

# On the Complex Prime Numbers Which Are to Be Considered in the Theory of Residues of the 5th, 8th, and 12th Powers

By C. G. J. Jacobi, Professor . . .

(Read in the Academy of Sciences on May 16, 1839)

translated from the German by Sky Shields

September 27, 2007

Gauss, in his investigations of biquadratic residues, introduced the complex numbers of the form  $a + b\sqrt{-1}$  as moduli or divisors. In so doing, he could present a law of reciprocity between the biquadratic characters of two complex prime numbers of the form  $a + b\sqrt{-1}$  of as much simplicity and perfection as accompanies the celebrated fundamental theorem of quadratic residues, which he called the jewel [*Kleinod*] of higher arithmetic. But however simple such an introduction of complex numbers as moduli may now seem, it belongs nonetheless to the most profound notions of science; indeed, I don't believe that arithmetic alone led the way to such concealed notions, but rather that it was derived from the study of elliptical transcendentals, and indeed the particular type that are given by the rectification of the arcs of the lemniscate. That is to say that in the theory of the multiplication and the division of the arcs of the lemniscate, the complex numbers of the form  $a + b\sqrt{-1}$  play exactly the same role as the usual numbers. Just as the trigonometric functions of the  $n$ -fold arc of the circle are represented through rational expressions, the arcs of the lemniscate can be multiplied with a complex number  $a + b\sqrt{-1}$  by means of rational formulas; just as the arcs of the circle can be divided into  $n$  parts through the solution of an equation of the  $n$ th degree, the arcs of the lemniscate can likewise be divided into  $a + b\sqrt{-1}$  by the solution of an equation of degree  $aa + bb$ . Just as a circular arc, if it is to be divided into 15 parts, must first be divided into 3 and 5 parts, while the division sought is found from both of these, so too, in order to divide an arc of the lemniscate into 17 parts, it must first be divided into  $1 + 4\sqrt{-1}$  and  $1 - 4\sqrt{-1}$  parts, and the division into 17 combined from the both of these. And so, in the investigation of that particular type of elliptical integral, if their nature is only even lightly fathomed, one is driven by necessity to introduce the number  $a + b\sqrt{-1}$  as a *divisor*. Even if that investigation of the integral calculus appears more complicated and more difficult than that simple notion of number theory, it is however not always the simple which first presents itself. *Gauss* assured, in the *Disquisitiones Arithmeticae*, that it were possible to apply his method for the division of the circle to the division of the entire lemniscate, and promised an *amplum opus* on this, in we he certainly did not [sicher noch nicht], according to [zufolge] his own later assertion, occupy himself with biquadratic residues. It is also not unlikely that he obtained the fundamental theorem of biquadratic residues from this source. *Abel* was the first to honor this promise of *Gauss*', by giving at least the main features of this extension of the Gaussian method of circle division to the division of the lemniscate in his first work on elliptical transcendentals, published in this present journal. It is likely as interesting a problem as it is difficult, to extract a geometric interpretation of the division of the arc of the lemniscate into  $a + b\sqrt{-1}$  parts, and the composition of the  $p$ th parts of the arc from its division into  $a + b\sqrt{-1}$  and  $a - b\sqrt{-1}$ . In recent times geometry has allotted a place within its domain to the imaginary numbers as well; it is to be expected that, with the remarkable impetus that geometry has received at the hands of *Steiner*, it will also make itself the master of these abstruse ideas.

It required no new notions to find the law of *cubic* reciprocity; for this it was only necessary to introduce as divisors, in an entirely analogous way, complex numbers of the form  $\frac{a + b\sqrt{-3}}{2}$ , or such that are composed from the cubic roots of unity. These investigations can also be related to the theory of a particular elliptical integral. The law of reciprocity for cubic residues, which I communicated in an

earlier notice, is even simpler than that presented by *Gauss* for the biquadratic residues, and is yielded quite directly from the known formulas of circle division.

Now that *Gauss* has dealt with the elements of complex numbers of the form  $a + b\sqrt{-1}$ , it remains to ascertain which among the methods and results of their arithmetic are also applicable for these complex numbers. So it is easily seen for example that the *Lagrange* method for the reduction of quadratic forms can also be extended to such expressions  $pyy + qyz + rzz$ , where  $p, q, r, y, z$  denote complex numbers of the given type. In order to take the simplest complex form,  $yy - \sqrt{-1} \cdot zz$ , it can be proven that every number  $a + b\sqrt{-1}$  which divides such a form must itself have the same form, and the proof is completely analogous to the proof of the known theorem that every number which divides the form  $yy + zz$  is also the sum of two squares. If  $p = aa + bb$  is a prime number of the form  $8n + 1$ , it proven immediately from the elements of the theory of these complex numbers that  $\sqrt{-1}$  is a quadratic residue of  $a + b\sqrt{-1}$ , or what is the same, that  $a + b\sqrt{-1}$  is a divisor of a form  $yy - \sqrt{-1} \cdot zz$ , and thus, by the theorem just mentioned, has the same form. If this form is broken down into the two factors  $y + \sqrt[4]{-1} \cdot z$  and  $y - \sqrt[4]{-1} \cdot z$ , and we set

$$y = y' + y''\sqrt{-1}, \quad z = z' + z''\sqrt{-1},$$

where  $y', y'', z', z''$  signify real whole numbers, then the decomposition of  $a + b\sqrt{-1}$  into two factors,

$$y' + y''\sqrt{-1} + \sqrt[4]{-1}[z' + z''\sqrt{-1}], y' + y''\sqrt{-1} - \sqrt[4]{-1}[z' + z''\sqrt{-1}],$$

is obtained. That is, a decomposition into two complex numbers which are composed of the 8th roots of unity. If  $\alpha$  is written for the 8th root of unity, or for  $\sqrt[4]{-1}$ , and

$$\Phi\alpha = y' + y''\alpha^2 + z'\alpha + z''\alpha^3,$$

then

$$a + b\sqrt{-1} = a + b\alpha^2 = \Phi\alpha \cdot \Phi\alpha^5$$

and, if  $\alpha^3$  is put in place of  $\alpha$ ,

$$a - b\sqrt{-1} = a - b\alpha^2 = \Phi\alpha^3 \cdot \Phi\alpha^7.$$

The prime number  $p = aa + bb$ , of the form  $8n + 1$ , is hence always the product of the four complex numbers

$$\Phi\alpha \cdot \Phi\alpha^3 \cdot \Phi\alpha^5 \cdot \Phi\alpha^7.$$

It is easily seen that the product  $\Phi\alpha \cdot \Phi\alpha^3$  receives the form  $c + d\sqrt{-2}$  and the product  $\Phi\alpha \cdot \Phi\alpha^7$  receives the form  $e + f\sqrt{2}$ . The three ways in which the four factors can be organized into two pairs therefore give the representations of the same prime numbers in the three forms  $a^2 + b^2, c^2 + 2d^2, e^2 + 2f^2$ , which are here derived from a common source, so that the six numbers  $a, b, c, d, e, f$  are expressed in a rational way through four other numbers  $y', y'', z', z''$ . This decomposition of prime numbers of the form  $8n + 1$  into four complex factors which are composed of eight roots of unity can also be derived through the usual methods of arithmetic. By exactly the same method it can also be proven that the prime numbers of the form  $12n + 1$  can be decomposed into four factors which are composed of the twelfth roots of unity; the three different ways in which these four factors can be ordered into two pairs give the representation of the prime number by the three forms  $a^2 + b^2, c^2 + 3d^2, e^2 + 3f^2$ . Prescriptions can easily be given for the discovery of this decomposition, according to which Herr Oberlehrer *Zornow* in Königsburg was kind enough to calculate for me the decomposition of the prime numbers of the form  $8n + 1$  and  $12n + 1$  up to 1000.

At the same time as I engaged in these considerations I directed my attention to certain properties of the complex numbers to which the theory of the division of the circle led. I remarked in the above-mentioned notice that if  $\lambda$  is a divisor of  $p - 1$ , the prime number  $p$  can be represented as the product of two complex numbers which are composed of the  $\lambda$ th roots of unity, and this as a rule in several different ways. It now happens—and this can be proven by the theory of the division of the circle itself—that several of these complex numbers can be multiplied with one another, and that the product can be again divided by another complex number of the same type, so that the quotient becomes likewise a whole complex number without it being seen how the complex numbers in the denominator cancel with

respect to those in the numerator. A close consideration of this remarkable circumstance leads me to the conviction that these complex factors of the prime number  $p$  must in general also themselves be composite, so that if they are resolved into the true *complex prime numbers*, the complex prime numbers which form the factors of the denominator can cancel individually with respect to the prime factors of the numerator. Since I had already arrived at these results in an entirely different fashion for  $\lambda = 8$  and  $\lambda = 12$ , I undertook the somewhat laborious attempt with  $\lambda = 5$ , and in fact attained it for the prime numbers of the form  $5n + 1$  with which I undertook the attempt to decompose each of their two factors, composed of the 5th roots of unity, again into two whole factors of the same type; whereupon it was then not difficult to find a general proof for this decomposability. Therefore the prime numbers of the form  $5n + 1$ ,  $8n + 1$ ,  $12n + 1$  can thus be represented as the product of four complex whole numbers which are composed of the 5th, 8th, and 12th roots of unity respectively. It becomes clear moreover that for the prime numbers of the form  $5n + 1$ , their representation in the form  $a^2 - 5b^2$  is obtained through another pairwise combination of the four factors.

The new factors are necessarily prime numbers. That is, if  $f\alpha$  is one of these, where  $\alpha$  is for the three types of prime number a primitive 5th, 8th, or 12th root of unity respectively, then  $f\alpha$  can not be represented as a product of two complex whole numbers of the same type  $\Phi\alpha$  and  $\Psi\alpha$  if one of them is not so composed that the product of their four values is not equal to unity. Since it is easily seen that the product of the four values of  $f\alpha$ ,  $\Phi\alpha$ ,  $\Psi\alpha$ , is a real number, and since the product of the four values of  $f\alpha$  is a prime number, both of the other products cannot give real numbers which are both simultaneously different from unity, since their product becomes equal to the prime number.

Between these prime numbers  $f\alpha$  the laws of reciprocity of the 5th, 8th, and 12th powers must be sought, and it would perhaps be feasible to find them through pure induction, according as [*nachdem*] their true form is recognized, if such an induction were not exceedingly cumbersome. If the reciprocity law is extended to compound numbers, entirely similar to what I did in the notice communicated earlier to the academy in connection with the quadratic, cubic, and biquadratic residues, then the simple reciprocity laws for the particular case for the residues of the 5th, 8th, and 12th powers, can be derived directly from the theory of the division of the circle if the number is real. The determination whether it will be possible to derive the more general theorems for every two complex numbers from the same source by means of modern artifices [*Kunstgriffe*] must be reserved for later investigations.