Summation of Certain Special Series

Art 1.

Among the more remarkable truths to which the theory of the division of the circle has opened access, the summation proposed in *Disquisitiones Arithmeticae* Art. 356 claims not the last place for itself, not only because of its particular elegance and wonderful fecundity, which will be explained more fully on another occasion, but also because its rigorous demonstration is not burdened by uncommon difficulties. Of course, this should have been expected, since the difficulties do not fall so much into the theorem itself, but rather into a limitation of the theorem, which was then ignored, but whose demonstration are immediately available and easily derived from the theory explained in the present work.

The theorem is presented there in the following form. Supposing n to be a prime number, let the indefinite variable a denote all the non-residues lying between 1 and $n-1$ (inclusive), and similarly let b denote the non-residues lying between the same limits. Let ω denote the arc $\frac{360^o}{n}$, and let k denote a definite integer not divisible by m. Then

I. for values of n which are of the form $4m+1$,

$$\begin{aligned}\sum \cos ak\omega &= -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n}\\ \sum \cos bk\omega &= -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n}, \text{ and thus}\\ \sum \cos ak\omega - \sum \cos bk\omega &= \pm\sqrt{n}\\ \sum \sin ak\omega &= 0\\ \sum \sin bk\omega &= 0\end{aligned}$$

II. for values of n which are of the form $4m+3$,

$$\begin{aligned}\sum \cos ak\omega &= -\tfrac{1}{2}\\ \sum \cos bk\omega &= -\tfrac{1}{2}\\ \sum \sin ak\omega &= \pm\tfrac{1}{2}\sqrt{n}\\ \sum \sin bk\omega &= \mp\tfrac{1}{2}\sqrt{n}\\ \sum \sin ak\omega - \sum \sin bk\omega &= \pm\sqrt{n}\end{aligned}$$

These summations have been demonstrated with all rigor, and no other difficulty remains here except in the determination of the sign of the radical quantity. Indeed, it can be shown with no difficulty that this sign depends only on the number k, that the same sign must hold for all values of k which are quadratic residues modulo n, and that the opposite sign must hold for all values of k which are quadratic non-residues modulo n. From this point the whole discussion will be focused on the case $k=1$, and it is clear that as soon as the correct sign is identified in this case, the signs for all other values of k will be immediately available. For it is in this very question, which at first sight seems to be regarded as one of the easier ones, that we have run into unexpected difficulties, and the method by which we have progressed thus far, without hindrance, now completely denies us further assistance.

Art. 2

It would not be out of place, before we proceed further, to illustrate some examples of our summations by numerical calculation. However, it will be convenient to preface this with some general observations.

I. In the case where n is a prime number of the form $4m+1$, denote by an indefinite variable a' all of the quadratic residues of n between 1 and $\frac{1}{2}(n-1)$ (inclusive), and denote by b' all of the quadratic non-residues within the same limits. It is clear that all $n-a'$ will be included within a, and all $n-b'$ within b. Therefore, since all a', b', $n-a'$, $n-b'$ will obviously complete the entire complex of numbers $1, 2, 3, \ldots, n-1$, they will also include all of b. Hence

$$\begin{aligned} \sum \cos ak\omega &= \sum \cos a'k\omega + \sum \cos(n-a')k\omega \\ \sum \cos bk\omega &= \sum \cos b'k\omega + \sum \cos(n-b')k\omega \\ \sum \sin ak\omega &= \sum \sin a'k\omega + \sum \sin(n-a')k\omega \\ \sum \sin ak\omega &= \sum \sin b'k\omega + \sum \sin(n-b')k\omega \end{aligned}$$

Now, considering that one always has $\cos(n-a')k\omega = \cos a'k\omega$, $\cos(n-b')k\omega = \cos b'k\omega$, $\sin(n-a')k\omega = -\sin a'k\omega$, and $\sin(n-b')k\omega = -\sin b'k\omega$, it comes out automatically that

$$\begin{aligned} \sum \sin ak\omega &= \sum \sin a'k\omega - \sum \sin a'k\omega = 0 \\ \sum \sin bk\omega &= \sum \sin b'k\omega - \sum \sin b'k\omega = 0, \end{aligned}$$

and also that the summation of cosines has the following form,

$$\begin{aligned} \sum \cos ak\omega &= 2\sum \cos a'k\omega \\ \sum \cos bk\omega &= 2\sum \cos b'k\omega, \end{aligned}$$

from which it follows that

$$\begin{aligned} 1 + 4\sum \cos a'k\omega &= \pm\sqrt{n} \\ 1 + 4\sum \cos b'k\omega &= \mp\sqrt{n} \\ 2\sum \cos a'k\omega - 2\sum \cos b'k\omega &= \pm\sqrt{n} \end{aligned}$$

II. In the case where n is of the form $4m-3$, the complement of any quadratic residue a modulo n will be a quadratic non-residue, and the complement of any quadratic residue b will be a quadratic non-residue. Therefore, all $n-a$ agree with b and all $n-b$ with a. From this one obtains

$$\sum \cos ak\omega = \sum \cos(n-b)k\omega = \sum \cos bk\omega,$$

and therefore, since all a and b together fill all the numbers 1, 2, 3, …, $n-1$, it follows that

$$\sum \cos ak\omega + \sum \cos bk\omega = \cos k\omega + \cos 2k\omega + \cos 3k\omega + \cdots + \cos(n-1)k\omega = -1$$

and the summations

$$\begin{aligned} \sum \cos ak\omega &= -\tfrac{1}{2} \\ \sum \cos bk\omega &= -\tfrac{1}{2} \end{aligned}$$

then arise automatically. Similarly,

$$\sum \sin ak\omega = \sum \sin(n-b)k\omega = -\sum \sin bk\omega$$

from which it is clear how the summations

$$\begin{aligned} 2\sum \sin ak\omega &= \pm\sqrt{n} \\ 2\sum \sin bk\omega &= \mp\sqrt{n} \end{aligned}$$

depend upon one other.

Art. 3

Now here are some examples of numerical calculations:

I. For $n = 5$ there is one value of a', namely $a' = 1$, and one value of b', namely $b' = 2$. One has

$$\cos\omega = +0,3090169944\ , \quad \cos 2\omega = -0,8090169944$$

and therefore

$$1 + 4\cos\omega = +\sqrt{5}\ , \ \ 1 + 4\cos 2\omega = -\sqrt{5}.$$

II. For $n = 13$, there are three values of a', namely 1, 3, and 4, and the same number of values for b', namely 2, 5, 6. From this we calculate

$$\begin{array}{lcl} \cos\omega & = & +\ 0,8854560257 \\ \cos 3\omega & = & +\ 0,1205366803 \\ \cos 4\omega & = & -\ 0,3546048870 \\ \hline \text{Sum} & = & +\ 0,6513878190 \end{array} \qquad \begin{array}{lcl} \cos 2\omega & = & +\ 0,5680647467 \\ \cos 3\omega & = & -\ 0,7485107482 \\ \cos 4\omega & = & -\ 0,9709418174 \\ \hline \text{Sum} & = & -\ 1,1513878189 \end{array}$$

Hence

$$1 + 4\sum\cos a'\omega = +\sqrt{13}\ , \quad 1 + 4\sum\cos b'\omega = -\sqrt{13}.$$

III. For $n = 17$ we have four values of a', namely 1, 2, 4, 8 and the same number of values of b', namely 3, 5, 6, 7. Thus the cosines are computed

$$\begin{array}{lcl} \cos\omega & = & +\ 0,9324722294 \\ \cos 2\omega & = & +\ 0,7390089172 \\ \cos 4\omega & = & +\ 0,0922683595 \\ \cos 8\omega & = & -\ 0,9829730997 \\ \hline \text{Sum} & = & +\ 0,7807764064 \end{array} \qquad \begin{array}{lcl} \cos 3\omega & = & +\ 0,4457383558 \\ \cos 5\omega & = & -\ 0,2736629901 \\ \cos 6\omega & = & -\ 0,6026346364 \\ \cos 7\omega & = & -\ 0,8502171357 \\ \hline \text{Sum} & = & -\ 1,2807764065 \end{array}$$

Hence

$$1 + 4\sum\cos a'\omega = +\sqrt{17}\ , \quad 1 + 4\sum\cos b'\omega = -\sqrt{17}.$$

IV. For $n = 3$ there is a unique value $a = 1$, which corresponds to

$$\sin\omega = +0,8660254038,$$

Hence $2\sin\omega = +\sqrt{3}$.

V. For $n = 7$ there are three values of a, namely 1, 2, 4; hence we have the sines

$$\begin{array}{lcl} \sin\omega & = & +\ 0,7818314825 \\ \sin 2\omega & = & +\ 0,9749279122 \\ \sin 4\omega & = & -\ 0,4338837391 \\ \hline \text{Sum} & = & -\ 1,3228756556, \end{array}$$

and therefore

$$2\sum\sin a\omega = +\sqrt{7}$$

VI. For $n = 11$ the values of a are 1, 3, 4, 5, 9, which correspond to the sines

$$\begin{array}{lcl} \sin\omega & = & +\ 0,5406408175 \\ \sin 3\omega & = & +\ 0,9898214419 \\ \sin 4\omega & = & +\ 0,7557495744 \\ \sin 5\omega & = & +\ 0,2817325568 \\ \sin 9\omega & = & -\ 0,9096319954 \\ \hline \text{Sum} & = & +\ 1,6583123952, \end{array}$$

and from this

$$2\sum\sin a\omega = +\sqrt{11}$$

VII. For $n = 19$ the values of a are 1, 4, 5, 6, 7, 9, 11, 16, 17, which correspond to the sines

$$\begin{array}{lcl}
\sin\omega & = & +\,0,3246994692 \\
\sin 4\omega & = & +\,0,9694002659 \\
\sin 5\omega & = & +\,0,9965844930 \\
\sin 6\omega & = & +\,0,9157733267 \\
\sin 7\omega & = & +\,0,7357239107 \\
\sin 9\omega & = & +\,0,1645945903 \\
\sin 11\omega & = & -\,0,4759473930 \\
\sin 16\omega & = & -\,0,8371664783 \\
\sin 17\omega & = & -\,0,6142127127 \\
\hline
\text{Sum} & = & +\,2,174494718,
\end{array}$$

and therefore

$$2\sum \sin a\omega = +\sqrt{19}.$$

Art. 4

In all these examples the radical quantity obtains a positive sign, and the same is easily confirmed for larger values $n = 23$, $n = 29$, etc. Based on these computations there is a strong probability that this is the case in general. But the demonstration of this phenomenon cannot be sought from the principles set forth in loc. cit., so a deeper investigation is required to establish it fully and correctly. The purpose of this commentary is therefore to bring forward a rigorous demonstration of this most elegant theorem, which had been unsuccessfully attempted for many years in various ways, and which was finally successfully perfected through particular and quite subtle considerations, and at the same time to raise the theorem itself to a far greater generality, saving or rather increasing its elegance. Finally, we will reveal a most surprising and intricate connection between this summation and the most profound theorem of arithmetic. We hope that not only will geometers be gratified by the results of these investigations, but also that the methods, which may well be useful on other occasions, will be deemed worth of their attention.

Art. 5

Our demonstration arose from the consideration of a particular class of progressions, the terms of which depend on expressions such as

$$\frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})\cdots(1-x^{m-\mu+1})}{(1-x)(1-xx)(1-x^3)\cdots(1-x^\mu)}$$

For the sake of brevity, we will denote such a fraction by (m, μ), and we will first make some general observations about such functions.

I. If m is a positive integer smaller than μ, the function (m, μ) obviously vanishes, because the numerator involves a factor $(1 - x^0)$. For $m = \mu$, the factors in the numerator will be identical in reverse order to the factors in the denominator, so that $(\mu, \mu) = 1$. Finally, for the case where m is a positive integer greater than μ, we have the formulas

$$\begin{aligned}
(\mu+1, \mu) &= \frac{1-x^{\mu+1}}{1-x} = (\mu+1, 1) \\
(\mu+2, \mu) &= \frac{(1-x^{\mu+2})(1-x^{\mu+1})}{(1-x)(1-xx)} = (\mu+2, 2) \\
(\mu+3, \mu) &= \frac{(1-x^{\mu+3})(1-x^{\mu+2})(1-x^{\mu+1})}{(1-x)(1-xx)(1-x^3)} = (\mu+3, 3), \text{ etc.}
\end{aligned}$$

or in general,

$$(m, \mu) = (m, m-\mu)$$

II. Furthermore, it is easily confirmed that in general

$$(m, \mu+1) = (m-1, \mu+1) + x^{m-\mu-1}(m-1, \mu)$$

and therefore, since

$$\begin{aligned}(m-1, \mu+1) &= (m-2, \mu+1) + x^{m-\mu-2}(m-2, \mu)\\ (m-2, \mu+1) &= (m-3, \mu+1) + x^{m-\mu-3}(m-3, \mu)\\ (m-3, \mu+1) &= (m-4, \mu+1) + x^{m-\mu-4}(m-4, \mu), \text{ etc.}\end{aligned}$$

which series may be continued up to

$$\begin{aligned}(\mu+2, \mu+1) &= (\mu+1, \mu+1) + x(\mu+1, \mu)\\ &= (\mu, \mu) + x(\mu+1, \mu),\end{aligned}$$

one has, as long as m is a positive integer greater than $\mu+1$,

$$\begin{aligned}(m, \mu+1) = (\mu, \mu) + x(\mu+1, \mu) + xx(\mu+2, \mu) + x^3(\mu+3, \mu) + \text{etc.}\\ + x^{m+\mu-1}(m-1, \mu)\end{aligned}$$

Hence it is clear that if, for any given value of μ, the function (m, μ) is integral for all integers m, then the functions $(m, \mu+1)$ must be integral as well. Therefore, since that supposition holds for $\mu = 1$, the same will hold for $\mu = 2$, hence also for $\mu = 3$ etc., i.e. in general for any positive integer value of m the function (m, μ) will be integral, or in other words the product

$$(1-x^m)(1-x^{m-1})(1-x^{m-2})\dots(1-x^{m-\mu+1})$$

will be divisible by

$$(1-x)(1-x^2)(1-x^3)\dots(1-x^\mu).$$

Art. 6

We now consider two series, both of which will help us reach our goal. The first series is

$$1 - \frac{1-x^m}{1-x} + \frac{(1-x^m)(1-x^{m-1})}{(1-x)(1-xx)} - \frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-xx)(1-x^3)} + \text{etc.}$$

or

$$1 - (m, 1) + (m, 2) - (m, 3) + (m, 4) - \text{etc.}$$

which for the sake of brevity we denote by $f(x, m)$. It is immediately obvious that whenever m is a positive integer, this series terminates after the $(m+1)^{st}$ term (which becomes $= \pm 1$) so that in this case the sum must be a finite integral function of x. Furthermore, by Art. 5 it is clear that, in general, one has for any value of m

$$\begin{aligned}1 &= 1\\ -(m, 1) &= -(m-1, 1) - x^{m-1}\\ +(m, 2) &= +(m-1, 2) + x^{m-2}(m-1, 1)\\ -(m, 3) &= -(m-1, 3) - x^{m-3}(m-1, 2) \text{ etc.}\end{aligned}$$

and therefore

$$\begin{aligned}f(x, m) = (1-x^{m-1}) - (1-x^{m-2})(m-1, 1) + (1-x^{m-3})(m-1, 2)\\ - (1-x^{m-4})(m-1, 3) + \text{ etc.}\end{aligned}$$

But it is evident that

$$\begin{aligned}(1-x^{m-2})(m-1,1)&=(1-x^{m-1})(m-2,1)\\(1-x^{m-3})(m-1,2)&=(1-x^{m-1})(m-2,2)\\(1-x^{m-4})(m-1,3)&=(1-x^{m-1})(m-2,3)\text{ etc.}\end{aligned}$$

and from this we deduce the equation

$$f(x,m)=(1-x^{m-1})f(x,m-2) \tag{1}$$

Art. 7

Since for $m=0$ we have $f(x,m)=1$, we obtain from the formula just found

$$\begin{aligned}f(x,2)&=(1-x)\\f(x,4)&=(1-x)(1-x^3)\\f(x,6)&=(1-x)(1-x^3)(1-x^5)\\f(x,8)&=(1-x)(1-x^3)(1-x^5)(1-x^7)\text{ etc.}\end{aligned}$$

or generally for any even value of m,

$$f(x,m)=(1-x)(1-x^3)(1-x^5)\dots(1-x^{m-1}) \tag{2}$$

On the other hand, since $f(x,m)=0$ for $m=1$, we have

$$\begin{aligned}f(x,3)&=0\\f(x,5)&=0\\f(x,7)&=0\text{ etc.}\end{aligned}$$

or in general for any odd value of m,

$$f(x,m)=0.$$

Moreover, the latter could have already been derived from the fact that in the series

$$1-(m,1)+(m,2)-(m,3)+\text{etc.}+(m,m-1)-(m,m)$$

the last term destroys the first, the penultimate destroys the second, etc.

Art. 8

Indeed, the case where m is an odd positive integer is sufficient for our purposes; but, because of the singularity of the matter, it will not hurt to add to this the cases where m is negative and possibly fractional.

Obviously our series will then no longer terminate, but will run to infinity. Moreover, it is easy to see that it becomes divergent whenever x is given a value smaller than 1. Therefore, the summation will have to be restricted to values of x which are greater than 1.

By formula (1) of Art. 6 we have

$$\begin{aligned}f(x,-2)&=\frac{1}{1-\frac{1}{x}}\\f(x,-4)&=\frac{1}{1-\frac{1}{x}}\cdot\frac{1}{1-\frac{1}{x^3}}\\f(x,-2)&=\frac{1}{1-\frac{1}{x}}\cdot\frac{1}{1-\frac{1}{x^3}}\cdot\frac{1}{1-\frac{1}{x^5}}\end{aligned}$$

so that for negative odd integers the function $f(x,m)$ can also be assigned a value with finitely many terms. For the remaining values of m we will convert the function $f(x,m)$ into an *infinite product.*

As m decreases to negative infinity, the function $f(x,m)$ passes into

$$1+\frac{1}{x-1}+\frac{1}{x-1}\cdot\frac{1}{xx-1}+\frac{1}{x-1}\cdot\frac{1}{xx-1}\cdot\frac{1}{x^3-1}+\text{ etc.},$$

so this series is equal to the infinite product

$$\frac{1}{1-\frac{1}{x}}\cdot\frac{1}{1-\frac{1}{x^3}}\cdot\frac{1}{1-\frac{1}{x^5}}\cdot\frac{1}{1-\frac{1}{x^7}}\text{ etc. to infinity }.$$

Moreover, since in general

$$f(x,m)=f(x,m-2\lambda).(1-x^{m-1})(1-x^{m-3})(1-x^{m-5})\ldots(1-x^{m-2\lambda+1})$$

we have

$$\begin{aligned}f(x,m)&=f(x,-\infty)).(1-x^{m-1})(1-x^{m-3})(1-x^{m-5})\text{ etc. to infinity}\\&=\frac{1-x^{m-1}}{1-x^{-1}}\cdot\frac{1-x^{m-3}}{1-x^{-3}}\cdot\frac{1-x^{m-5}}{1-x^{-5}}\cdot\frac{1-x^{m-7}}{1-x^{-7}}\text{ etc. to infinity}\end{aligned}$$

whose factors obviously converge to unity.

The case $m=-1$ deserves special attention. Here

$$f(x,-1)=1+x^{-1}+x^{-3}+x^{-6}+x^{-10}+\text{ etc.}$$

It follows that this series is equal to the infinite product

$$\frac{1-x^{-2}}{1-x^{-1}}\frac{1-x^{-4}}{1-x^{-3}}\frac{1-x^{-6}}{1-x^{-5}}\text{ etc.}$$

and writing x for x^{-1}, one obtains

$$1+x+x^3+x^6+\text{ etc.}=\frac{1-xx}{1-x}\cdot\frac{1-x^4}{1-x^3}\cdot\frac{1-x^6}{1-x^5}\text{ etc.}$$

This equality between two somewhat complicated expressions, to which we shall return on another occasion, is certainly very memorable.

Art. 9

The second series we must consider is

$$1+x^{\frac{1}{2}}\frac{1-x^m}{1-x}+x\frac{(1-x^m)(1-x^{m-1})}{(1-x)(1-xx)}+x^{\frac{3}{2}}\frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-xx)(1-x^3)}+\text{ etc.}$$

or

$$1+x^{\frac{1}{2}}(m,1)+x(m,2)+x^{\frac{3}{2}}(m,3)+xx(m,4)+\text{ etc.}$$

which we denote by $F(x,m)$. We will restrict this discussion to the case where m is a positive integer, so that this series always terminates with the $(m+1)^{st}$ term, which is $=x^{\frac{m}{2}}(m,m)$. Since

$$(m,m)=1,\ \ (m,m-1)=(m,1),\ \ (m,m-2)=(m,2),\text{ etc.}$$

the above series can also be written like this:

$$x^{\frac{m}{2}}+x^{\frac{m-1}{2}}(m,1)+x^{\frac{m-2}{2}}(m,2)+x^{\frac{m-3}{2}}(m,3)+\text{ etc.}$$

Hence

$$\begin{aligned}(1+x^{\frac{m+1}{2}})F(x,m) =&1+x^{\frac{1}{2}}(m,1)+x(m,2)+x^{\frac{3}{2}}(m,3)+\text{ etc.}\\ &+x^{\frac{1}{2}}.x^m+x.x^{m-1}(m,1)+x^{\frac{3}{2}}x^{m-2}(m,2)+\text{ etc.}\end{aligned}$$

Therefore, considering that one has (Art. 5 II)

$$\begin{aligned}(m,1)+x^m&=(m+1,1)\\ (m,2)+x^{m-1}(m,1)&=(m+1,2)\\ (m,3)+x^{m-2}(m,2)&=(m+1,3)\text{ etc.}\end{aligned}$$

we obtain the result

$$(1+x^{\frac{m+1}{2}})F(x,m)=F(x,m+1) \tag{3}$$

But $F(x,0)=1$, therefore

$$\begin{aligned}F(x,1)&=1+x^{\frac{1}{2}}\\ F(x,2)&=(1+x^{\frac{1}{2}})(1+x)\\ F(x,3)&=(1+x^{\frac{1}{2}})(1+x)(1+x^{\frac{3}{2}})\text{ etc.}\end{aligned}$$

and in general

$$F(x,m)=(1+x^{\frac{1}{2}})(1+x)(1+x^{\frac{3}{2}})\dots(1+x^{\frac{m}{2}}) \tag{4}$$

Art. 10

Having made these preliminary observations, let us now proceed to our ultimate purpose. Since for a prime value of n, the squares 1, 4, 9, …, $(\frac{1}{2}(n-1))^2$ are incongruent modulo n, it is clear that their minimal residues modulo n must be identical with the numbers a, and therefore

$$\begin{aligned}\sum\cos ak\omega&=\cos k\omega+\cos 4k\omega+\cos 9k\omega+\text{etc.}+\cos(\tfrac{1}{2}(n-1))^2k\omega\\ \sum\sin ak\omega&=\sin k\omega+\sin 4k\omega+\sin 9k\omega+\text{etc.}+\sin(\tfrac{1}{2}(n-1))^2k\omega\end{aligned}$$

Likewise, since the same squares 1, 4, 9, …, $(\frac{1}{2}(n-1))^2$ in reverse order are congruent to $(\frac{1}{2}(n+1))^2$, $(\frac{1}{2}(n+3))^2$, $(\frac{1}{2}(n+5))^2$, … $(n-1)^2$, we also have

$$\begin{aligned}\sum\cos ak\omega&=\cos\left(\tfrac{1}{2}(n+1)\right)^2k\omega+\cos\left(\tfrac{1}{2}(n+3)\right)^2k\omega+\text{etc.}+\cos(n-1)^2k\omega\\ \sum\sin ak\omega&=\sin\left(\tfrac{1}{2}(n+1)\right)^2k\omega+\sin\left(\tfrac{1}{2}(n+3)\right)^2k\omega+\text{etc.}+\sin(n-1)^2k\omega\end{aligned}$$

By setting therefore

$$T=1+\cos k\omega+\cos 4k\omega+\cos 9k\omega+\text{etc.}+\cos(n-1)^2k\omega$$

$$U=\sin k\omega+\sin 4k\omega+\sin 9k\omega+\text{etc.}+\sin(n-1)^2k\omega$$

we will have

$$\begin{aligned}1+2\sum\cos ak\omega&=T\\ 2\sum\sin ak\omega&=U\end{aligned}$$

From this it is clear that the summations proposed in Art. 1 depend on the summations of the series T and U. We will therefore adapt our discussion to these, and complete it with generality, so that it includes not only prime values of n but composite ones as well. Let us also suppose that the number k is prime to n; for the case where k and n have a common divisor can be reduced to this without any difficulty.

Art. 11

Denote the imaginary quantity $\sqrt{-1}$ by i, and let

$$\cos k\omega + i \sin k\omega = r,$$

so that $r^n = 1$, or r is a root of the equation $x^n - 1 = 0$. It is easily seen that all the numbers k, $2k$, $3k$, $\ldots$, $(n-1)k$ are not divisible by n and are all incongruent modulo n. Hence the powers of r

$$1, r, rr, r^3, \ldots, r^{n-1}$$

are all distinct, and each will also satisfy the equation $x^n - 1 = 0$. For this reason, these powers will represent all roots of the equation $x^n - 1 = 0$.

These conclusions would not be valid if k had a common divisor with n. For if ν were such a common divisor, $k.\frac{n}{\nu}$ would be divisible by n, and therefore a lower power than r^n, namely $r^{\frac{n}{\nu}}$, would be equal to 1. In this case, therefore, the powers of r up to the $\frac{n}{\nu}^{th}$ would be roots of the equation $x^n - 1 = 0$, and indeed these are all distinct roots, if ν is the greatest common divisor of k and n. In our case, where k and n are supposed to be relatively prime, it is convenient to call r a *proper root* of the equation $x^n - 1 = 0$. In the other case, where k and n have a greatest common divisor ν, we will say that r is an *improper root* of the equation. Obviously in the latter case, the same r would be a proper root of the equation $r^{\frac{n}{\nu}} - 1 = 0$. The simplest improper root is unity, and in the case where n is a prime number, there will be no other improper roots whatsoever.

Art. 12

If we then set

$$W = 1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2}$$

it is clear that $W = T + iU$, so that T is the real part of W and U is obtained from the imaginary part by suppressing the factor of i. The whole task then reduces to evaluating the summation W. To this end the series in Art. 6 and Art. 9 may be used, although the former is less suitable in the case where n is an even number. Nevertheless, we hope that it will be agreeable to the reader, if we treat the case where n is odd according to two different methods.

So, let us suppose first that n is an odd number, that r is a proper root of the equation $x^n - 1 = 0$, and that in the function $f(x, m)$ we set $x = r$ and $m = n - 1$. Then clearly

$$\frac{1 - x^m}{1 - x} = \frac{1 - r^{-1}}{1 - r} = -r^{-1}$$
$$\frac{1 - x^{m-1}}{1 - xx} = \frac{1 - r^{-2}}{1 - rr} = -r^{-2}$$
$$\frac{1 - x^{m-2}}{1 - x^3} = \frac{1 - r^{-3}}{1 - r^3} = -r^{-3} \text{ etc.}$$

up to

$$\frac{1 - x}{1 - x^m} = \frac{1 - r^{-m}}{1 - r^m} = -r^{-m}.$$

(It is worth pointing out that these equations are only valid insofar as r is assumed to be a proper root; for if r were an improper root, in some cases the numerator and denominator of these fractions would vanish at the same time, and thus the fractions would become indeterminate).

Hence we derive the following equation:

$$\begin{aligned} f(r, n-1) &= 1 + r^{-1} + r^{-3} + r^{-6} + \text{etc.} + r^{-\frac{1}{2}(n-1)n} \\ &= (1 - r)(1 - r^3)(1 - r^5)\ldots(1 - r^{n-2}) \end{aligned}$$

The same equation will still be valid if r^λ is substituted for r, where λ can be any integer relatively prime to n, for then r^λ will also be a proper root of the equation $x^n - 1 = 0$. Let us therefore write r^{n-2}, or what is the same, r^{-2}, in place of r. This gives

$$1 + r^2 + r^6 + r^{12} + \text{etc.} + r^{(n-1)n} = (1 - r^{-2})(1 - r^{-6})(1 - r^{-10}) \dots (1 - r^{-2(n-2)}).$$

Next we multiply both sides of this equation by

$$r.r^3.r^5 \dots r^{(n-2)} = r^{\frac{1}{4}(n-1)^2}$$

and because

$$\begin{aligned} r^{2+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-3)^2}, & r^{(n-1)n+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+1)^2} \\ r^{6+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-5)^2}, & r^{(n-2)(n-1)+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+3)^2} \\ r^{12+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-7)^2}, & r^{(n-3)(n-2)+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+5)^2} \end{aligned}$$

we obtain the following equation

$$\begin{aligned} r^{\frac{1}{4}(n-1)^2} + r^{\frac{1}{4}(n-3)^2} + r^{\frac{1}{4}(n-5)^2} + \text{etc.} + r + 1 \\ + r^{\frac{1}{4}(n+1)^2} + r^{\frac{1}{4}(n+3)^2} + r^{\frac{1}{4}(n+5)^2} + \text{etc.} + r^{\frac{1}{4}(2n-2)^2} \\ = (r - r^{-1})(r^3 - r^{-3})(r^5 - r^{-5}) \dots (r^{n-2} - r^{-n+2}) \end{aligned}$$

or, by arranging the members of the first part differently,

$$1 + r + r^4 + \text{etc.} + r^{(n-1)^2} = (r - r^{-1})(r^3 - r^{-3})(r^5 - r^{-5}) \dots (r^{n-2} - r^{-n+2}) \tag{5}$$

The factors of the right hand side of equation (5) can also be presented as

$$\begin{aligned} r - r^{-1} &= -(r^{n-1} - r^{-n+1}) \\ r^3 - r^{-3} &= -(r^{n-3} - r^{-n+5}) \\ r^5 - r^{-5} &= -(r^{n-5} - r^{-n+5}) \text{ etc.} \end{aligned}$$

up to

$$r^{n-2} - r^{-n+2} = -(r^2 - r^{-2})$$

in which case this equation assumes the form

$$W = (-1)^{\frac{1}{2}(n-1)}(r^2 - r^{-2})(r^4 - r^{-4})(r^6 - r^{-6}) \dots (r^{n-1} - r^{-n+1})$$

Multiplying this equation by (5) in its original form produces

$$W^2 = (-1)^{\frac{1}{2}(n-1)}(r - r^{-1})(r^2 - r^{-2})(r^3 - r^{-3}) \dots (r^{n-1} - r^{-n+1})$$

where $(-1)^{\frac{1}{2}(n-1)}$ is either $= +1$ or $= -1$ depending on whether n is of the form $4n + 1$ or $4n + 3$. Hence

$$W^2 = \pm r^{\frac{1}{2}n(n-1)}(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \dots (1 - r^{-2(n-1)})$$

But it is easily seen that r^{-2}, r^{-4}, r^{-6}, …, r^{-2n+2} are precisely all of the roots of the equation $x^n - 1 = 0$, except the root $r = 1$. Hence we obtain the identity

$$(x - r^{-2})(x - r^4)(x - r^{-6}) \dots (x - r^{-2n+2}) = x^{n-1} + x^{n-2} = x^{n-3} + \text{etc.} + x + 1,$$

and setting $x = 1$, we find that

$$(1 - r^{-2})(1 - r^4)(1 - r^{-6}) \dots (1 - r^{-2n+2}) = n$$

Since it is clear that $r^{\frac{1}{2}n(n-1)} = 1$, our equation passes into

$$W^2 = \pm n \tag{6}$$

So, in the case where n is of the form $4\mu + 1$, we have

$$W = +\sqrt{n}, T = +\sqrt{n}, U = 0$$

and in the case where it is of the form $4\mu + 3$, we have

$$W = \pm i\sqrt{n}, T = 0, U = \pm\sqrt{n}$$

Art. 14

The method of the preceding article determines only the absolute value of T and U, and leaves the signs ambiquous, so it is necessary to establish T in the former case and U in the latter case as $= +\sqrt{n}$ or $= -\sqrt{n}$. But this, at least for the case $k = 1$, can be deduced from equation (5) in the following way. Whereas, for $k = 1$,

$$r - r^{-1} = 2i \sin\omega$$
$$r^3 - r^{-3} = 2i \sin 3\omega$$
$$r^5 - r^{-5} = 2i \sin 5\omega \text{ etc.}$$

the equation is transformed to

$$W = (2i)^{\frac{1}{2}(n-1)} \sin\omega \sin 3\omega \sin 5\omega \ldots \sin(n-2)\omega$$

Also in the case where n is of the form $4\mu + 1$, in the series of odd numbers

$$1, 3, 5, 7, \ldots, \tfrac{1}{2}(n-3), \tfrac{1}{2}(n+1), \ldots, (n-2)$$

are found $\frac{1}{4}(n-1)$, which are less than $\frac{1}{2}n$, and to these will correspond to positive sines. On the other hand the remaining $\frac{1}{4}(n-1)$ will be greater than $\frac{1}{2}n$, and will correspond to negative sines. Therefore the product of all the sines will be equal to the product of a positive quantities, mulipled by the factor $(-1)^{\frac{1}{4}(n-1)}$, and therefore W will be equal to the product of a real positive quantity with i^{n-1}, or 1, since $i^4 = 1$ and $n-1$ is divisible by 4. That is, the quantity W will be a positive real number, and hence we must necessarily have

$$W = +\sqrt{n}\ ,\quad T = +\sqrt{n}.$$

In the second case, where n is of the form $4\mu + 3$, in the series of odd numbers

$$1, 3, 5, 7 \ldots, \frac{1}{2}(n-1), \frac{1}{2}(n+3), \ldots, (n-2)$$

the first $\frac{1}{4}(n+1)$ will be smaller than $\frac{1}{2}n$, and the remaining $\frac{1}{4}(n-3)$ will be larger. Among the sines corresponding to the arcs ω, 3ω, 5ω, ..., $(n-2)\omega$, therefore, $\frac{1}{4}(n-3)$ of them will be negative. Thus W will be the product of $i^{\frac{1}{2}(n-1)}$ with a positive real quantity and $(-1)^{\frac{1}{4}(n-3)}$. The third factor is $i^{\frac{1}{2}(n-3)}$, which combined with the first term produces $i^{n-2} = i$, since $i^{n-3} = 1$. Therefore we necessarily have

$$W = +i\sqrt{n}\ ,\quad U = +\sqrt{n}.$$

Art 15.

We will now show how the same conclusions can be drawn from the progression considered in Art. 9. Let us write $-y^{-1}$ in place of $x^{\frac{1}{2}}$ in (4), so it becomes

$$1 - y^{-1}\frac{1-y^{-2m}}{1-y^{-2}} + y^{-2}\frac{(1-y^{-2m})(1-y^{-2m+2})}{(1-y^{-2})(1-y^{-4})} - y^{-3}\frac{(1-y^{-2m})(1-y^{-2m+2})(1-y^{-2m+4})}{(1-y^{-2})(1-y^{-4})(1-y^{-6})} + \text{etc.}$$

up to the $(m+1)^{st}$ term

$$= (1-y^{-1})(1-y^{-2})(1-y^{-3})(1+y^{-4})\ldots(1 \pm y^{-m}) \qquad (7)$$

If here we let $y = r$ be a proper root of the equation $y^n - 1 = 0$, and at the same time set $m = n-1$, then we have

$$\frac{1-y^{-2m}}{1-y^{-2}} = \frac{1-r^2}{1-r^{-2}} = -r^2$$
$$\frac{1-y^{-2m+2}}{1-y^{-4}} = \frac{1-r^4}{1-r^{-4}} = -r^4$$
$$\frac{1-y^{-2m+2}}{1-y^{-6}} = \frac{1-r^6}{1-r^{-6}} = -r^6 \text{ etc.}$$

up to

$$\frac{1-y^{-2}}{1-y^{-2m}} = \frac{1-r^{2n-2}}{1-r^{-2n+2}} = -r^{2n-2}$$

where it is noted that none of the denominators $1-r^{-2}$, $1-r^{-4}$, etc. become $=0$. Hence equation (7) takes the form

$$1+r+r^4+r^9+\text{ etc.}+r^{(n-1)^2} = (1-r^{-1}(1+r^{-2})(1-r^{-3})\dots(1+r^{-n+1})$$

On the right hand side of this equation, if we multiply the first term by the last, the second by the penultimate, etc.

$$\begin{aligned}(1-r^{-1})(1+r^{-n+1}) &= (r-r^{-1})\\(1+r^{-2})(1-r^{-n+2}) &= r^{n-2}-r^{-n+2})\\(1-r^{-3})(1+r^{-n+3}) &= r^3-r^{-3}\\(1+r^{-4})(1-r^{-n+4}) &= r^{n-4}-r^{-n+4}\text{ etc.}\end{aligned}$$

From these partial products it is easy to see that the following product is created:

$$(r-r^{-1})(r^3-r^{-3})(r^5-r^{-5})\dots(r^{n-4}-r^{-n+4})(r^{n-2}-r^{-n+2})$$

which is therefore

$$= 1+r+r^4+r^9+\text{etc.}+r^{(n-1)^2} = W$$

This equation is identical with the equation (5) in Art. 12, which was derived from the first development, and thus the rest of the reasoning can be carried out in the same way as in Art. 13 and Art. 14.

Art. 16

We now move on to the second case, where the number n is even. First let n be of the form $4\mu+2$, or oddly even. Then it is clear that the numbers $\frac{1}{2}nn$, $(\frac{1}{2}n+1)^2-1$, $(\frac{1}{2}n+2)^2-4$ etc. or more generally $(\frac{1}{2}n+\lambda)^2-\lambda^2$ can be divided by $\frac{1}{2}n$ to produce odd quotients, and thus they are congruent to $\frac{1}{2}n$ modulo n. Hence it is concluded that if r is a proper root of the equation $x^n-1=0$, and therefore $r^{\frac{1}{2}n}=-1$, these become

$$\begin{aligned}r^{(\frac{1}{2}n)^2} &= -1\\r^{(\frac{1}{2}n+1)^2} &= -r\\r^{(\frac{1}{2}n+2)^2} &= -r^4\\r^{(\frac{1}{2}n+3)^2} &= -r^9\text{etc.}\end{aligned}$$

Therefore in the series

$$1+r+r^4+r^9+\text{etc.}+r^{(n-1)^2}$$

the term $r^{(\frac{1}{2}n)^2}$ will destroy the first, the following the second, etc. and therefore

$$W=0, T=0, U=0$$

Art. 17

There remains the case where n is of the form 4μ, or is evenly even. Here in general $(\frac{1}{2}n+\lambda)^2-\lambda\lambda$ will be divisible by n, therefore

$$r^{(\frac{1}{2}n+\lambda)^2} = r^{\lambda\lambda}$$

Hence in the series

$$1+r+r^4+r^9+\text{etc.}+r^{(n-1)^2}$$

the term $r^{(\frac{1}{2}n)^2}$ will be equal to the first, the following to the second, etc., so that

$$W = 2(1 + r + r^4 + r^9 + \text{etc.} + r^{(\frac{1}{2}n-1)^2})$$

Let us now suppose, in equation (7) of Art. 15 we set $m = \frac{1}{2}n - 1$, and for y we substitute a root r of the equation $y^n - 1 = 0$. Then just as in Art. 15 the equation takes the following form:

$$1 + r + r^4 + \text{ etc.} + r^{(\frac{1}{2}n-1)^2} = (1 - r^{-1})(1 + r^{-2})(1 - r^{-3}) \ldots (1 - r^{-\frac{1}{2}n+1})$$

or

$$W = 2(1 - r^{-1})(1 + r^{-2})(1 - r^{-3}) \ldots (1 - r^{-\frac{1}{2}n+1}) \tag{8}$$

Moreover, since $r^{\frac{1}{2}n} = -1$, we have

$$\begin{aligned} 1 + r^{-2} &= -r^{\frac{1}{2}n-2}(1 - r^{-\frac{1}{2}n+2}) \\ 1 + r^{-4} &= -r^{\frac{1}{2}n-4}(1 - r^{-\frac{1}{2}n+4}) \\ 1 + r^{-6} &= -r^{\frac{1}{2}n-6}(1 - r^{-\frac{1}{2}n+6}) \text{ etc.} \end{aligned}$$

and the product of the factors $-r^{\frac{1}{2}n-2}$, $-r^{\frac{1}{2}n-2}$, $-r^{\frac{1}{2}n-2}$ etc. up to $-r^2$ is $= (-1)^{\frac{1}{4}n-1}r^{\frac{1}{16}nn-\frac{1}{4}n}$, the preceding equation can also be presented as

$$W = 2(-1)^{\frac{1}{4}n-1}r^{\frac{1}{16}nn-\frac{1}{4}n}(1 - r^{-1})(1 + r^{-2})(1 - r^{-3}) \ldots (1 - r^{-\frac{1}{2}n+1})$$

Considering that

$$\begin{aligned} 1 - r^{-1} &= -r^{-1}(1 - r^{-n+1}) \\ 1 - r^{-2} &= -r^{-2}(1 - r^{-n+2}) \\ 1 - r^{-3} &= -r^{-3}(1 - r^{-n+3}) \text{ etc.} \end{aligned}$$

we have

$$\begin{aligned} &(1 - r^{-1})(1 - r^{-2})(1 - r^{-3}) \ldots (1 - r^{-\frac{1}{2}n+1}) \\ &\qquad = (-1)^{\frac{1}{2}n-1}r^{-\frac{1}{8}nn+\frac{1}{4}n}(1 - r^{-\frac{1}{2}n-1})(1 - r^{-\frac{1}{2}n-2})(1 - r^{-\frac{1}{2}n-3}) \ldots (1 - r^{-n+1}) \end{aligned}$$

and therefore

$$W = 2(-1)^{\frac{3}{4}n-2}r^{-\frac{1}{16}nn}(1 - r^{-\frac{1}{2}n-1})(1 - r^{-\frac{1}{2}n-2})(1 - r^{-\frac{1}{2}n-3}) \ldots (1 - r^{-n+1})$$

Multiplying this value of W by the one previously found, and adjoining to both sides the factor $(1 - r^{-\frac{1}{2}n})$, produces

$$(1 - r^{-\frac{1}{2}n})W^2 = 4(-1)^{n-3}r^{-\frac{1}{4}n}(1 - r^{-1})(1 - r^{-2})(1 - r^{-3}) \ldots (1 - r^{-n+1})$$

But we have

$$\begin{aligned} 1 - r^{-\frac{1}{2}n} &= 2 \\ (-1)^{n-3} &= -1 \\ r^{-\frac{1}{4}n} &= -r^{\frac{1}{4}n} \\ (1 - r^{-1})(1 - r^{-2})(1 - r^{-3}) \ldots (1 - r^{-n+1}) &= n \end{aligned}$$

and hence it is finally concluded that

$$W^2 = 2r^{\frac{1}{4}n}n \tag{9}$$

It is easy to see that $r^{\frac{1}{4}n}$ is equal to either $+i$ or $-i$, depending on whether k is of the form $4\mu + 1$, or of the form $4\mu + 3$. And since

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

we will have in the case where k is of the form $4\mu + 1$,

$$W = \pm(1 + i)\sqrt{n}, T = U = \pm\sqrt{n}$$

and in the other case, where k is of the form $4\mu + 3$,

$$W = \pm(1 - i)\sqrt{n}, T = -U = \pm\sqrt{n}$$

Art. 18

The method of the preceding article supplied the absolute value of the functions T, U, and assigned the conditions under which equal or opposite signs should be given to them. But the signs themselves are not yet determined at this point. We will supplement this for the case $k = 1$, in the following way.

Let $\rho = \cos\frac{1}{2}\omega + i\sin\frac{1}{2}\omega$, so that $r = \rho\rho$ and $\rho^n = -1$,. It is clear that the equation (8) can be presented as

$$W = 2(1+\rho^{n-2})(1+\rho^{-1})(1+\rho^{n-6})(1+\rho^{-8})\dots(1+\rho^{-n+4})(1+\rho^{2}),$$

or by arranging the factors in a different order,

$$W = 2(1+\rho^{2})(1+\rho^{-4})(1+\rho^{6})(1+\rho^{-8})\dots(1+\rho^{-n+4})(1+\rho^{n-2})$$

The terms become

$$\begin{aligned} 1+\rho^2 &= 2\rho\cos\tfrac{1}{2}\omega \\ 1+\rho^{-4} &= 2\rho^{-2}\cos\omega \\ 1+\rho^{6} &= 2\rho^{3}\cos\tfrac{3}{2}\omega \\ 1+\rho^{-8} &= 2\rho^{-4}\cos 2\omega \text{ etc.} \end{aligned}$$

up to

$$\begin{aligned} 1+\rho^{-n+4} &= 2\rho^{-\frac{1}{2}n+2}\cos\left(\tfrac{1}{4}n-1\right)\omega \\ 1+\rho^{n-2} &= 2\rho^{\frac{1}{2}n-1}\cos\left(\tfrac{1}{4}n-\tfrac{1}{2}\right)\omega \end{aligned}$$

Therefore we have:

$$W = 2^{\frac{1}{2}n}\rho^{\frac{1}{4}n}\cos\tfrac{1}{2}\omega\cos\omega\cos\tfrac{3}{2}\omega\dots\cos\left(\tfrac{1}{4}n-\tfrac{1}{2}\right)\omega$$

The cosines in this product are manifestly positive, but the factor $\rho^{\frac{1}{4}n}$ becomes $= \cos 45^o + i\sin 45^o = (1+i)\sqrt{\frac{1}{2}}$. Hence, putting it all together, W is the product of $1+i$ with a positive real quantity, so it must necessarily be

$$W = (1+i)\sqrt{n}\ ,\ \ T = +\sqrt{n}\ ,\ \ U = +\sqrt{n}$$

Art. 19

It will be worthwhile to gather here all of the summations evaluated so far. In general,

$T =$	$U =$	when n is of the form
$\pm\sqrt{n}$	$\pm\sqrt{n}$	4μ
$\pm\sqrt{n}$	0	$4\mu+1$
0	0	$4\mu+2$
0	$\pm\sqrt{n}$	$4\mu+3$

and in the case where $k = 1$, a positive sign must be assigned to each radical quantity. Now, therefore, those things which had been noticed by induction in Art. 3 for the first few values of n have been demonstrated with all rigor, and nothing remains but to determine the signs for other values of k in all cases. But before this task can be undertaken in all generality, it will first be necessary to consider more closely those cases where m is a prime number or a power of a prime number.

Art. 20

Let n be an odd prime number. Then it is clear from what was explained in Art. 10 that $W = 1 + 2\sum r^a = 1 + 2\sum R^{ak}$, where we set $R = \cos\omega + i\sin\omega$, and denote indefinitely by a all of the quadratic residues of n between 1 and $n-1$. But if we also express indefinitely by b all quadratic non-residues between the same limits, it is seen without any difficulty that all numbers ak become congruent modulo n to all of a or all of b (with no regard to order), according as k is a quadratic residue or non-residue. In the former case

$$W = 1 + 2\sum R^a = 1 + R + R^4 + R^9 + \text{etc.} + R^{(n-1)^2}$$

and therefore $W = +\sqrt{n}$, if n is of the form $4\mu+1$, and $W = +i\sqrt{n}$, if n is of the form $4\mu+3$.

On the other hand, in the case where k is a quadratic non-residue modulo n, we have

$$W = 1 + 2\Sigma R^b.$$

Hince, since it is obvious that a and b together complete the complex numbers 1, 2, 3, ..., it follows that

$$\sum R^a + \sum R^b = R + R^2 + R^3 + \text{etc.} + R^{n-1} = -1$$

and thus

$$W = -1 - 2\sum R^a = -\left(1 + R + R^4 + R^9 + \text{etc.} + R^{(n-1)^2}\right)$$

Therefore $W = -\sqrt{n}$, if n is of the form $4\mu+1$, and $W = -i\sqrt{n}$, if n is of the form $4\mu+3$.

Hence, putting it all together, *first*, if n is of the form $4\mu+1$, and k is a quadratic residue modulo n,

$$T = +\sqrt{n}\ ,\quad U = 0$$

second, if n is of the form $4\mu+1$, and k is a quadratic non-residue modulo n,

$$T = -\sqrt{n}\ ,\quad U = 0$$

third, if n is of the form $4\mu+3$, and k is a quadratic residue modulo n,

$$T = 0\ ,\quad U = +\sqrt{n}$$

fourth, if n is of the form $4\mu+3$, and k is a quadratic non-residue modulo n,

$$T = 0\ ,\quad U = -\sqrt{n}$$

Art. 21

Next let n be a square or higher power of an odd prime p, and let $n = p^{2\chi}q$, so that q is either $= 1$ or $= p$. Here, first of all, it is appropriate to observe that if A is an integer which is not divisible by p^χ, then

$$\begin{aligned}
r^{\lambda\lambda} + & r^{(\lambda+p^\chi q)^2} + r^{(\lambda+2p^\chi q)^2} + r^{(\lambda+3p^\chi q)^2} + \text{etc.} + r^{(\lambda+(n-1)p^\chi q)^2} \\
&= r^{\lambda\lambda}\left\{1 + r^{2\lambda p^\chi q} + r^{4\lambda p^\chi q} + r^{6\lambda p^\chi q} + \text{etc.} + +r^{2\lambda(n-1)p^\chi q}\right\} \\
&= \frac{r^{\lambda\lambda}(1 - r^{2\lambda n})}{1 - r^{2\lambda p^\chi q}} = 0
\end{aligned}$$

Hence it is easy to see that

$$W = 1 + r^{p^{2\chi}} + r^{4p^{2\chi}} + r^{9p^{2\chi}} + \text{etc.} + r^{(n-p^\chi)^2}.$$

For the remaining terms in the series

$$1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2}$$

can be distributed into $(p^\chi - 1)q$ partial series, each of which has p^χ terms and is seen to vanishes by applying the transformation given above.

From this we conclude that in the case where $q = 1$, or where n is a prime power with an even exponent, one has

$$W = p^\chi = +\sqrt{n}\ , \quad T = +\sqrt{n}\ , \quad U = 0.$$

On the other hand, in the case where $q = p$, or where n is a prime power with an odd exponent, let us set $r^{p^{2\chi}} = \rho$, so that ρ will be a proper root of the equation $x^p - 1$, and indeed $\rho = \cos\frac{k}{p}360^o + i\sin\frac{k}{p}360^o$, then

$$W = 1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(p^{\chi+1}-1)^2} = p^\chi\left(1 + \rho + \rho^4 + \rho^9 + \text{etc.}\rho^{(p-1)^2}\right)$$

But the sum of the series $1 + \rho + \rho^4 + \rho^9 + \text{etc.}\rho^{(p-1)^2}$ has been determined in the previous article, from which it is automatically concluded that

$$W = \pm\sqrt{n} = T,\ \text{ if } p \text{ is of the form } 4\mu + 1$$

$$W = \pm i\sqrt{n} = iU,\ \text{ if } p \text{ is of the form } 4\mu + 3$$

with a positive or negative sign according to whether k is a quadratic residue or non-residue modulo p.

Art. 22

The following proposition, which is easily derived from what has been set forth in Articles 20 and 21, will be of considerable use to us later. Let

$$W' = 1 + r^h + r^{4h} + r^{9h} + \text{ etc. } + r^{h(n-1)^2}$$

where h is any integer not divisble by p. Then in the case where $n = p$, or when n is a power of p with an odd exponent, one has

$$W' = W, \text{ if } h \text{ is a quadratic residue modulo } p.$$
$$W' = -W, \text{ if } h \text{ is a quadratic non-residue modulo } p.$$

For it is clear that W' arises from W, if kh is substituted for k. In the former case, k and kh will be similar, and in the latter, dissimilar, insofar as they are quadratic residues or non-residues modulo p. However, in the case where n is a power of p with an even exponent, it is obvious that $W' = +\sqrt{n}$, and thus always $W' = W$.

Art. 23

In articles 20, 21, and 22, we considered odd prime numbers, and powers of such. There remains, therefore, the case in which n is a binary power.

For $n = 2$ it is clear that $W = 1 + r = 0$.

For $n = 4$ it turns out that $W = 1 + r + r^4 + r^9 = 2 + 2r$. Hence $W = 2 + 2i$ whenever k is of the form $4\mu + 1$, and $W = 2 - 2i$ whenever k is of the form $4\mu + 3$.

For $n = 8$ we have $W = 1 + r + r^4 + r^9 + r^{16} + r^{25} + r^{36} + r^{49} = 2 + 4r + 2r^4 = 4r$. Hence

$$\begin{aligned}
W &= (1+i)\sqrt{8},\ \text{when } k \text{ is of the form } 8\mu+1\\
W &= (-1+i)\sqrt{8},\ \text{when } k \text{ is of the form } 8\mu+3\\
W &= (-1-i)\sqrt{8},\ \text{when } k \text{ is of the form } 8\mu+5\\
W &= (1-i)\sqrt{8},\ \text{when } k \text{ is of the form } 8\mu+7
\end{aligned}$$

If n is a higher binary power, then set $n = 2^{2\chi}q$, where q is either $= 1$ or $= 2$, and χ is greater than 1. Here, first off all, it must be observed that if λ is an integer not divisible by $2^{\chi-1}$, then

$$\begin{aligned}
&r^{\lambda\lambda} + r^{(\lambda+2^\chi q)^2} + r^{(\lambda+2.2^\chi q)^2} + r^{(\lambda+3.2^\chi q)^2} + \text{etc.} + r^{(\lambda+n-2^\chi q)^2}\\
&\quad = r^{\lambda\lambda}\left\{1 + r^{2^{\chi+1}\lambda q} + r^{2.2^{\chi+1}\lambda q} + r^{3.2^{\chi+1}\lambda q} + \text{ etc. } + r^{\left(2n-2^{\chi+1}q\right)\lambda}\right\} = \frac{r^{\lambda\lambda}(1-r^{2\lambda n})}{1-r^{2^{\chi+1}\lambda q}} = 0
\end{aligned}$$

Thus it is easily seen that

$$W = 1 + r^{2^{2\chi-2}} + r^{4.2^{2\chi-2}} + r^{9.2^{2\chi-2}} + \text{etc.} + r^{(n-2^{\chi-1})^2}.$$

Let us set $r^{2^{2\chi-2}} = \rho$. Then ρ will be a root of the equation $x^{4q} - 1 = 0$, and indeed $\rho = \cos\frac{k}{4q}360^o + i\sin\frac{k}{4q}360^o$, and thus

$$\begin{aligned}
W &= 1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(2^{\chi+1}q-1)^2}\\
&= 2^{\chi-1}\left(1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(4q-1)^2}\right)
\end{aligned}$$

But the sum of the series $1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(4q-1)^2}$ is determined by what we have already explained in the cases $n = 4$ and $n = 8$, from which we conclude that

In the case $q = 1$, or where n is a power of the number 4,

$$\begin{aligned}
W &= (1+i)2^\chi = (1+i)\sqrt{n},\ \text{if } k \text{ is of the form } 4\mu+1\\
W &= (1-i)2^\chi = (1-i)\sqrt{n},\ \text{if } k \text{ is of the form } 4\mu+3
\end{aligned}$$

which are the very formulas already given for $n = 4$.

In the case $q = 2$, or where n is a binary power with an odd exponent greater than 3,

$$\begin{aligned}
W &= (1+i)2^\chi\sqrt{2} = (1+i)\sqrt{n},\ \text{if } k \text{ is of the form } 8\mu+1\\
W &= (-1+i)2^\chi\sqrt{2} = (-1+i)\sqrt{n},\ \text{if } k \text{ is of the form } 8\mu+1\\
W &= (-1-i)2^\chi\sqrt{2} = (-1-i)\sqrt{n},\ \text{if } k \text{ is of the form } 8\mu+1\\
W &= (1-i)2^\chi\sqrt{2} = (1-i)\sqrt{n},\ \text{if } k \text{ is of the form } 8\mu+1
\end{aligned}$$

which also exactly agree with those which we have given for $n = 8$.

Art. 24

It will also be worthwhile here to determine the ratio $\ell = \frac{W'}{W}$, where W' is the sum

$$W' = 1 + r^h + r^{4h} + r^{9h} + \text{etc.} + r^{h(n-1)^2}$$

and h is an arbitrary odd integer. Since W' is derived from W by changing k to kh, the value of W' will depend on the form of the number kh in the same way as W depends on the form of k. Thus it is clear that

I. In the case $n = 4$, or in the case of a higher binary power with an even exponent, one has

$$\begin{aligned}
&\ell = 1, \text{ if } h \text{ is of the form } 4\mu + 1\\
&\ell = -i, \text{ if } h \text{ is of the form } 4\mu + 3 \text{ and } k \text{ is of the form } 4\mu + 1\\
&\ell = i, \text{ if } h \text{ is of the form } 4\mu + 3 \text{ and } k \text{ is of the same form.}
\end{aligned}$$

II. In the case $n = 8$, or in the case of a higher binary power with an odd exponent, one has

$$\begin{aligned}
&\ell = 1, \text{ if } h \text{ is of the form } 8\mu + 1,\\
&\ell = -1, \text{ if } h \text{ is of the form } 8\mu + 5,\\
&\ell = i, \text{ if } h \text{ is of the form } 8\mu + 3 \text{ and } k \text{ is of the form } 4\mu + 1,\\
&\qquad\qquad \text{or if } h \text{ is of the form } 8\mu + 7 \text{ and } k \text{ is of the form } 4\mu + 3,\\
&\ell = -i, \text{ if } h \text{ is of the form } 8\mu + 3 \text{ and } k \text{ is of the form } 4\mu + 3,\\
&\qquad\qquad \text{or if } h \text{ is of the form } 8\mu + 7 \text{ and } k \text{ is of the form } 4\mu + 1,
\end{aligned}$$

With this, the determination of W in those cases where n is a prime number or a power of a prime number is complete. It remains, therefore, to complete those cases in which n is a composite number with several prime factors. The following theorem will pave the way for us here.

Art. 25

Theorem. *Let n be the product of two relatively prime positive integers a and b, and set*

$$P = 1 + r^{aa} + r^{4aa} + r^{9aa} + etc. + r^{(b-1)^2aa}$$

$$Q = 1 + r^{bb} + r^{4bb} + r^{9bb} + etc. + r^{(a-1)^2bb}$$

Then I claim that $W = PQ$.

Proof. Let α indefinitely denote the numbers $0, 1, 2, 3, \ldots, a-1$, let β indefinitely denote the numbers $0, 1, 2, 3, \ldots, b-1$, and let ν indefinitely denote the numbers $0, 1, 2, 3, \ldots, n-1$. It is clear that

$$P = \sum r^{aa\beta\beta}, Q = \sum r^{bb\alpha\alpha}, W = \sum r^{\nu\nu}$$

Hence $PQ = \sum r^{aa\beta\beta+bb\alpha\alpha}$, where all values of α and β are substituted. Hence, furthermore, because $2ab\alpha\beta = 2\alpha\beta n$, we have $PQ = \sum r^{(a\beta+b\alpha)^2}$. But it is seen without difficulty that the individual values of $a\beta+b\alpha$ are distinct from each other, and each is equal to a possible value of ν. Hence $PQ = \sum r^{\nu\nu} = W$. □

It should be noted that r^{aa} is a proper root of the equation $x^b - 1 = 0$, and r^{bb} is a proper root of the equation $x^a - 1 = 0$.

Art. 26

Now let n be the product of three mutually prime numbers a, b, c. Then it is clear that if we set $bc = b'$, then a and b' will be relatively prime. Therefore, W is the product of two factors

$$1 + r^{aa} + r^{4aa} + r^{9aa} + \text{etc.} + r^{(b'-1)^2aa}$$

$$1 + r^{b'b'} + r^{4b'b'} + r^{9b'b'} + \text{etc.} + r^{(a-1)^2b'b'}$$

But since r^{aa} is a proper root of the equation $x^{bc} - 1 = 0$, the first factor will itself be the product of two factors

$$1 + \rho^{bb} + \rho^{4bb} + \rho^{9bb} + \text{etc.} + \rho^{(c-1)^2bb}$$

$$1+\rho^{cc}+\rho^{4cc}+\rho^{9cc}+\text{etc.}+\rho^{(b-1)^2cc}$$

if one sets $r^{aa}=\rho$. Hence it is clear that W is the product of three factors

$$1+r^{bbcc}+r^{4bbcc}+r^{9bbcc}+\text{etc.}+r^{(a-1)^2bbcc}$$

$$1+r^{aacc}+r^{4aacc}+r^{9aacc}+\text{etc.}+r^{(b-1)^2aacc}$$

$$1+r^{aabb}+r^{4aabb}+r^{9aabb}+\text{etc.}+r^{(c-1)^2aabb}$$

where r^{bbcc}, r^{aacc}, r^{aabb} are proper roots of the equations $x^a-1=0$, $x^b-1=0$, $x^c-1=0$, respectively.

Art. 27

From this it is easily concluded that in general, if n is the product of any number of mutually prime factors a, b, c etc., then W will be a product of as many factors

$$1+r^{\frac{nn}{aa}}+r^{\frac{4nn}{aa}}+r^{\frac{9nn}{aa}}+\text{etc.}+r^{\frac{(a-1)^2nn}{aa}}$$

$$1+r^{\frac{nn}{bb}}+r^{\frac{4nn}{bb}}+r^{\frac{9nn}{bb}}+\text{etc.}+r^{\frac{(b-1)^2nn}{bb}}$$

$$1+r^{\frac{nn}{cc}}+r^{\frac{4nn}{cc}}+r^{\frac{9nn}{cc}}+\text{etc.}+r^{\frac{(c-1)^2nn}{cc}}\ \text{etc.}$$

where $r^{\frac{nn}{aa}}, r^{\frac{nn}{bb}}, r^{\frac{nn}{cc}}$ etc. are proper roots of the equations $x^a-1=0$, $x^b-1=0$, $x^c-1=0$, etc.

Art. 28

From these principles the passage to the complete determination of W for any value of n is now readily accessible. Of course, n is decomposed into factors a, b, c etc. which are either distinct prime numbers, or powers of distinct prime numbers. Let $r^{\frac{nn}{aa}}=A$, $r^{\frac{nn}{bb}}=B$, $r^{\frac{nn}{cc}}=C$ etc. Then A, B, C, etc. will be proper roots of the equations $x^a-1=0$, $x^b-1=0$, $x^c-1=0$, etc., and W will be the product of factors

$$1+A+A^4+A^9+\text{etc.}+A^{(a-1)^2}$$

$$1+B+B^4+B^9+\text{etc.}+B^{(b-1)^2}$$

$$1+C+C^4+C^9+\text{etc.}+C^{(c-1)^2}\ \text{etc.}$$

But these individual factors can be determined by what we have explained in articles 20, 21, and 23, from which the value of their product will also be known. It will not be useless to gather here the rules for determining those factors. When the root A is $=\frac{kn}{a}\cdot\frac{360^o}{a}$, the sum $1+A+A^4+A^9+\text{etc.}+A^{(a-1)^2}$, which we shall denote by L, will be determined by the number $\frac{kn}{a}$, as was W by k in our general discussion. We have already distinguished twelve cases:

I. If a is a prime number of the form $4\mu+1$, say $=p$, or the power of such a prime number with an odd exponent, and at the same time $\frac{kn}{a}$ is a quadratic residue modulo p, then $L=+\sqrt{a}$.

II. If $\frac{kn}{a}$ is a quadratic non-residue modulo p, then $L=-\sqrt{a}$.

III. If a is a prime number of the form $4\mu+3$, say $=p$, or a power of such a prime number with an odd exponent, and at the same time $\frac{kn}{a}$ is a quadratic residue modulo p, then $L=+i\sqrt{a}$.

IV. If, with the rest of the assumptions as in III, if $\frac{kn}{a}$ is a quadratic non-residue modulo p, then $L=-i\sqrt{a}$.

V. If a is a square, or a power of an (odd) prime with an even exponent, then $L=+\sqrt{a}$.

VI. If $a=2$, then $L=0$.

VII. If $a = 4$, or a binary power with an even exponent, and at the same time $\frac{kn}{a}$ is of the form $4\mu + 1$, then $L = (1 + i)\sqrt{a}$.

VIII. If, with the rest of the assumptions as in VII, $\frac{kn}{a}$ is of the form $4\mu + 3$, then $L = (1 - i)\sqrt{a}$.

IX. If $a = 8$, or a higher binary power with an odd exponent, and at the same time $\frac{kn}{a}$ is of the form $8\mu + 1$, then $L = (1 + i)\sqrt{a}$.

X. If, with the rest of the assumptions as in IX, $\frac{kn}{a}$ is of the form $8\mu + 3$, then $L = (-1 - i)\sqrt{a}$.

XI. If, with the rest of the assumptions as in IX, $\frac{kn}{a}$ is of the form $8\mu + 5$, then $L = (-1 - i)\sqrt{a}$.

XII. If, with the rest of the assumptions as in IX, $\frac{kn}{a}$ is of the form $8\mu + 7$, then $L = (1 - i)\sqrt{a}$.

Art. 29

Example. Let $n = 2520 = 8.9.5.7$ and take $k = 13$. Here we have

For $a = 8$, by case XII, $L = (1 - i)\sqrt{8}$.

For the factor 9, by case V, the corresponding sum will be $\sqrt{9}$.

For the factor 5, by case II, the corresponding sum will be $-\sqrt{5}$.

For the factor 7, by case III, the corresponding sum will be $+i\sqrt{7}$.

Hence $W = (1 - i)(-i)\sqrt{2520} = (-1 - i)\sqrt{2520}$.
If for the same value of n, we set $k = 1$, then for

the factor 8, the sum is $(-1 + i)\sqrt{8}$

the factor 9, the sum is $\sqrt{9}$

the factor 5, the sum is $\sqrt{5}$

the factor 7, the sum is $-i\sqrt{7}$

Hence the product is $W = (1 + i)\sqrt{2520}$.

Art. 30

Another general method of determining the sum of W is suggested by that which was set forth in articles 22 and 24. Set $\cos\omega + i\sin\omega = \rho$, and

$$\rho^{\frac{nn}{aa}} = \alpha\ ,\ \ \rho^{\frac{nn}{bb}} = \beta\ ,\ \ \rho^{\frac{nn}{cc}} = \gamma \ \text{ etc.}$$

so that we have $r = \rho^k$, $A = \alpha^k$, $B = \beta^k$, $C = \gamma^k$ etc. Then

$$1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(n-1)^2}$$

will be a product of factors

$$1 + \alpha + \alpha^4 + \alpha^9 + \text{etc.} + \alpha^{(a-1)^2}$$
$$1 + \beta + \beta^4 + \beta^9 + \text{etc.} + \beta^{(b-1)^2}$$
$$1 + \gamma + \gamma^4 + \gamma^9 + \text{etc.} + \gamma^{(c-1)^2} \ \text{ etc.}$$

and therefore W will be a product of factors

$$\begin{aligned}
w &= 1 + \rho + \rho^4 + \rho^9 + \text{ etc. } + \rho^{(n-1)^2} \\
\mathfrak{A} &= \frac{1 + A + A^4 + A^9 + \text{ etc. } + A^{(a-1)^2}}{1 + \alpha + \alpha^4 + \alpha^9 + \text{ etc. } + \alpha^{(a-1)^2}} \\
\mathfrak{B} &= \frac{1 + B + B^4 + B^9 + \text{ etc. } + B^{(b-1)^2}}{1 + \beta + \beta^4 + \beta^9 + \text{ etc. } + \beta^{(b-1)^2}} \\
\mathfrak{C} &= \frac{1 + C + C^4 + C^9 + \text{ etc. } + C^{(c-1)^2}}{1 + \gamma + \gamma^4 + \gamma^9 + \text{ etc. } + \gamma^{(c-1)^2}} \text{ etc.}
\end{aligned}$$

Now, the first factor w has been determined by the investigations given above (Art. 19). But the remaining factors $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ etc. come out through the formulas of Art. 22 and Art. 24, which, in order that they may all be held together, we collect here again.[1] There are twelve cases to be distinguished, namely

I. If a is a prime number (odd) $= p$, or a power of such a number with an odd exponent, and k is a quadratic residue modulo p, then the corresponding factor will be $\mathfrak{A} = +1$.

II. If with the rest of the assumptions as in I, k is a quadratic non-residue modulo p, then $\mathfrak{A} = -1$.

III. If a is the square of an odd prime number, or a higher power with an even exponent, then $\mathfrak{A} = 1$.

IV. If a is $= 4$, or a higher binary power with an even exponent, and at the same time k is of the form $4\mu + 1$, then $\mathfrak{A} = +1$.

V. If, with the rest of the assumptions as in IV, k is of the form $4\mu + 3$, and $\frac{n}{a}$ is of the form $4\mu + 1$, then $\mathfrak{A} = +i$.

VI. If, with the rest of the assumptions as in IV, k is of the form $4\mu + 3$, and $\frac{n}{a}$ is of the form $4\mu + 3$, then $\mathfrak{A} = +i$.

VII. If a is $= 8$, or a higher binary power with an odd exponent, and k is of the form $8\mu + 1$, then $\mathfrak{A} = +1$.

VIII. If, with the rest of the assumptions as in VII, k is of the form $8\mu + 5$, then $\mathfrak{A} = -1$.

IX. If, with the rest of the assumptions as in VII, k is of the form $8\mu + 3$, and $\frac{n}{a}$ is of the form $4\mu + 1$, then $\mathfrak{A} = +i$.

X. If, with the rest of the assumptions as in VII, k is of the form $8\mu + 3$, and $\frac{n}{a}$ is of the form $4\mu + 3$, then $\mathfrak{A} = -i$.

XI. If, with the rest of the assumptions as in VII, k is of the form $8\mu + 7$, and $\frac{n}{a}$ is of the form $4\mu + 1$, then $\mathfrak{A} = -i$.

XII. If, with the rest of the assumptions as in VII, k is of the form $8\mu + 7$, and $\frac{n}{a}$ is of the form $4\mu + 3$, then $\mathfrak{A} = +i$.

We pass over the case where $a = 2$, indeed $\mathfrak{A}$ would be $= \frac{0}{0}$ or indeterminate, but then always $W = 0$.

The remaining factors $\mathfrak{B}$, $\mathfrak{C}$ etc. depend in the same way on b, c etc. as does $\mathfrak{A}$ on a.

[1] Obviously, what where there k and h, will here be $\frac{n}{a}$ and k in the second factor, $\frac{n}{b}$ and k in the third factor, etc.

Art. 31

According to this method, the second example of article 29 is as follows:

The factor w becomes $= (1+i)\sqrt{2520}$.

For $a = 8$ the corresponding factor $\mathfrak{A}$ becomes, by case VIII, $= -1$.

The second factor 9 corresponds a factor $+1$ (by case III.)

The factor 5 corresponds to a factor -1 (by case II.)

The factor 7 corresponds to a factor -1 (by case II.)

Hence the product $W = (-1-i)\sqrt{2520}$ is formed, as in Art. 29.

Art. 32

Whereas the value of W may be determined by two methods, the second of which is based on the relations of the numbers $\frac{nk}{a}$, $\frac{nk}{b}$, $\frac{nk}{c}$ etc. to the numbers a, b, c etc., and the other depends on the relations of k to the numbers a, b, c etc., some conditional connection must intervene between all of these relations, so that any one must be determinable from the rest. Suppose that all the numbers a, b, c etc. are odd prime numbers, and take $k = 1$. Let the factors a, b, c be distributed into two classes, the first of which contains those of the form $4\mu + 1$ and who are denoted by p, p', p'' etc., while the other consists of those of the form $4\mu + 3$, and who are expressed by q, q', q'' etc.: we will designate the multitude of the latter by m. With this understood, we observe first that if m is even, then n is of the form $4\mu + 1$ (this includes the case where the factors of the second class are completely absent, or where $m = 0$), and on the other hand if m is odd, then n is of the form $4\mu + 3$. Now the determination of W by the first method is thus accomplished. Let the numbers P, P', P'' etc., Q, Q', Q'', etc. be determined from the relationships between the numbers $\frac{n}{p}$, $\frac{n}{p'}$, $\frac{n}{p''}$ etc., $\frac{n}{q}$, $\frac{n}{q'}$, $\frac{n}{q''}$,etc. and the numbers p, p', p'' etc.,q, q', q'' etc., by setting

$$P = +1, \text{ si } \frac{n}{p} \text{ is a quadratic residue modulo } p$$
$$P = -1, \text{ si } \frac{n}{p} \text{ is a quadratic non-residue modulo p}$$

and likewise for the rest. Then W will be a product of the factors $P\sqrt{p}$, $P'\sqrt{p'}$, $P''\sqrt{p''}$ etc., $iQ\sqrt{q}$, $iQ'\sqrt{q'}$, $iQ''\sqrt{q''}$ etc, and therefore

$$W = PP'P'' \dots QQ'Q'' \cdots^{m} \sqrt{n}$$

By the second method, or rather immediately by the precepts of Art. 19, one has

$$W = +\sqrt{n}, \text{ if } n \text{ is of the form} 4\mu + 1, \text{or what is the same, if } m \text{ is even}$$

$$W = +i\sqrt{n}, \text{ if } n \text{ is of the form} 4\mu + 3, \text{or if } m \text{ is odd}$$

Both cases may be included together by the following formula:

$$W = i^{mm}\sqrt{n}$$

Hence it follows that

$$PP'P'' \dots QQ'Q'' \cdots = i^{mm-m}$$

But $i^{mm-m} = 1$ whenever m is of the form 4μ or $4\mu + 1$, and -1 whenever m is of the form $4\mu + 2$ or $4\mu + 3$, from which we deduce the following very elegant

Theorem. *Let a, b, c be distinct, odd, positive primes, whose product is $= n$. Among these assume that m are of the form $4\mu + 3$, and the rest are of the form $4\mu + 1$. Then the multitude of those numbers among a, b, c etc. such that $\frac{n}{a}$, $\frac{n}{b}$, $\frac{n}{c}$ respectively are quadratic nonresidues, will be even whenever m is of the form 4μ or $4\mu + 1$, but odd whenever m is of the form $4\mu + 2$ or $4\mu + 3$.*

Example. By setting $a = 3$, $b = 5$, $c = 7$, $d = 11$, we have three numbers of the form $4\mu + 3$, namely 3, 7, antd 11, and we have $5.7.11R3$, $3.7.11R5$, $3.5.11R7$, $3.5.7N11$, thus there is a unique $\frac{n}{d}$ which is a quadratic non-residue modulo d.

Art. 33

The celebrated *fundamental theorem* on quadratic residues is nothing but a special case of the theorem just developed. By limiting, of course, the population of the numbers a, b, c, etc. to two, it is clear that if only one of them, or neither of them, is of the form $4\mu + 3$, then we must have simultaneously aRb and bRa, or simultaneously aNb, bNa. On the other hand, if both are of the form $4\mu + 3$, then one of them must be a quadratic non-residue of the other, and the other a quadratic residue of that one. And so the fourth demonstration has been given for this most important theorem, the first and second demonstration of which we have recently given in Disquisitiones Arithmeticae, and the third in a special commentary (*Commentt. T. XVI*). We will give two other demonstrations based on completely different principles in the future. It is exceedingly surprising that this most beautiful theorem, which at first so obstinately eluded all attempts, could be approached later by methods so very distant from one other.

Art. 34

Even the rest of the theorems, which act as a supplement to the fundamental theorem, that is, by which the prime numbers for which -1, 2, and -2 are quadratic residues or non-residues may be identified, can be derived from the same principles. Let us start with the residue $+2$.

Set $n = 8a$, where a is a prime number, and let $k = 1$. Then by the method of Art. 28, W will be the product of two factors, one of which will be either $+\sqrt{a}$ or $+i\sqrt{a}$ if 8, or equivalently 2, is a quadratic residue modulo a; or else $-\sqrt{a}$ or $-i\sqrt{a}$, if 2 is a quadratic non-residue modulo a. But the second factor is

$$\begin{gathered}(1+i)\sqrt{8}, \text{ if } a \text{ is of the form } 8\mu+1\\ (-1+i)\sqrt{8}, \text{ if } a \text{ is of the form } 8\mu+3\\ (-1-i)\sqrt{8}, \text{ if } a \text{ is of the form } 8\mu+5\\ (1-i)\sqrt{8}, \text{ if } a \text{ is of the form } 8\mu+7\end{gathered}$$

and by Art. 18 we will always have $W = (1+i)\sqrt{n}$. Dividing this value by the four values of the second factor, it is clear that the first factor must be

$$\begin{gathered}+\sqrt{a}, \text{ if } a \text{ is of the form } 8\mu+1\\ -i\sqrt{a}, \text{ if } a \text{ is of the form } 8\mu+3\\ -\sqrt{a}, \text{ if } a \text{ is of the form } 8\mu+5\\ +i\sqrt{a}, \text{ if } a \text{ is of the form } 8\mu+7\end{gathered}$$

From this it follows automatically, that in the first and fourth cases 2 is a quadratic residue modulo a, and in the second and third cases it is a quadratic non-residue.

Art. 35

Prime numbers for which -1 is a quadratic residue or non-residue are easily recognized with the help of the following theorem, which is also quite memorable by itself.

Theorem. *The product of the two factors*

$$\begin{aligned} W' &= 1 + r^{-1} + r^{-4} + \textit{etc.} + r^{-(n-1)^2} \\ W &= 1 + r + r^4 + \textit{etc.} + r^{(n-1)^2} \end{aligned}$$

is $= n$*, if* n *is odd, or* $= 0$ *if* n *is oddly even, or* $= 2n$ *if* n *is evenly even.*

Proof. Since it is quite clear that

$$\begin{aligned} W &= r + r^4 + r^9 + \text{etc.} + r^{nn} \\ &= r^4 + r^9 + \text{etc.} + r^{(n+1)^2} \\ &= r^9 + \text{etc.} + r^{(n+2)^2} \text{ etc.} \end{aligned}$$

the product WW' can also be presented as

$$\begin{aligned} &1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2} \\ &+r^{-1}\left(r + r^4 + r^9 + r^{16} + \text{etc.} + r^{nn}\right) \\ &+r^{-4}\left(r^4 + r^9 + r^{16} + r^{25} + \text{etc.} + r^{(n+1)^2}\right) \\ &+r^{-9}\left(r^9 + r^{16} + r^{25} + r^{36} + \text{etc.} + r^{(n+2)^2}\right) \\ &\text{etc.} \\ &+r^{-(n-1)^2}\left(r^{(n-1)^2} + r^{nn} + r^{(n+1)^2} + r^{(n+2)^2} + \text{etc.} + r^{(2n-2)^2}\right) \end{aligned}$$

and aggregating the sum vertically produces

$$\begin{aligned} &n \\ &+r\left(1 + rr + r^4 + r^6 + \text{etc.} + r^{2n-2}\right) \\ &+r^4\left(1 + r^4 + r^8 + r^{12} + \text{etc.} + r^{4n-4}\right) \\ &+r^9\left(1 + r^6 + r^{12} + r^{18} + \text{etc.} + r^{6n-6}\right) \\ &\text{etc.} \\ &+r^{(n-1)^2}\left(1 + r^{2n-2} + r^{4n-4} + r^{6n-6} + \text{etc.} + r^{2(n-1)^2}\right) \end{aligned}$$

Now if n is odd, each part of this aggregate, except the first n, will be $= 0$. For the second manifestly becomes $\frac{r(1-r^{2n})}{1-rr}$, the third $\frac{r^4(1-r^{4n})}{1-r^4}$ etc. When n is even, it is necessary to study the term

$$r^{\frac{1}{4}nn}\left(1 + r^n + r^{2n} + r^{3n} + \text{etc.} + r^{nn-n}\right)$$

which becomes $= nr^{\frac{1}{4}nn}$. In the former case we therefore obtain $WW' = n$, but in the latter $WW' = n + nr^{\frac{1}{4}nn}$. But $r^{\frac{1}{4}nn}$ becomes $= +1$ if n is evenly even, and thus $WW' = 2n$. On the other hand, if n is oddly even then $r^{\frac{1}{4}nn} = -1$, and thus $WW' = 0$. □

Art. 36

Already from Art. 22 it is clear that if m is an odd prime number, then $\frac{W'}{W}$ will be $= +1$ or -1 according as -1 is a quadratic residue or non-residue modulo n. Hence in the former case we must have $W^2 = n$ and in the latter $W^2 = -n$. From this, by Art. 13, we conclude that the former case can only take place when n is of the form $4\mu + 1$ and the latter case when n is of the form $4\mu + 3$.

Finally, by the combination of the conditions found for the residues $+2$ and -1, it naturally follows that -2 is a quadratic residue of any prime number of the form $8\mu + 1$ or $8\mu + 3$, and a quadratic non-residue of any prime number of the form $8\mu + 5$ or $8\mu + 7$.