in virtue of the uniqueness of the decomposition of a complex integer into prime complex integers, π would not be a complex prime divisor of any natural number. But $\pi\pi' = N(\pi)$, which is a contradiction.

We have thus proved

THEOREM 7. *The complex prime integers are those of the following three classes and their associates*:

1. $1+i$,
2. *the complex prime factors of the primes of the form* $4k+1$,
3. *primes of the form* $4k+3$.

Here are the prime complex integers (one out of each of the four associates) whose norms are less than 100:

$$1+i,\quad 1\pm 2i,\quad 3,\quad 2\pm 3i,\quad 1\pm 4i,\quad 2\pm 5i,\quad 1\pm 6i,$$
$$4\pm 5i,\quad 7,\quad 2\pm 7i,\quad 5\pm 6i,\quad 3\pm 8i,\quad 5\pm 8i,\quad 4\pm 9i.$$

Two complex primes whose difference is 2 are said to form a pair of *twin* complex primes. For example, $4+i$, $6+i$; $3i$, $2+3i$; $3+2i$, $5+2i$; $7i$, $2+7i$. There are known twin complex primes that form arithmetical progressions of difference 2 consisting of three terms. For example, $2+i$, $4+i$, $6+i$ or $1+2i$, $3+2i$, $5+2i$.

Conjecture H (Chapter III, § 8) implies that there exist infinitely many pairs of complex twin primes. In fact, let $f_1(x) = x^2-2x+2$, $f_2(x) = x^2+2x+2$. The polynomials $f_1(x)$ and $f_2(x)$ have no rational roots and consequently they are irreducible. We also have $f_1(0)f_2(0) = 4$, $f_1(1)f_2(1) = 5$, which shows that the condition S is satisfied. Therefore, in view of conjecture H, there exist infinitely many natural numbers x such that $f_1(x)$ and $f_2(x)$ are both prime. But $f_1(x) = (x-1)^2+1$, $f_2(x) = (x+1)^2+1$ and x must be odd since otherwise $2\,|\,f_2(x)$ and $f_2(x) > 2$, whence $f_2(x)$ would be composite. Consequently, the numbers $f_1(x)$ and $f_2(x)$ are both of the form $4k+1$ and so the numbers $x-1\pm i$ and $x+1\pm i$ are prime complex integers, their difference being equal to 2. Thus we have obtained an infinite sequence of different pairs of complex twin primes. Such pairs are obtained, for example, for $x = 3, 5, 15, 25, 55, \ldots$ However, there are pairs of complex twin primes that are not obtained in this way, for example, $1+2i$, $3+2i$ or $3+8i$ and $5+8i$.

Pairs of complex twin primes have been considered by D. Shanks (see Shanks [3]).

§ 5. The factorization of complex integers into complex prime factors. We now show a method how a complex integer z can be represented as the product of complex primes.

Let $N(z) = n$. Any prime factor of the number z is of course a prime factor of its norm $n = zz'$. Complex prime factors of the natural number n can easily be obtained by finding its rational prime factors. In fact, let

$$n = 2^{a}p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}q_1^{\beta_1}q_2^{\beta_2}\ldots q_l^{\beta_l}, \tag{20}$$

where the p's are primes of the form $4t+1$ [1] and the q's are primes of the form $4t+3$. Let π_j and π_j', $j = 1, 2, \ldots, k$, denote the conjugate complex prime factors of the number p_j. Let $\pi_j = a+bi$ and $\pi_j' = a-bi$; then $p_j = a^2+b^2$. Then the factorization of n into complex prime factors is as follows:

$$n = (-i)^{a}(1+i)^{2a}\pi_1^{a_1}\pi_1'^{a_1}\pi_2^{a_2}\pi_2'^{a_2}\ldots\pi_k^{a_k}\pi_k'^{a_k}q_1^{\beta_1}q_2^{\beta_2}\ldots q_l^{\beta_l}. \tag{21}$$

Since $n = zz'$, we see that

$$z = i^{\nu}(1+i)^{\lambda}\pi_1^{\lambda_1}\pi_1'^{\lambda_1'}\pi_2^{\lambda_2}\pi_2'^{\lambda_2'}\ldots\pi_k^{\lambda_k}\pi_k'^{\lambda_k'}q_1^{\mu_1}q_2^{\mu_2}\ldots q_l^{\mu_l}, \tag{22}$$

where ν is one of the numbers 1, 2, 3, 4, the remaining exponents λ $\lambda_1, \lambda_1', \ldots, \lambda_k, \lambda_k', \mu_1, \ldots, \mu_l$ being non-negative integers. Passing to the norms in (22), in virtue of the equalities $N(\pi_j) = p_j$ and $N(q_j) = q_j^2$, we obtain

$$N(z) = 2^{\lambda}p_1^{\lambda_1+\lambda_1'}p_2^{\lambda_2+\lambda_2'}\ldots p_k^{\lambda_k+\lambda_k'}q_1^{2\mu_1}q_2^{2\mu_2}\ldots q_l^{2\mu_l},$$

whence, by (21) and the fact that $N(z) = n$, comparing the exponents on equal primes, we obtain

$$\begin{gathered}\lambda = a,\quad \lambda_1+\lambda_1' = a_1,\quad \lambda_2+\lambda_2' = a_2,\quad \ldots,\quad \lambda_k+\lambda_k' = a_k,\\ 2\mu_1 = \beta_1,\quad 2\mu_2 = \beta_2,\quad \ldots,\quad 2\mu_l = \beta_l.\end{gathered} \tag{23}$$

Equalities (23) show that all the exponents β must be even.

Thus we reach the conclusion that, *if a natural number n is the norm of a complex integer, then in the factorization of n into primes the primes of the form $4k+3$ have even exponents.*

[1] Here p_n does not denote the nth prime.

Further, equalities (23) give

$$\lambda = \alpha, \qquad \mu_1 = \tfrac{1}{2}\beta_1, \qquad \mu_2 = \tfrac{1}{2}\beta_2, \qquad \ldots, \qquad \mu_l = \tfrac{1}{2}\beta_l.$$

Thus the exponents $\lambda, \mu_1, \mu_2, \ldots, \mu_l$ are uniquely defined.

In order to establish the exponents λ_j and λ_j', where $j = 1, 2, \ldots, k$, we use another rule which can be deduced as follows.

Let k_j be the greatest exponent for which $p_j^{k_j} \mid z$, i.e. let k_j be the greatest exponent for which $p_j^{k_j}$ divides both a and b, where $z = a+bi$. Then

$$(24) \qquad \left.\begin{aligned} \lambda_j &= a_j - k_j \\ \lambda_j' &= k_j \end{aligned}\right\} \text{if } p_j^{k_j}\pi_j \mid z, \qquad \left.\begin{aligned} \lambda_j' &= a_j - k_j \\ \lambda_j &= k_j \end{aligned}\right\} \text{if } p_j^{k_j}\pi_j \nmid z.$$

In fact, it follows from the definition of the exponent k_j that the complex integer $z/p_j^{k_j}$ cannot be divisible by π_j and π_j' simultaneously, because, if it could, then, since $(\pi_j, \pi_j') = 1$, it would be divisible by $\pi_j\pi_j' = p_j$, whence $p_j^{k_j+1} \mid z$, contrary to the definition of k_j.

Consequently if $\pi_j \mid (z/p_j^{k_j})$, then the number $z/p_j^{k_j}$ is not divisible by π_j'. Hence, in view of $p_j^{k_j} = \pi_j^{k_j}\pi_j'^{k_j}$, it follows by (22) that $\lambda_j' = k_j$, whence, by (23), $\lambda_j = a_j - k_j$. If the number $z/p_j^{k_j}$ is not divisible by π_j, then, as one easily sees, $\lambda_j = k_j$ and $\lambda_j' = a_j - k_j$.

This completes the proof of the rule provided by (24).

Finally, the exponent ν is easily found by a simple division of z by the product of the prime factors whose exponents have already been defined.

EXAMPLES. **1.** Let $z = 22+7i$. We then have

$$N(z) = 484+49 = 533 = 13\cdot 41, \qquad p_1 = 13 = 2^2+3^2, \qquad p_2 = 41 = 4^2+5^2.$$

Consequently,

$$z = i^{\nu}\pi_1^{\lambda_1}\pi_1'^{\lambda_1'}\pi_2^{\lambda_2}\pi_2'^{\lambda_2'},$$

where $\pi_1 = 2+3i$, $\pi_1' = 2-3i$, $\pi_2 = 4+5i$, $\pi_2' = 4-5i$. Clearly, $k_1 = k_2 = 0$. The number

$$z/\pi_1 = (22+7i)/(2+3i) = (22+7i)(2-3i)/13 = 5-4i$$

is a complex integer, and so $\lambda_1 = a_1 - 0 = 1$, $\lambda_1 = 0$. Similarly, the quotient z/π_2 could be calculated, but it is sufficient to note that the number $5-4i$ is a prime complex integer. Hence immediately,

$$22+7i = (2+3i)(5-4i)$$

is the required factorization.

2. Let $z = 19+17i$. We then have

$$N(z) = 361+289 = 650 = 2\cdot 5^2\cdot 13 = 2\cdot p_1^2\cdot p_2.$$

Consequently,

$$z = i^{\nu}(1+i)\pi_1^{\lambda_1}\pi_1'^{\lambda_1'}\pi_2^{\lambda_2}\pi_2'^{\lambda_2'},$$

where $\pi_1 = 1+2i$, $\pi_1' = 1-2i$, $\pi_2 = 2+3i$, $\pi_2' = 2-3i$, $a_1 = 2$, $a_2 = 1$.

Since neither $5 \mid z$ nor $13 \mid z$, we have $k_1 = k_2 = 0$. Therefore the number $(19+17i)/(1+2i)$ is not a complex integer, and so $\lambda_1 = 0$ and $\lambda_1' = 2$. The number $(19+17i)/(2+3i)$ is not a complex integer either. Therefore $\lambda_2 = 0$ and $\lambda_2' = 1$. We then have

$$z = i^{\nu}(1+i)(1-2i)^2(2-3i),$$

where a simple division shows that $\nu = 2$. Therefore the required factorization is

$$19+17i = (1+i)(1-2i)^2(-2+3i).$$

3. Let $z = 10+100i$. We may write $z = 10(1+10i)$ and since

$$10 = 2\cdot 5 = -i(1+i)^2(1+2i)(1-2i),$$

it is sufficient to find the factorization of $1+10i$. We have $N(1+10i) = 101$. This is a prime of the form $4k+1$. Hence, by theorem 7, $1+10i$ is a prime complex integer. Therefore

$$10+100i = -i(1+i)^2(1+2i)(1-2i)(1+10i).$$

EXERCISE. Find the factorization into prime complex integers of the complex integers: $1+7i$, $9+i$, $7+9i$, $107+198i$, $10+i$, $7+24i$.

Answer. $1+7i = -i(1+i)(1+2i)^2$, $9+i = -i(1+i)(4+5i)$, $7+9i = (1+i)(1+2i)(3-2i)$, $107+198i = -(1+6i)^3$, $10+i = 10+i$, $7+24i = -(1+2i)^4$.

§ 6. The number of complex integers with a given norm. Now we are going to investigate the question how many there are complex integers with norms equal to a given natural number n.

The question is important not only in itself; another source of its applicability lies in the fact that it is equivalent to the problem of finding the number of the pairs of rational integers x, y for which $x^2+y^2 = n$. In other words, the number $\tau(n)$ of complex integers with norms equal to n is equal to the number of representations of the number n as the sum of the squares of two rational integers. Therefore the function $\tau(n)$ appears to be the same as has already been investigated in Chapter XI, § 2.

Let (20) be the factorization of the number n into primes and let (21) be its factorization into prime complex integers. As we have already shown (cf. § 5), $N(z) = n$ holds only in the case where the exponents β_j, $j = 1, 2, \ldots, l$ are even. Suppose that this condition is satisfied. Then, as we have learned, a number z with the norm n has a factorization into complex primes as in (22), equalities (23) for the exponents being satisfied, and ν is one of the numbers 1, 2, 3, 4. Conversely, if $\lambda, \lambda_1, \lambda_1', \lambda_2, \lambda_2' \ldots, \lambda_k, \lambda_k', \mu_1, \mu_2, \ldots, \mu_l$ is an arbitrary system of non-negative integers which satisfy equalities (23) and ν is one of the numbers $1, 2, 3, 4$, then the number z, uniquely defined by (22), has the norm n. Thus, since the numbers $\lambda, \mu_1, \mu_2, \ldots, \mu_i$ are uniquely defined by conditions (23) the question about the number of different complex integers whose norms are equal to n is equivalent to the question about the number of different systems of non-negative ν, λ_1, λ_1', λ_2, λ_2', $\ldots$, λ_k, λ_k' that satisfy the conditions

$$1 \leqslant \nu \leqslant 4, \qquad \lambda_1+\lambda_1' = a_1, \qquad \lambda_2+\lambda_2' = a_2, \qquad \ldots, \qquad \lambda_k+\lambda_k' = a_k.$$

There are four possible values for the number ν: $1, 2, 3, 4$. For λ_1, λ_1' we have the following a_1+1 possibilities: $0, a_1$; $1, a_1-1$; $2, a_1-2$; $\ldots$; $a_1, 0$. Similarly, there are a_2+1 possible values for λ_2, λ_2' and so on. This shows that

$$(25) \qquad \tau(n) = 4(a_1+1)(a_2+1)\ldots(a_k+1).$$

This formula has been obtained under the assumption that the exponents on the primes of the form $4t+3$ in the factorization of n into primes are all even. Otherwise, the equation $N(z) = n$ is not solvable in complex integers z, and so $\tau(n) = 0$. Thus we have proved the following

THEOREM 8. *If a natural number n is factorized into prime factors as in* (20), *then the number $\tau(n)$ of the representations of n as the sum of the squares of two rational integers is equal to $4(a_1+1)(a_2+1)\ldots(a_k+1)$ provided the exponents on the primes of the form $4t+3$ that appear in the factorization are even. Otherwise $\tau(n) = 0$.*

The theorem obtained in Chapter XI, § 1, in a different way is an immediate consequence of theorem 8.

In particular, if n is a prime of the form $4t+1$, then $\tau(n) = 8$, whence, immediately, theorem 9 of Chapter V follows.

Now let $f(h)$ be a function defined as follows:

$$(26) \qquad f(h) = \begin{cases} 0 & \text{if} \quad h \text{ is even,} \\ +1 & \text{if} \quad h \text{ is of the form } 4t+1, \\ -1 & \text{if} \quad h \text{ is of the form } 4t+3. \end{cases}$$

It is easy to see that for any rational integers a, b

$$f(ab) = f(a)f(b).$$

Hence, if

$$n = h_1^{a_1}h_2^{a_2}\ldots h_k^{a_k}$$

is the factorization of n into prime factors, then, as is easy to see,

$$\sum_{d|n} f(d) = \big(f(1)+f(h_1)+f(h_1^2)+\ldots+f(h_1^{a_1})\big)\ldots\big(f(1)+f(h_k)+\ldots+f(h_k^{a_k})\big).$$

According to (26) we have

$$f(1) = f(1)+f(2)+f(2^2)+\ldots+f(2^a) = 1.$$

If $h = 4t+1$, then

$$f(1)+f(h)+f(h^2)+\ldots+f(h^a) = a+1.$$

If $h = 4t+3$, then

$$(27) \quad f(1)+f(h)+f(h^2)+\ldots+f(h^a) = 1-1+1-\ldots+(-1)^a = \frac{1+(-1)^a}{2}.$$

In virtue of the formula for $\sum_{d|n} f(d)$ we have

$$\sum_{d|n} f(d) = (a_1+1)(a_2+1)\ldots(a_k+1),$$

whence, by theorem 8,

$$(28) \qquad \tau(n) = 4\sum_{d|n} f(d),$$

provided all prime factors of n of the form $4t+3$ have even exponents in the factorization of n into primes. Otherwise, by (27),

$$\sum_{d|n} f(d) = 0,$$

which, by theorem 8, shows that equality (28) is valid. Consequently it is valid for any n. This can be formulated in the following *theorem of Jacobi.*

THEOREM 9. *The number of representations of a natural number n as the sum of the squares of two rational integers is equal to the difference between the number of the prime divisors of the form $4t+1$ of n and the number of divisors of the form $4t+3$ of n, multiplied by four.*

In fact, in (28) the summand $+1$ appears as many times as there are prime divisors of the form $4t+1$ of number n; the summand -1 appears as many times as there are prime divisors of the form $4t+3$ of number n.

By (28) we obtain

$$(29) \qquad \frac{1}{4}\sum_{n=1}^{[x]} \tau(n) = \sum_{k=1}^{[x]} f(k)\left[\frac{x}{k}\right].$$

Since the summands $f(d)$ appear in the sum $\sum_{n=1}^{[x]}\sum_{d|n} f(d)$ as many times as there are numbers $n \leqslant s$ for which $d \mid n$, i.e. $\left[\dfrac{x}{d}\right]$ times.

In virtue of formula (6) of Chapter XI, § 2, we have

$$\frac{1}{4}\sum_{n=1}^{[x]}\tau(n) = \sum_{k=0}^{[\sqrt{x}]}[\sqrt{x-k^2}],$$

whence

$$\sum_{k=0}^{[\sqrt{x}]}[\sqrt{x-k^2}] = \sum_{k=1}^{[\sqrt{x}]}f(k)\left[\frac{x}{k}\right], \tag{30}$$

and so

$$[\sqrt{x}]+[\sqrt{x-1^2}]+[\sqrt{x-2^2}]+\ldots = \left[\frac{x}{1}\right]-\left[\frac{x}{3}\right]+\left[\frac{x}{5}\right]-\left[\frac{x}{7}\right]+\ldots,$$

where the sequence of summands on the left-hand side breaks up at the last positive term under the sign of square root, and that on the right-hand side breaks up at the last fraction for which the numerator is not less than the denominator.

This is known under the name of *Liouville's identity.*

In particular, for $x = 10$, we have

$$[\sqrt{10}]+[\sqrt{9}]+[\sqrt{6}]+[\sqrt{1}] = [\tfrac{10}{1}]-[\tfrac{10}{3}]+[\tfrac{10}{5}]-[\tfrac{10}{7}]+[\tfrac{10}{9}],$$

whence, indeed, $3+3+2+1 = 10-3+2-1+1$.

Liouville's identity implies Jacobi's theorem the other way round.

It is worth-while to mention that, by inequalites of Chapter XI, § 2, Liouville's identity implies Leibniz's expansion of the number π:

$$\frac{\pi}{4} = \frac{1}{1}-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\ldots$$

in an elementary way.

What is astonishing in this expansion is the rôle of the consecutive odd numbers that appear in the denominators of the summands of the expansion. The ancients used to say "Numero impari deus gaudet". In a purely arithmetical way we have obtained a formula for the most important geometric constant: the ratio of the circumference of a circle to its diameter; the formula which is simply a series of reciprocals of the consecutive odd natural numbers equipped with alternating signs.

Another formula for π built up of the consecutive odd numbers is that due to Euler,

$$\frac{\pi^2}{8} = \frac{1}{1^2}+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\frac{1}{9^2}+\ldots$$

This formula can also be obtained in an elementary way. Of the other formulae for the number π that are proved in analysis we mention here the following:

Wallis's formula

$$\frac{\pi}{4} = \left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{5^2}\right)\left(1-\frac{1}{7^2}\right)\left(1-\frac{1}{9^2}\right)\ldots,$$

Euler's formula

$$\frac{\pi^3}{32} = \frac{1}{1^3}-\frac{1}{3^3}+\frac{1}{5^3}-\frac{1}{7^3}+\frac{1}{9^3}-\ldots,$$

and the *formula of Brouncker*

$$\frac{4}{\pi} = 1+\frac{1^2|}{|2}+\frac{3^2|}{|2}+\frac{5^2|}{|2}+\frac{7^2|}{|2}+\frac{9^2|}{|2}+\ldots$$

§ 7. Jacobi's four-square theorem. Now we are going to prove a theorem of Jacobi that concerns the representations of a number as the sum of four squares.

At first we consider the case where the natural number n is of the form $n = 4u$. Let

$$4u = x^2+y^2+z^2+t^2 \tag{31}$$

be a representation of $4u$ as the sum of four odd squares.

It is clear, that, since x, y, z, t are odd,

$$x^2+y^2 = 2u' \quad \text{and} \quad z^2+t^2 = 2u'', \tag{32}$$

where u' and u'' are odd natural numbers. In view of (31) and (32) we have

$$2u = u'+u''. \tag{33}$$

On the other hand, if w is an odd number and $2w = a^2+b^2$, then the numbers a, b are odd. The reason is that if a, b were both even, then $2w$ would be divisible by 4, contrary to the assumption that w is odd. If one of the numbers a, b were odd, the other being even, then the number $2w$ would be odd, which is clearly false.

Thus we see that, in order to find all the representations of the number $4u$ as the sum of four odd squares, it is sufficient to find all possible representations of $2u$ as sums of two odd numbers u' and u'', and then to find the representations of either of the numbers u', u'' as the sum of two squares.

Denote by $\theta(4u)$ the number of all possible representations of the number $4u$ as the sum of four odd squares.

For any pair of two fixed odd numbers u' and u'' that satisfy equality (33), by (28) and the equality $\tau(2m) = \tau(m)$, $m = 1, 2, \ldots$, which follows from (25), the number of all corresponding representations of the number $4u$ as the sum of four squares of odd numbers is

$$\tau(2u')\tau(2u'') = 16\sum_{d'|u'} f(d')\sum_{d''|u''} f(d'').$$

Hence, the total number of such representations is

$$\theta(4u) = 16\sum_{u'+u''=2u}\Big(\sum_{d'|u'} f(d')\cdot\sum_{d''|u'} f(d'')\Big), \tag{34}$$

where the summation in the first sum extends all over the pairs u', u, of natural numbers that satisfy (33). Since any divisor of an odd number is odd, by (26), we have

$$\sum_{d'|u'} f(d') = \sum_{d'|u'} (-1)^{\frac{1}{2}(d'-1)}$$

and similarly

$$\sum_{d''|u''} f(d'') = \sum_{d''|u''} (-1)^{\frac{1}{2}(d''-1)}$$

This applied to (34) gives

$$\theta(4u) = 16\sum_{u'+u''=2u}\Big(\sum_{d'|u'} (-1)^{\frac{1}{2}(d'-1)}\cdot\sum_{d''|u''} (-1)^{\frac{1}{2}(d''-1)}\Big). \tag{35}$$

The product of the sums in brackets can be expressed as the sum of products according to the rule

$$\sum_{m=1}^{p} a_m\sum_{n=1}^{q} b_n = (a_1+a_2+\ldots+a_p)(b_1+b_2+\ldots+b_q) = \sum_{m=1}^{p}\sum_{n=1}^{q} a_m b_n.$$

Thus (35) gives

$$\theta(4u) = 16\sum_{u'+u''=2u}\sum_{d'|u'}\sum_{d''|u''} (-1)^{\frac{1}{2}(d'-1)+\frac{1}{2}(d''-1)} \tag{36}$$

In virtue of the identity

$$\tfrac{1}{2}(d'-1)+\tfrac{1}{2}(d''-1) = \tfrac{1}{2}(d'-d'')+d''-1$$

and since d'' as a divisor of an odd number is odd, we have

$$(-1)^{\frac{1}{2}(d'-1)+\frac{1}{2}(d''-1)} = (-1)^{\frac{1}{2}(d'-d'')}$$

Thus (36) turns into

$$\theta(4u) = 16\sum_{u'+u''=2u}\sum_{d'|u'}\sum_{d''|u''} (-1)^{\frac{1}{2}(d'-d'')}. \tag{37}$$

For any pair of odd natural numbers u' and u'' that satisfy (33) and for any pair of divisors d' and d'', we denote the corresponding complementary divisors by δ', δ''. We then have

$$u' = d'\delta', \quad u'' = d''\delta''. \tag{38}$$

Accordingly, by (33), we have

$$2u = d'\delta'+d''\delta'', \tag{39}$$

where δ' and δ'' as divisors of odd numbers are odd. Consequently, to each summand of the sum (37) corresponds the unique system of four odd natural numbers

$$d', \quad d'', \quad \delta', \quad \delta', \tag{40}$$

which satisfy equality (39). It is clear that, conversely, since the first two of the indices d', d'', δ', δ'' that define the summand are given and the other two are defined by (38), the unique summand of the sum (37) corresponds to any system of natural numbers (40) which satisfy (39).

Therefore we may write

$$\theta(4u) = 16\sum_{d'\delta'+d''\delta''=2u} (-1)^{\frac{1}{2}(d'-d'')} \tag{41}$$

where the summation on the right-hand side extends all over the systems (40) consisting of four odd numbers that satisfy (39).

Now we divide the summands of (41) into two classes, the first consisting of the summands for which $d' = d''$ and the second of those for which $d' \neq d''$.

Given an odd natural number d, we are going to calculate the sum of the summands of (41) for which $d' = d'' = d$. As follows from (39), d is a divisor of the number $2u$ and, being odd, it must be a divisor of u. We then have $u = d\delta$, whence by (39)

$$2\delta = \delta'+\delta''.$$

This shows that the number of the summands of (41) for which $d' = d'' = d$ is equal to the number of representations of 2δ as the sum of two natural numbers, this being equal to δ. But since any such summand is equal to $+1$, the sum of the summands is equal to $\delta = u/d$.

From this we infer that the sum of the summands that belong to the first class is

$$\sum_{d|u}\frac{u}{d} = \sum_{d|u} d = \sigma(u).$$

The summands that belong to the second class are again divided into two groups, the first consisting of the summands for which $d' > d''$, the second of those for which $d'' > d'$. To each summand defined by a system of the first group corresponds the unique summand of the second group defined by the system $d', d'', \delta', \delta''$ and *vice versa*. Therefore it is sufficient to calculate the sum of the summands that belong to the first group and multiply it by 2.

Let

$$\vartheta = \left[\frac{d''}{d'-d''}\right]. \tag{42}$$

To any summand of the first group defined by system (40) corresponds a summand defined by the system

$$d_1,\quad d_2,\quad \delta_1,\quad \delta_2, \tag{43}$$

where

$$\begin{aligned} d_1 &= \delta'+(\vartheta+1)(\delta'+\delta''), & d_2 &= \delta'+\vartheta(\delta'+\delta''),\\ \delta_1 &= d''-\vartheta(d'-d''), & \delta_2 &= (\vartheta+1)(d'-d'')-d''. \end{aligned} \tag{44}$$

First of all we show that system (43) defined by formulae (44) indeed defines a summand of the first group. Since ϑ is an integer and the numbers of (40) are odd, the numbers $\delta'+\delta''$ and $d'-d''$ are even. Hence, by (44), we see that the numbers of (43) are odd integers.

By (42), the number ϑ is non-negative since, for the summands of the first group, $d' > d''$. Consequently, by (44), the numbers d_1 and d_2 are positive. Moreover, by (42),

$$\frac{d''}{d'-d''}-1 < \vartheta \leqslant \frac{d''}{d'-d''},$$

which, multiplied by $d'-d'' > 0$, gives

$$d''-(d'-d'') < \vartheta(d'-d'') \leqslant d''.$$

This, by (44), shows that $\delta_1 \geqslant 0$ and $\delta_2 > 0$. But the number δ_1, being odd, cannot be equal to zero, consequently $\delta_1 > 0$.

Thus we see that the four numbers of (43) are odd and positive.

Further, by (44), we find

$$d_1-d_2 = \delta'+\delta''. \tag{45}$$

This shows that $d_1 > d_2$. Moreover,

$$\delta_1+\delta_2 = d'-d'', \tag{46}$$

whence, by (45) and the identity

$$d_1\delta_1+d_2\delta_2 = d_1(\delta_1+\delta_2)-(d_1-d_2)\delta_2,$$

we obtain

$$d_1\delta_1+d_2\delta_2 = d_1(d'-d'')-(\delta'+\delta'')\delta_2.$$

Hence, in virtue of (44), we have

$$d_1\delta_1+d_2\delta_2 = \delta'(d'-d'')+(\delta'+\delta'')d'',$$

which, by (39), gives

$$d_1\delta_1+d_2\delta_2 = 2u.$$

From this we conclude that system (43) indeed defines a summand of the first group.

System (43) is different from system (40). This is because of the fact that, if the two systems were identical, then by (45) we would have $d'-d'' = \delta'+\delta''$, whence, by (39)

$$2u = (d'-d'')\delta'+(\delta'+\delta'')d'' = (\delta'+\delta'')(\delta'+d'')$$

and so, since the numbers $\delta'+\delta''$ and $\delta'+d''$ are even, $2u$ would be divisible by 4, contrary to the assumption that u is odd.

To find the numbers (40) we solve the equations (44), whence, by (45) and (46) we obtain

$$\delta' = d_1-(\vartheta+1)(d_1-d_2) = d_2-\vartheta(d_1-d_2), \qquad d'' = \delta_1+\vartheta(\delta_1+\delta_2).$$

Hence, by (45) and (46),

$$\begin{aligned} \delta'' &= d_1-d_2-\delta' = (\vartheta+1)(d_1-d_2)-d_2,\\ d' &= \delta_1+\delta_2+d'' = \delta_1+(\vartheta+1)(\delta_1+\delta_2). \end{aligned}$$

In virtue of formulae (44) and (42) we obtain

$$\vartheta_1 = \left[\frac{d_2}{d_1-d_2}\right] = \left[\frac{\delta'+\vartheta(\delta'+\delta'')}{\delta'+\delta''}\right] = \left[\frac{\delta'}{\delta'+\delta''}+\vartheta\right] = \vartheta \tag{47}$$

because ϑ is an integer and $\delta'/(\delta'+\delta'')$ is a proper fraction. Thus, finally, we obtain

$$\begin{aligned} d' &= \delta_1+(\vartheta_1+1)(\delta_1+\delta_2), & d'' &= \delta_1+\vartheta_1(\delta_1+\delta_2),\\ \delta' &= d_2-\vartheta_1(d_1-d_2), & \delta'' &= (\vartheta_1+1)(d_1-d_2)-d_2. \end{aligned} \tag{48}$$

Comparing formulae (47) and (48) with formulae (42) and (44) we come to the conclusion that systems (43) and (40) correspond to each other with respect to the correspondence defined above. In other words, the correspondence we have defined orders the summands of the first group in pairs in such a way that each pair consists of two summands, one defined by system (40) and the other by (43), linked together by formulae (44).

Let us calculate the sum of the summands that belong to the same pair, i.e. the sum

$$(-1)^{(d'-d'')/2}+(-1)^{(d_1-d_2)/2}, \tag{49}$$

where d', d'', d_1 and d_2 are linked together by formulae (44).

In virtue of (39) and (45) we have $2u = (d'-d'')\delta'+(d_1-d_2)d''$, and so

$$\frac{d'-d''}{2}\delta'+\frac{d_1-d_2}{2}d'' = u.$$

Hence, since the numbers δ', d'' and u are odd,

$$\frac{d'-d''}{2}+\frac{d_1-d_2}{2} \equiv 1 (\mathrm{mod}\, 2).$$

This proves that sum (49) is equal to zero. In other words, this means that the summands that belong to the same pair cancel each other.

Thus the sum of the summands of the first group, and consequently the total sum of the summands of the second class in the first partition into two classes is zero. As we have already proved, the sum of the summands of the first class is equal to $\sigma(u)$; therefore, by (41), we obtain

THEOREM 10. *If u is an odd natural number, then*

$$\theta(4u) = 16\sigma(u).$$

This theorem was first formulated (in a slightly different way) and proved by Jacobi [1]. The proof we have presented here, simpler than the original one of Jacobi, is due to Dirichlet [1] (cf. also Bachmann [2], pp. 349-354).

Now let

$$u = \xi^2+\eta^2+\zeta^2+\vartheta^2 \tag{50}$$

be a representation of an odd natural number u as the sum of four squares and let

$$\begin{aligned} x' &= \xi+\eta+\zeta+\vartheta, & y' &= \xi+\eta-\zeta-\vartheta,\\ z' &= \xi-\eta+\zeta-\vartheta, & t' &= \xi-\eta-\zeta+\vartheta. \end{aligned} \tag{51}$$

Since, clearly, $w^2 \equiv w (\mathrm{mod}\, 2)$ for any integer w, by (50), $x' \equiv u (\mathrm{mod}\, 2)$, which in view of the fact that u is odd proves that x' is odd. Further, since formulae (50) imply that

$$y' = x'-2(\xi+\vartheta), \quad z' = x'-2(\eta+\vartheta), \quad t' = x'-2(\eta+\zeta),$$

all the four numbers x', y', z', t' are odd. In virtue of (50) and (51) we can easily verify that

$$x'^2+y'^2+z'^2+t'^2 = 4u.$$

Therefore the system

$$x',\ y',\ z',\ t' \tag{52}$$

defined by (50) gives a representation of the number $4u$ as the sum of four odd squares.

On the other hand, let

$$\begin{aligned} x'' &= -\xi+\eta+\zeta+\vartheta, & y'' &= \xi-\eta+\zeta+\vartheta,\\ z'' &= \xi+\eta-\zeta+\vartheta, & t'' &= \xi+\eta+\zeta-\vartheta. \end{aligned} \tag{53}$$

Here also the numbers

$$x'', y'', z'', t'' \tag{54}$$

are all odd and, again,

$$x''^2+y''^2+z''^2+t''^2 = 4u.$$

It can be verified that systems (52) and (54) are different. This is because, by (51) and (53), we find

$$x'+y'+z'+t' = 4\xi, \quad x''+y''+z''+t'' = 2(\xi+\eta+\zeta+\vartheta) \tag{55}$$

and so, since $\xi+\eta+\zeta+\vartheta$ is odd, the sum of the numbers (52) is divisible by 4 while the sum of the numbers (54) is not.

In virtue of (51) and (53) to any representation of an odd number u as the sum of four squares correspond two different representations of the number $4u$ as the sum of four odd squares.

We now prove that any representation (31) of the number $4u$ as the sum of four odd squares corresponds the unique representation of the number u as the sum of four squares.

In fact, the number

$$s = x+y+z+t,$$

being the sum of four odd numbers of (31), is even. We consider two cases:

(i) $s \equiv 0 (\mathrm{mod}\, 4)$. Formulae (53) imply (55), consequently there are no integers ξ, η, ζ, ϑ which satisfy (50) and are such that numbers x'', y'', z'', t'' defined by them are equal to x, y, z, t, respectively; this is because the existence of such integers would imply that s is divisible by 4, contrary to the assumption. On the other hand, there exists precisely one system of integers ξ, η, ζ, ϑ which satisfy (50) and for which

$$\begin{aligned} x &= \xi+\eta+\zeta+\vartheta, & y &= \xi+\eta-\zeta-\vartheta,\\ z &= \xi-\eta+\zeta-\vartheta, & t &= \xi-\eta+\zeta-\vartheta \end{aligned} \tag{56}$$

because the validity of (56) implies the validity of

$$\begin{aligned} \frac{x+y+z+t}{4} &= \xi, & \frac{x+y-z-t}{4} &= \eta,\\ \frac{x-y+z-t}{4} &= \zeta, & \frac{x-y-z+t}{4} &= \vartheta, \end{aligned} \tag{57}$$

and this proves that the system x, y, z, t corresponds to at most one system $\xi, \eta, \zeta, \vartheta$ for which formulae (57) hold. If we calculate the numbers ξ, η, ζ, ϑ from formulae (57), we see that, in the case under consideration, the numbers obtained are integers which satisfy (56) and, by (31), they must satisfy (50), which proves that the system x, y, t, z corresponds to at least one such system.

Thus in case (i) there is a one-to-one correspondence between representations (31) and representations (50) of u as sums of four squares.

(ii) $s \equiv 2 (\mathrm{mod}\, 4)$. In this case, since formulae (51) imply formulae (55), there are no integers ξ, η, ζ, ϑ for which formulae (51) give a system

$$x' = x, \quad y' = y, \quad z' = z, \quad t' = t,$$

because otherwise the sum s would be divisible by 4, contrary to the assumption. On the other hand, there exists a unique system of integers ξ, η, ζ, ϑ which satisfy (50) and are such that formula

$$\begin{aligned} x &= -\xi+\eta+\zeta+\vartheta, & y &= \xi-\eta+\zeta+\vartheta, \\ z &= \xi+\eta-\zeta+\vartheta, & t &= \xi+\eta+\zeta-\vartheta \end{aligned} \tag{58}$$

is valid because the validity of (58) imply the validity of

$$\begin{aligned} \frac{-x+y+z+t}{4} &= \xi, & \frac{x-y+z+t}{4} &= \eta, \\ \frac{x+y-z+t}{4} &= \zeta, & \frac{x+y+z-t}{4} &= \vartheta. \end{aligned} \tag{59}$$

This proves that the system x, y, z, t corresponds to at most one system ξ, η, ζ, ϑ for which formulae (59) hold. If the numbers ξ, η, ζ, ϑ are calculated from formulae (59), we see that, in the case under consideration, they must be integers which satisfy (58). By (31), (58) implies that to the system x, y, z, t corresponds at least one such system ξ, η, ζ, ϑ.

Therefore, in case (ii), there is a one-to-one correspondence between representations (31) and representations (50) of the number u as sums of four squares.

In virtue of what we have proved above, the number of the representations of $4u$ as the sum of four odd squares is twice as large as the number $\tau_4(u)$ of representations of the (odd) number u as the sum of four squares.

Hence, by theorem 10, we obtain the validity of the formulae

$$\tau_4(u) = 8\sigma(u) \tag{60}$$

for any odd natural number u. Thus we have

THEOREM 11. *The number of representations of an odd number as the sum of four squares is equal to the sum of its divisors multiplied by* 8.

Since the number of divisors of an odd number >1 is at least 4, by theorem 11 we see that any odd natural number >1 has at least 32 representations as the sum of four squares. Since any odd square has precisely 8 representations as the sum of four squares three of which are equal to zero, we conclude that any odd square greater than 1 is a sum of four squares at least, two of them different from zero. Hence, by Lagrange's theorem, the following corollary is obtained

COROLLARY. *Any natural number greater than* 1 *is a sum of four squares at least two of which are different from zero.*

Now, we are going to calculate the number of representations of the number $4u$ (where u is odd) as the sum of four squares.

Let

$$4u = x^2+y^2+z^2+t^2 \tag{61}$$

be such a representation.

If one of the numbers x, y, z, t were even, the remaining ones being odd, or if one were odd, the remaining ones being even, then the sum of the squares of those numbers would be odd, contrary to (61).

If two of the numbers x, y, z, t were even, the other two being odd, then the sum of their squares would be of the form $4k+2$, contrary to formula (61).

Consequently, the numbers x, y, z, t must be all odd or all even.

The case where x, y, z, t are odd is fully described by theorem 10, which gives the number of representations of $4u$ as the sum of four odd squares. Thus it remains to calculate the number of representations of the number $4u$ as the sum of four even squares.

It is easy to see that to any such representation

$$4u = (2\xi)^2+(2\eta)^2+(2\zeta)^2+(2\vartheta)^2$$

corresponds a representation of u as the sum of four squares, namely

$$u = \xi^2+\eta^2+\zeta^2+\vartheta^2,$$

and *vice versa*. From this we infer that the number of representations of $4u$ as the sum of four even squares is equal to the number of representations of the number u as the sum of four squares, this, by (60) being equal to $8\sigma(u)$. Consequently, the total number of representations of the number $4u$ (where u is odd) as the sum of four squares is

$$16\sigma(u)+8\sigma(u) = 24\sigma(u).$$

Hence

$$\tau_4(4u) = 24\sigma(u) \tag{62}$$

for any odd u.

Finally we calculate the number of representations of the number $2u$ as the sum of four squares. We shall prove that

$$\tau_4(2u) = \tau_4(4u). \tag{63}$$

In fact, if (61) is a representation of the number $4u$ (where u is odd) as the sum of four squares, then, as we have already learned, the numbers x, y, z, t are either all even or all odd. In any case

$$\xi = \frac{x+y}{2}, \quad \eta = \frac{x-y}{2}, \quad \zeta = \frac{z+t}{2}, \quad \vartheta = \frac{z-t}{2} \tag{64}$$

are integers. We rewrite formula (61) in the form

$$2u = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2,$$

whence the representation

$$2u = \xi^2+\eta^2+\zeta^2+\vartheta^2 \tag{65}$$

is obtained.

Thus to any representation (61) of the number $4u$ as the sum of four squares corresponds a representation (65) of the number $2u$ as the sum of four squares. On the other hand, it is clear that to any representation (65) of the number $2u$ as the sum of four squares corresponds precisely one representation (61) of the number $4u$ as the sum of four squares. The proof easily follows from the fact that, under the assumption that a representation (65) corresponds to a representation (61) with respect to the correspondence defined above, formulae (64) hold. So we obtain

$$\xi+\eta = x, \quad \xi-\eta = y, \quad \zeta+\vartheta = z, \quad \zeta-\vartheta = t,$$

and this defines uniquely the representation (64). Thus a one-to-one correspondence between the representations of the number $4u$ as the sum of four squares and the representations of the number $2u$ as the sum of four squares is defined. Formula (63) is thus proved. Hence, by (62), we obtain

$$\tau_4(2u) = 24\sigma(u) \tag{66}$$

for any odd u.

Our present aim is to calculate the number of the representations of the number $2^h u$ ($h = 3, 4, \ldots$; u is odd) as the sum of four squares.

Let

$$2^h u = x^2+y^2+z^2+t^2 \tag{67}$$

be such a representation. The numbers x, y, z, t cannot all be even because, if they were, the right-hand side of (67) would be congruent to $4 \pmod 8$, while (since $h > 3$) the left-hand side is divisible by 8. Similarly, if two of the numbers were even, the other two being odd, then the right-hand side of (67) would be congruent to $2 \pmod 4$, which is impossible. From this we easily infer that all the numbers x, y, z, t must be even.

Let

$$x = 2\xi, \quad y = 2\eta, \quad z = 2\zeta, \quad t = 2\vartheta,$$

where $\xi, \eta, \zeta, \vartheta$ are integers. In virtue of (67) we have

$$2^{h-2}u = \xi^2+\eta^2+\zeta^2+\vartheta^2. \tag{68}$$

Thus we see that to any representation (67) of the number $2^h u$ as the sum of four squares corresponds a representation (68) of the number $2^{h-2}u$ as the sum of four squares. On the other hand, it is clear that to any representation (68) of $2^{h-2}u$ precisely one representation of the number $2^h u$ corresponds, namely the representation

$$2^h u = (2\xi)^2+(2\eta)^2+(2\zeta)^2+(2\vartheta)^2.$$

Hence

$$\tau_4(2^h u) = \tau_4(2^{h-2}u) \tag{69}$$

for any $h \geqslant 3$ and any odd natural number u.

Now, let s be any natural number and u an odd natural number. If $s = 1$ or $s = 2$, then by (66) or by (62) respectively we obtain

$$\tau_4(2^s u) = 24\sigma(u). \tag{70}$$

If $s > 2$, we consider two cases.

(i) $s = 2k$. Then, by (69), we may write

$$\tau_4(2^s u) = \tau_4(2^{2k}u) = \tau_4(2^{2k-2}u) = \tau_4(2^{2k-4}u) = \ldots = \tau_4(2^2 u)$$

which, for this case, proves (70).

(ii) $s = 2k+1$. By (69) we have

$$\tau_4(2^s u) = \tau_4(2^{2k+1}u) = \tau_4(2^{2k-1}u) = \ldots = \tau_4(2^3 u) = \tau_4(2u),$$

whence, by (66), formula (70) follows.

Thus we see that formula (70) is true for any natural number s and any odd natural number u.

Formulae (60) and (70) can be formulated in one theorem. Accordingly we suppose that n is an arbitrary natural number, and by $\sigma^*(n)$ we denote the sum of divisors of the natural number n which are not divisible by 4.

If $n = u$ is odd, then none of the divisors of n is divisible by 4, so

$$\sigma^*(n) = \sigma(n). \tag{71}$$

If n is even, we put $n = 2^s u$, where s is a natural number and u is an odd natural number. It is clear that any divisor of the number $2^s u$ which is not divisible by 4 is a divisor of the number $2u$ and, conversely, any divisor of the number $2u$ is a divisor of the number $2^s u$ which is not divisible by 4.

Consequently

$$\sigma^*(n) = \sigma^*(2^s u) = \sigma(2u),$$

whence, since $(2, u) = 1$ implies

$$\sigma(2u) = \sigma(2)\sigma(u) = 3\sigma(u),$$

we have

$$\sigma^*(n) = 3\sigma(u). \tag{72}$$

Formulae (71) and (72) combined with formulae (60) and (70) prove the validity of

$$\tau_4(n) = 8\sigma^*(n) \tag{73}$$

for any natural number n. Thus we have shown the following

THEOREM 12. *The number of representations of a natural number n as the sum of four squares is equal to the sum of divisors which are not divisible by 4 of n multiplied by 8.*

Since any natural number has at least one divisor which is not divisible by 4 (e.g. the number 1), then as an immediate consequence of theorem 12 we obtain the theorem stating that any natural number is a sum of four squares. This theorem was proved in Chapter XI in a different way.

An extensive list of references concerning the number of representations of number as the sum of any number of squares is given by R. A. Rankin [1].

EXAMPLES. In virtue of (70) we have

$$\tau_4(100) = 24\sigma(25) = 24\frac{5^3-1}{5-1} = 24.31 = 744.$$

So the number 100 has 744 representations as the sum of four squares.

Similarly

$$\tau_4(90) = 24\sigma(45) = 24\frac{3^3-1}{3-1}\cdot\frac{5^2-1}{5-1} = 24\cdot 13\cdot 6 = 1872.$$

This is the greatest number of representations as the sum of four squares for a number $\leqslant 100$.

In the same way we obtain

$$\tau_4(7) = 8\sigma(7) = 8\cdot 8 = 64, \qquad \tau_4(6) = 24\sigma(3) = 24\cdot 4 = 96,$$
$$\tau_4(96) = 24\sigma(3) = 24\cdot 4 = 96, \qquad \tau_4(1024) = \tau_4(2^{10}) = 24\sigma(1) = 24.$$

In virtue of (73) we easily obtain

$$\sum_{n=1}^{[x]} \tau_4(n) = 8S(x) - 32S\left(\frac{x}{4}\right),$$

where

$$S(x) = \sum_{k=1}^{[x]} k\left[\frac{x}{k}\right] = \frac{1}{2}\sum_{k=1}^{[x]}\left[\frac{x}{k}\left[\left[\frac{x}{k}\right]+1\right]\right].$$

From this we can easily deduce the inequality

$$\left|\sum_{n=1}^{[x]} \tau_4(n) - \frac{\pi^2 x^2}{2}\right| < 100x\sqrt{x},$$

valid for any integer x and obtain the formula of Euler

$$\frac{\pi^2}{6} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \ldots$$

in a purely arithmetical way.