and thus Weingarten's symbols, $\left\{ \begin{smallmatrix} 11 \\ 1 \end{smallmatrix} \right\}$, &c., have the values

$$\left\{ \begin{smallmatrix} 11 \\ 1 \end{smallmatrix} \right\} = \frac{1}{a} \left[a_{12} \left(-\frac{da_{12}}{dp} + \frac{1}{2} \frac{da_{11}}{dq} \right) + a_{22} \left(\frac{1}{2} \frac{da_{11}}{dp} \right) \right],$$

$$\left\{ \begin{smallmatrix} 12 \\ 1 \end{smallmatrix} \right\} = \frac{1}{a} \left[a_{12} \left(-\frac{1}{2} \frac{da_{22}}{dp} \right) + a_{22} \left(\frac{1}{2} \frac{da_{11}}{dq} \right) \right],$$

$$\left\{ \begin{smallmatrix} 22 \\ 1 \end{smallmatrix} \right\} = \frac{1}{a} \left[a_{12} \left(-\frac{1}{2} \frac{da_{22}}{dq} \right) + a_{22} \left(\frac{da_{12}}{dq} - \frac{1}{2} \frac{da_{22}}{dp} \right) \right],$$

$$\left\{ \begin{smallmatrix} 11 \\ 2 \end{smallmatrix} \right\} = \frac{1}{a} \left[a_{12} \left(-\frac{1}{2} \frac{da_{11}}{dp} \right) + a_{11} \left(\frac{da_{12}}{dp} - \frac{1}{2} \frac{da_{11}}{dq} \right) \right],$$

$$\left\{ \begin{smallmatrix} 12 \\ 2 \end{smallmatrix} \right\} = \frac{1}{a} \left[a_{12} \left(-\frac{1}{2} \frac{da_{11}}{dq} \right) + a_{11} \left(\frac{1}{2} \frac{da_{22}}{dp} \right) \right],$$

$$\left\{ \begin{smallmatrix} 22 \\ 2 \end{smallmatrix} \right\} = \frac{1}{a} \left[a_{12} \left(-\frac{da_{12}}{dq} + \frac{1}{2} \frac{da_{22}}{dp} \right) + a_{11} \left(\frac{1}{2} \frac{da_{22}}{dq} \right) \right],$$

values which give, as they should do,

$$\left\{ \begin{smallmatrix} 11 \\ 1 \end{smallmatrix} \right\} + \left\{ \begin{smallmatrix} 12 \\ 2 \end{smallmatrix} \right\} = \frac{1}{\sqrt{a}} \frac{d\sqrt{a}}{dp}, \quad \text{and} \quad \left\{ \begin{smallmatrix} 12 \\ 1 \end{smallmatrix} \right\} + \left\{ \begin{smallmatrix} 22 \\ 2 \end{smallmatrix} \right\} = \frac{1}{\sqrt{a}} \frac{d\sqrt{a}}{dq}.$$

The foregoing comparison serves to explain the notation of Weingarten's valuable memoir.

On Complex Primes formed with the Fifth Roots of Unity.

By H. W. LLOYD TANNER. Read March 9th, 1893.

Abstract.

The object of this paper is to explain a method of calculating complex prime factors of real primes included in the form $10\mu + 1$. The only published method which I have met with is due to Kummer. This is not restricted to the particular case here considered; but, as it involves the determination of the G.C.M. of two complex numbers, it is probably more laborious than the method now communicated. The method adopted by Reuschle in the calculation of his Tables does not appear to have been published. The present process is based on the indeterminate equation

$$X^2 - 5Y^2 = 4p.$$

A minimum solution of this equation gives the "simplest" prime factor according to Kummer's definition (*Berlin Monatsberichte*, 1870, p. 413), and solutions in which Y is a multiple of 5 give the "primary" prime factors, which Kummer found it necessary to use in order to establish the general law of reciprocity. In solving the equation Lagrange's method turns out to be impracticable, and a short discussion—treated graphically—is introduced, which is sufficient to show the relations between the different solutions. These relations can be expressed in the form

$$\left(\begin{smallmatrix} 2, & 0 \\ 0, & 2 \end{smallmatrix} \right) (X, Y) = \left(\begin{smallmatrix} a, & 5b \\ b, & a \end{smallmatrix} \right) (X', Y'),$$

and it is interesting to note the intimate connection between these matrices and the complex units. From any solution (X, Y) three numbers A_0, A_1, A_2 are found, A_0 being the integer next greater than $2X/5$; and these serve to determine the values and sequence of the coordinates a_0, a_1 , &c., in the required prime factor

$$a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 + a_4\omega^4.$$

The values of a have to satisfy certain conditions, some of which are tested by mere inspection. To give some idea of the facility of the method from the calculator's point of view, it may be stated that the determination of the prime factors of two primes selected at random in the second million (viz., 1562051 and 1671781) was completed in three hours. The only auxiliary table required is a table of squares, and if this extends to the square of 7000 it will suffice for the factorization of all primes in the first nine millions. Tables are appended giving the simplest—and simplest primary—prime factors of all suitable primes less than 10000. The reciprocal factors are also given after the first thousand. For the first thousand the reciprocal factors have already been published, and, instead of giving these again, a comparison is indicated between the factors here given and those published in Renschle's Tables. The result of the comparison suggests that Renschle's method of calculation was not the same as that now communicated.

My thanks are again due to my colleague, Mr. Pinkerton, for much and valuable help.

Preliminary Explanations (Arts. 1-4).

1. Let ω be an imaginary fifth root of unity, so that

$$\Omega = 1 + \omega + \omega^2 + \omega^3 + \omega^4$$

is the complex zero. If a_0, a_1, a_2, a_3, a_4 represent any real integers

(coordinates), the expression

$$a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 + a_4\omega^4$$

is a complex integer. This may be indicated by $a\omega$, where a is a functional symbol, so that

$$a\omega^h = a_0 + a_1\omega^h + a_2\omega^{2h} + a_3\omega^{3h} + a_4\omega^{4h}.$$

The norm of $a\omega$,

$$= N.a\omega = a\omega . a\omega^2 . a\omega^4 . a\omega^3,$$

is a real integer; and the chief object of the present paper is to determine the coordinates so that this norm may be equal to a given prime p of the form $10\mu + 1$.

2. A complex integer, $a\omega$, may be changed in three distinct ways without changing the norm.

(i.) The addition of $j\Omega$, where j is any real integer, positive or negative, increases each of the coordinates by j ; but the norm, which is a function of the differences of the coordinates, is not changed.

(ii.) If ω be replaced by ω^h ($h = 1, 2, 3, 4$), the factors in the norm are merely rearranged.

(iii.) The norm is unchanged if $a\omega$ be multiplied by a complex unit; viz., by a complex integer ua such that $N.ua = 1$. These units are of three kinds: the real units ± 1 ; the simple units, ω^k ($k = 0, 1, 2, 3, 4$), and powers of the cyclotomic unit (Kummer's *Kreistheilungseinheit*) $(\omega + \omega^{-1})^i$, where i is any positive or negative integer. It is known that, for the fifth roots of unity, every unit can be expressed as a product of integral powers of these units. We shall frequently write e or e_1 for $\omega + \omega^{-1}$, and e_2 for $\omega^2 + \omega^{-2}$; and

$$\text{since} \quad e_1 . e_2 = (\omega + \omega^{-1})(\omega^2 + \omega^{-2}) = -1,$$

any negative power of e_1 may be replaced by the corresponding positive power of e_2 .

3. It appears, then, that all the complex numbers included in the formula

$$\pm e^i . \omega^k . a\omega^h + j\Omega$$

have the same norm as $a\omega$; and, if the norm is a real prime, the converse is also true. The formula represents a doubly infinite series, for i, j may have any integral values, positive or negative; each term of the series gives 20 arrangements of the coordinates,

since h may have any one of the four values 1, 2, 3, 4, and k is 0, 1, 2, 3, or 4. Finally, the sign of the complex integer may be reversed.

An obvious corollary is that, if the five coordinates of a complex integer are given, without any indication of the sequence, it will, in general, be possible to form 6 complex integers which have different norms. There are, in fact, 120 arrangements of the five coordinates, and these belong in twenties to co-normal integers. Exceptions occur if there are equal coordinates.

4. The discussion which follows enables us to select a particular prime factor of p (the values of h, k, i, j being determinate) as a representative of the whole series, and to determine this representative factor, either directly, by calculating its coordinates, or by derivation from any given prime factor of p .

For this purpose, three auxiliary functions are used—the coordinate-sum, the half-norm, and the reciprocal factors of p .

The coordinate-sum fixes the value of j and the sign. (Art. 5.)

The half-norm fixes the value of i , and furnishes a means of calculating the coordinates a . (Arts. 6, *sqq.*)

The reciprocal factors determine h, k (except that, for certain values of p , the sign of h is left indeterminate), and give further means of lessening the labour. (Arts. 27, *sqq.*)

The Coordinate-Sum (Art. 5).

5. The sum of the coordinates of $a\omega$, namely,

$$a(1) = a_0 + a_1 + a_2 + a_3 + a_4,$$

will be denoted by the letter s . When $a\omega$ is changed to $a\omega + j\Omega$, s becomes $s + 5j$. Hence, by properly choosing j , we can make the new $s = 0, \pm 1, \pm 2$. The case $s = 0$ is excluded from consideration; for, if $s = 0$, $a\omega$ is divisible by $1 - \omega$, and therefore $N a\omega$ is divisible by $N(1 - \omega)$, which is 5. The other cases are reduced to two, viz., $s = 1, s = 2$, since we are at liberty to change the sign of $a\omega$.

The coordinate-sum of $\epsilon^i a\omega$ or of $\epsilon^i_2 a\omega$, when i is a positive integer, is $2^i s$, for the coordinate-sum of any product is the product of the coordinate-sums of the factors. By using this it is possible, in an infinite number of ways, to make the new $s = 2$ (or any other selected value except 0 or a multiple of 5). There are advantages in adopting this course, but they are more than counterbalanced by the disadvantage that larger numbers are introduced into the calculations than if we allow the reduced s to be either 1 or 2. It will, therefore, be taken that the coordinate-sum of the standard prime

factor is either 1 or 2. If a standard factor has its coordinate-sum equal to 1, factors with coordinate-sum 2 can at once be found by multiplication into ϵ_1 or ϵ_2 .

When $a\omega$ is changed to $a\omega + j\Omega$, s^2 becomes $s^2 + 10js + 25j^2$.

The Half-Norm (Arts. 6-9).

6. The product $a\omega \cdot a\omega^{-1}$ is a normal product (since ω, ω^{-1} make up a period), and will be called the half-norm.

We have

$$a\omega \cdot a\omega^{-1} = A_0 + A_1(\omega + \omega^{-1}) + A_2(\omega^2 + \omega^{-2}),$$

where

$$A_0 = a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2,$$

$$A_1 = a_0a_1 + a_1a_2 + a_2a_3 + a_3a_4 + a_4a_0,$$

$$A_2 = a_0a_2 + a_2a_4 + a_4a_1 + a_1a_3 + a_3a_0.$$

The subscripts to the A thus denote the minimum difference, mod. 5, between the subscripts of the factors in the several terms. A_0 is the "square-sum," and A_1, A_2 are the "product-sums" of $a\omega$.

7. A_0 is not altered by a change of ω ; A_1, A_2 are interchanged if ω is replaced by ω^2 or ω^3 , but are not changed if ω^{-1} is put for ω . Neither of the A is affected when $a\omega$ is changed to $\pm \omega^k \cdot a\omega$.

8. When $a\omega$ becomes $\epsilon^i \cdot a\omega$, the A change. To determine the new A , we consider the more general case in which $a\omega$ becomes $a\omega \cdot b\omega$; $b\omega$ being another complex integer whose square-sum and product-sums are B_0, B_1, B_2 . Denoting by A'_0, A'_1, A'_2 the corresponding functions for the product $a\omega \cdot b\omega$, we shall have

$$A'_0 = A_0B_0 + 2A_1B_1 + 2A_2B_2,$$

$$A'_1 = A_0B_1 + A_1(B_0 + B_2) + A_2(B_1 + B_2),$$

$$A'_2 = A_0B_2 + A_1(B_1 + B_2) + A_2(B_0 + B_1).$$

It will suffice to prove the second of these. A similar process will serve to establish the others.

We have

$$a\omega \cdot b\omega = \sum a_i b_{-i} + \omega \sum a_i b_{1-i} + \omega^2 \sum a_i b_{2-i} + \omega^3 \sum a_i b_{3-i} + \omega^4 \sum a_i b_{4-i},$$

where each Σ includes the five terms for which $i = 0, 1, 2, 3, 4$. Hence

$$A'_1 = \sum_h \left\{ \sum_i a_i b_{h-i} \times \sum_j a_j b_{h+1-j} \right\}; \quad h, i, j = 0, 1, 2, 3, 4.$$

Now, considering any one value i , the values of j are i , $i \pm 1$, $i \pm 2$.

$$\begin{aligned} \therefore A'_i &= \sum_h \sum_i \{ a_i^2 b_{h-i} b_{h+1-i} + a_i a_{i+1} b_{h-i} b_{h-i} + a_i a_{i-1} b_{h-i} b_{h-i+2} \\ &\quad + a_i a_{i+2} b_{h-i} b_{h-i-1} + a_i a_{i-2} b_{h-i} b_{h-i+3} \} \\ &= \sum_i \{ a_i^2 B_1 + a_i a_{i+1} B_0 + a_i a_{i-1} B_2 + a_i a_{i+2} B_1 + a_i a_{i-2} B_3 \} \\ &= A_0 B_1 + A_1 B_0 + A_1 B_2 + A_2 B_1 + A_2 B_3, \end{aligned}$$

which is the equation to be proved.

In particular, taking $b\omega$ to be $\epsilon_1 = \omega + \omega^4$, we have $B_0 = 2$, $B_1 = 0$, $B_2 = 1$, so that

$$\begin{aligned} A'_0 &= 2A_0 && + 2A_2, \\ A'_1 &= && + 3A_1 + A_2, \\ A'_2 &= A_0 + A_1 + 2A_2. \end{aligned}$$

9. If $a\omega$ becomes $a\omega + j\Omega$, the increments of A_0 , A_1 , A_2 are equal, viz., each is increased by $2sj + 5j^2$. The increment of s^2 (Art. 5) is five times as large. Hence the expressions

$$5A_0 - s^2, \quad A_2 - A_1, \quad A_0 - A_1, \quad A_0 - A_2, \quad A_0 + 2A_1 + 2A_2 - s^2$$

are independent of j . The last is, in fact, zero, for

$$s^2 = A_0 + 2A_1 + 2A_2.$$

The first two are fundamental in the theory, and are denoted by $2X$, Y , namely,

$$\begin{aligned} 2X &= 5A_0 - s^2, &= 4A_0 - 2A_1 - 2A_2, \\ Y &= A_2 - A_1. \end{aligned}$$

From which we obtain

$$\begin{aligned} 10A_0 &= 4X && + 2s^2, \\ 10A_1 &= -X - 5Y + 2s^2, \\ 10A_2 &= -X + 5Y + 2s^2. \end{aligned}$$

Concerning X and Y (Arts. 10-24).

10. We have, hence,

$$\begin{aligned} A_0 - A_1 &= \frac{1}{2} (X + Y), \\ A_0 - A_2 &= \frac{1}{2} (X - Y). \end{aligned}$$

Now,

$$\begin{aligned}
 p &= N \cdot a\omega = \{A_0 + A_1(\omega + \omega^{-1}) + A_2(\omega^3 + \omega^{-2})\} \\
 &\quad \times \{A_0 + A_1(\omega^2 + \omega^{-2}) + A_2(\omega + \omega^{-1})\} \\
 &= (A_0 - A_1)(A_0 - A_2) - (A_1 - A_2)^2 \\
 &= \frac{1}{4}(X + Y)(X - Y) - Y^2; \\
 \therefore 4p &= X^2 - 5Y^2.
 \end{aligned}$$

11. The quantity X is essentially positive, for $2X$ is the sum of ten squares, viz.,

$$2X = \sum (a_i - a_j)^2, \quad i = 0, 1, 2, 3, \quad j = i + 1, \dots, 4,$$

as is at once verified by substituting for the A , in the definition of $2X$, their values given in Art. 6.

It appears, from the definition of Y , that it may be either positive or negative; in fact, the sign of Y is changed when $a\omega$ is changed to $a\omega^2$ or $a\omega^3$. The only other change of $a\omega$ that affects Y , and the only change that affects X , is multiplication by a cyclotomic unit. This we proceed to discuss.

12. Suppose that, when $a\omega$ is replaced by $a\omega \cdot b\omega$, X, Y become X', Y' . Then we have, using the notation and results of Art. 8,

$$\begin{aligned}
 2X' &= 4A'_0 - 2A'_1 - 2A'_2 \\
 &= 2A_0(2B_0 - B_1 - B_2) - 2A_1(B_0 - 3B_1 + 2B_2) \\
 &\quad - 2A_2(B_0 + 2B_1 - 3B_2) \\
 &= (2B_0 - B_1 - B_2)X + 5(B_2 - B_1)Y; \\
 2Y' &= 2A'_2 - 2A'_1 \\
 &= 2A_0(B_2 - B_1) + 2A_1(B_1 - B_0) + 2A_2(B_2 - B_0) \\
 &= (B_2 - B_1)X + (2B_0 - B_1 - B_2)Y.
 \end{aligned}$$

These results are conveniently combined in the matrical equation

$$\begin{pmatrix} 2, & 0 \\ 0, & 2 \end{pmatrix} \begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} 2B_0 - B_1 - B_2, & 5(B_2 - B_1) \\ B_2 - B_1, & 2B_0 - B_1 - B_2 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

The terms of the matrix on the right (if we disregard the coefficient 5) are related to $b\omega$ in the same way as X, Y are related to $a\omega$. In particular, they are changed when $b\omega$ is multiplied by ϵ^i . The sign of $B_2 - B_1$ is reversed when $b\omega$ is changed to $b\omega^2$ or $b\omega^3$; but they are not affected by any other change of $b\omega$ which leaves $Nb\omega$ the same.

13. When $b\omega = \epsilon = \omega + \omega^{-1}$, $B_0 = 2$, $B_1 = 0$, $B_2 = 1$. Thus

$$\left(\begin{smallmatrix} 2, & 0 \\ 0, & 2 \end{smallmatrix} \chi X_1, Y_1 \right) = \left(\begin{smallmatrix} 3, & 5 \\ 1, & 3 \end{smallmatrix} \chi X, Y \right).$$

When $b\omega = \epsilon_2$, we find, in like manner (or by using the remark at the end of the preceding article), that

$$\left(\begin{smallmatrix} 2, & 0 \\ 0, & 2 \end{smallmatrix} \chi X_{-1}, Y_{-1} \right) = \left(\begin{smallmatrix} 3, & -5 \\ -1, & 3 \end{smallmatrix} \chi X, Y \right).$$

In general, if $a\omega$ be changed to $\epsilon^i \cdot a\omega$, and (X, Y) become X_i, Y_i , we have

$$(X_i, Y_i) = M^i(X, Y),$$

where

$$M = \begin{pmatrix} 3/2, & 5/2 \\ 1/2, & 3/2 \end{pmatrix}.$$

14. If X, Y satisfy the equation

$$X^2 - 5Y^2 = 4p,$$

then X_i, Y_i also satisfy the equation. For, as in Art. 10,

$$X_i^2 - 5Y_i^2 = 4N(\epsilon^i a\omega) = 4Naw = 4p.$$

Moreover, if X, Y are integers, so likewise are X_i, Y_i . For, from the equation, it follows that X, Y , if integral, are both even or both odd. Therefore $X_{\pm 1}, Y_{\pm 1}$, which are equal to $\frac{1}{2}(3X \pm 5Y)$, $\frac{1}{2}(\pm X + 3Y)$, are integers. It follows, by the method called induction, that X_i, Y_i are integral, where i is any positive or negative integer.

15. The discussion will be simplified by considering X_i, Y_i as the coordinates of a point P_i upon the hyperbola

$$X^2 - 5Y^2 = 4p,$$

or, rather, since X_i is positive, upon the positive branch of this

hyperbola. It is convenient to speak of the system of points P_i [namely, the points whose coordinates are $M^i(X, Y)$ where i is integral] as the range P_i . Two ranges, P_i, Q_i , which have a point in common, are clearly identical. It will now be shown that, when two ranges are not identical, the points of each are separated by the points of the other; or, what is the same thing, there cannot be two points of one range between two consecutive points of the other.

To prove this we note that, O being the origin of coordinates, the area of the triangle OPP_1

$$\begin{aligned} &= \frac{1}{2} (XY_1 - X_1Y) \\ &= \frac{1}{2} \{X(X+3Y) - (3X+5Y)Y\} \\ &= \frac{1}{2} (X^2 - 5Y^2) \\ &= p. \end{aligned}$$

Since this area is positive, it follows that the displacement from P to P_1 along the curve is always in the same sense (indicated by an arrow-head in the figure). Also

$$\Delta OPP_1 > \Delta OPP_1 + \Delta OP_1P_2 > 2p,$$

and, generally,

$$\Delta OPP_i > ip.*$$

On the other hand, if R, S be points between two consecutive points Q, Q_1 of a range, the triangle ORS (taken so as to give a positive area) is included in the triangle OQQ_1 , and its area is less than p . Hence R, S cannot belong to one range; we cannot have, for example, two points of the range P_i between two consecutive points of the range Q_i , nor two points of the range Q_i between two consecutive points of the range P_i ; in other words, the points of any range P_i are separated by those of any other range Q_i .

It follows that an arc terminated by two consecutive points—say Q, Q_1 —of any range contains just one point of every range on the curve.†

* In this inequality, the integer i is positive; but this merely fixes the sequence of the points P, P_i .

† A well-known example of the dynamics of a particle illustrates this result so aptly that I venture to quote it. It is easy to verify that the area of the sector OPP_1 , like that of the triangle, is independent of the position of P . The curve, therefore, is the orbit of a particle moving under repulsion from O varying directly as the distance; and the time of passing from any point to the consecutive point in the same range is constant. Take this as the unit of time. Then a point Q belongs to a range P_i or not, according as the time from P to Q is or is not an integral number of units. If the particle reaches Q t units of time after passing P , it will reach Q_1 $t+1$ units of time from the moment of passing P . If, then, t is integral, Q, Q_1 belong to the range P_i ; but, if t is not integral, then, as there is just one integer between t and $t+1$, there is just one point of the range P_i between Q and Q_1 .

16. Now in Art. 14 it was shown that, if a range contains an integer-point—that is to say, a point the coordinates of which are integral—then all the points on the range are integer-points. Art. 15 shows that, to detect all the integer-ranges on the curve, it is sufficient to determine the integer-points on an arc QQ_1 . The particular arc which is suggested by considerations of symmetry and of ease in calculation, is that shown in the figure, namely, the arc which is bisected by the vertex. In this case, the coordinates of Q , Q_{-1} are $\sqrt{5p}$, $\pm\sqrt{p/5}$. The solutions within these limits—say “reduced” solutions—may be recognized by the value of X being between $2\sqrt{p}$ and $\sqrt{5p}$; or, more conveniently, by the condition that both the expressions $X \pm 5Y$ are positive, while, for every unreduced solution, one is positive and the other negative. From the formulæ at the end of Art. 9 it will be seen that, for a reduced solution with $s = 1$ or 2 , neither of the product-sums A_1 , A_2 is positive; for all other solutions, one of the product-sums is positive.

17. It is easy to see the operations by which, from an unreduced solution—or from a prime factor of p , $a\omega$, which gives an unreduced solution—we can form the reduced solution and the corresponding prime factor. If the Y of the given solution is positive (so that the positive product-sum is A_2), the integer point P must be moved backwards to bring it nearer to the vertex. Hence we must act upon (X, Y) with the matrix M^{-1} , repeated if necessary; and the given prime factor $a\omega$ must be multiplied by $\epsilon_2 (= \omega^2 + \omega^{-2})$ to the same extent. When the Y is negative (so that A_1 is the positive product-sum), the matrix M and the unit $\epsilon (= \omega + \omega^{-1})$ are to be used, because the point P has to move forwards to approach the vertex.

In the *Berlin Monatsberichte* for June, 1870, Kummer has given, as a criterion for the simplest form of complex numbers, that X must be a minimum. The “reduced” solutions, therefore, give the simplest prime factors of p , and thus become of considerable importance.

18. In general, it happens that a reduced solution is the first that presents itself. The following is an example of how other cases arise. $\omega^3 + 2\omega^4$ is given by Reuschle as a “simple” prime factor of 11. Bringing this to the proper coordinate-sum (Art. 5), it becomes $1 + \omega + \omega^3 - \omega^4$, which gives $A_0 = 4$, $A_1 = -1$, $A_2 = 1$; so that $X = 8$, $Y = 2$. Now, 8, 2 satisfy the equation

$$X^2 - 5Y^2 = 4p = 44,$$

but they are not "reduced," because $8-5 \times 2$ is negative, and the prime factor is not a "simplest" prime factor. Taking the Y to be positive, we form the solution

$$X_{-1}, Y_{-1} = M^{-1}(X, Y) = (7, -1),$$

which is reduced. The prime factor is replaced by

$$(\omega^3 + \omega^{-3})(1 + \omega + \omega^3 - \omega^4) = 1 + 2\omega^3 + \omega^4;$$

and, reducing this to its proper coordinate-sum, by subtracting it from Ω , it becomes

$$\omega + \omega^2 - \omega^3,$$

which is one of the "simplest" prime factors of p .*

19. The outcome of the preceding Articles (5-18) is that, from the general form

$$\pm \epsilon^i \cdot \omega^k \cdot a\omega^h + j\Omega$$

of the complex integers whose norm is p , we have selected one in which the ambiguous signs and i, j are fixed. Before completing the specification of the standard form, it will be convenient to recall Kummer's definition of a primary number, and then indicate how, from a simplest prime factor of p , a primary prime factor can be determined.

Primary Prime Factors (Art. 20).

20. A primary number $a\omega$ is defined by Kummer as one that satisfies the two congruences

$$a\omega \cdot a\omega^{-1} \equiv a(1) \cdot a(1), \text{ mod } \lambda,$$

$$a\omega \equiv a(1), \text{ mod } (1-\omega)^2.$$

* It may be remarked that the simplest prime factors are not necessarily the easiest to work with. In particular, if three of the coordinates of $a\omega$ are zero, multiplications become much less laborious than if a simpler form be used in which this is not the case. The real primes which have binomial prime factors are of the form $(a^5 + b^5)/(a + b)$, where b is positive or negative, and the prime factors are of the form $a\omega^i + b\omega^m$. Of the 305 primes less than 10,000, only 23 are of this form. Six binomial factors occur as simplest or primary factors in the appended tables—*e.g.*, $p = 31, 461$. Twelve more occur in the tables with three equal coordinates, so that the binomial form is obtained directly by subtracting a proper multiple of Ω . For instance, $p = 61, 421$. The five other primes with binomial factors are here given. The relation of the binomial factor to the simplest factor ($a\omega$) of the tables is indicated in the last line, where ϵ_2 means $\omega^2 + \omega^{-2}$.

p	$= 11,$	$181,$	$1621,$	$4621,$	$9931;$
binomial	$\left\{ \begin{array}{l} \omega + 2\omega^2, \\ -\epsilon_2 a\omega + \Omega, \end{array} \right.$	$\left\{ \begin{array}{l} 4\omega + 3\omega^2, \\ \epsilon_2 a\omega + \Omega, \end{array} \right.$	$\left\{ \begin{array}{l} 7\omega + 4\omega^2, \\ -\epsilon_2 a\omega + 3\Omega, \end{array} \right.$	$\left\{ \begin{array}{l} 9\omega^2 + 4\omega^3, \\ -\epsilon_2 a\omega + 3\Omega, \end{array} \right.$	$\left\{ \begin{array}{l} 6\omega^2 + 11\omega^3, \\ \epsilon_2 a\omega + 3\Omega. \end{array} \right.$
factor					

In the present case, when we are using 5th roots of unity, λ is 5. The first congruence in the notation of Art. 6 becomes

$$A_1 (\omega + \omega^4 - 2) + A_2 (\omega^2 + \omega^3 - 2) \equiv 0, *$$

which may be written

$$A_1 (\omega + \omega^4 + \omega^2 + \omega^3 - 4) + (A_2 - A_1) (\omega^2 + \omega^3 - 2) \equiv 0.$$

Now

$$\omega + \omega^4 + \omega^2 + \omega^3 - 4 = -5,$$

and $\omega^2 + \omega^3 - 2$ is not a multiple of 5. Hence Kummer's first condition is equivalent to

$$A_2 - A_1 \equiv 0, \text{ mod } 5,$$

that is to say

$$Y \equiv 0, \text{ mod } 5.$$

The second congruence merely fixes the absolute term in $a\omega$; and is in nowise peculiar to primary numbers. It will be considered later (Art. 25). In the meantime we proceed to investigate the residues of X , Y , when the modulus is a power of 5, and when the modulus is 4.

Residues of X , Y , for various Moduli (Arts. 21-24).

21. From the equation

$$X^2 - 5Y^2 = 4p,$$

we have at once, since

$$p = 10\mu + 1,$$

$$X^2 \equiv 4, *$$

whence

$$X \equiv \pm 2.$$

But, for any two consecutive X , we have

$$2X_{i+1} = 3X_i + 5Y_i,$$

so that

$$X_{i+1} \equiv -X_i.$$

Hence the residues of X_i are 2 and -2 alternately.

22. The residues of Y_i are determined by the equation

$$2Y_{i+1} = X_i + 3Y_i.$$

On multiplying both sides by 3, and transposing, it is found that

$$Y_{i+1} + Y_i \equiv 3X_i \equiv \pm 1.$$

* Congruences to modulus 5 will occur so frequently in the sequel that the modulus will usually not be expressed. Whenever, as in the present case, the modulus is not stated, it must be understood to be 5.

The consequences of this relation are most simply obtained by using it to write out a cycle of the residues of X_i, Y_i , beginning with an arbitrary pair (2, 0). For a reason that will presently appear, a line is added containing the residues of $3X_i Y_i$,

$$\begin{array}{cccccccc|c} X_i \equiv & 2 & -2 & 2 & -2 & 2 & -2 & 2 & -2 & 2 \\ Y_i \equiv & 0 & 1 & 3 & 3 & 1 & 0 & 4 & 2 & 2 & 4 \\ 3X_i Y_i \equiv & 0 & -1 & -2 & 2 & 1 & 0 & -1 & -2 & 2 & 1 \end{array} \quad \begin{array}{c} 2 \\ 0 \\ 0 \end{array}$$

The cycle is complete, for every residue of Y occurs once with $X \equiv 2$, and once with $X \equiv -2$. The cycle duly begins again after the tenth column, as will be seen. Hence in any five consecutive integer-points on one range there is one and only one whose ordinate is a multiple of 5. Such a point may be called a primary point, because the prime factors which correspond to it are primary prime factors. The table then shows that $3XY$ measures the distance of (X, Y) from a primary point; and, if we replace $3XY$ by its least residue, positive or negative, we get the distance of the nearest primary point. In this way, if we know a simplest prime factor of p , say $a\omega$, we can determine a simplest primary prime factor of p ; namely, $e^i \cdot a\omega$, where i is the smallest integer, positive or negative, satisfying the congruence $3XY \equiv i$.

23. Similar properties obtain when the modulus is any power of 5. In any set of 5^m consecutive integer-points on the same range there is one and only one which has for ordinate a multiple of 5^m . Between two of these special points there are four whose ordinates are

$$\equiv (1, 3, 3, 1) \times 5^{m-1}, \text{ mod } 5^m,$$

or
$$\equiv (4, 2, 2, 4) \times 5^{m-1}, \text{ mod } 5^m.$$

If (X, Y) be any point whose ordinate is a multiple of 5^{m-1} , then $M^{3XY}(X, Y)$ is a point whose ordinate is a multiple of 5^m .

These theorems can be established by proving that if they are true for m they must also be true for $m+1$; and, since they are true when $m=1$, they are true for all positive integral values of m .

Now, M being the matrix of Art. 13, if we write

$$M^i = \begin{pmatrix} a_i/2, & 5b_i/2 \\ b_i/2, & a_i/2 \end{pmatrix},$$

we have

$$\frac{a_i + b_i \sqrt{5}}{2} = \left(\frac{a_1 + b_1 \sqrt{5}}{2} \right)^i.$$

Therefore
$$\frac{a_{5i} + b_{5i}\sqrt{5}}{2} = \left(\frac{a_i + b_i\sqrt{5}}{2} \right)^5,$$

so that
$$16a_{5i} = a_i^5 + 50a_i^3b_i^2 + 125a_ib_i^4,$$

and
$$16b_{5i} = 5a_i^4b_i + 50a_i^2b_i^3 + 25b_i^5.$$

From the first of these

$$a_{5i} \equiv a_i^5 \equiv a_i, \text{ mod } 5,$$

so that, when i is a power of 5,

$$a_{5i} \equiv a_i \equiv \dots \equiv a_1 \equiv -2, \text{ mod } 5.$$

From the second
$$b_{5i} \equiv 5b_i, \text{ mod } 25b_i.$$

Now
$$b_1 = 1.$$

Therefore
$$b_5 \equiv 5, \text{ mod } 5^2,$$

$$b_{25} \equiv 25, \text{ mod } 5^3,$$

and, in general, if i is any power of 5,

$$b_i \equiv i, \text{ mod } 5i.$$

Assume that there is a Y which is a multiple of 5^m , and write $i = 5^m$. We have then

$$2Y_i = b_i X + a_i Y.$$

By supposition $Y = 5^m \cdot H$, where H is integral; and it has been proved that $a_i \equiv -2, \text{ mod } 5$, $b_i = 5^m \beta$, where $\beta \equiv 1, \text{ mod } 5$. Hence Y_i is divisible by $5^m = 5^m \cdot H_i$ say. The last equation becomes, on removing the common factor 5^m ,

$$2H_i \equiv X - 2H, \text{ mod } 5;$$

or, what is equivalent,

$$H_i + H \equiv 3X, \text{ mod } 5.$$

This congruence is the same as that of Art. 21, and by similar treatment we learn that one of the points $P, P_5, P_{25}, P_{125}, P_{625}$ has an ordinate which is a multiple of $5i (= 5^{m+1})$, so that, as stated, if the theorems enunciated are true for any value of m they are true for $m+1$.

It follows that, from a reduced solution, or indeed any solution, of

$$X^2 - 5Y^2 = 4p,$$

we can derive the solutions of

$$X^2 - 5^{2m+1} Y^2 = 4p,$$

and so find the corresponding prime factors of p .

24. To determine the residues of X_i, Y_i , mod 4, consider the equations

$$\begin{pmatrix} 2, & 0 \\ 0, & 2 \end{pmatrix} X_s, Y_s = \begin{pmatrix} 18, & 40 \\ 8, & 18 \end{pmatrix} X, Y,$$

which give

$$X_s = 9X + 20Y \equiv X, \text{ mod } 4,$$

$$Y_s = 4X + 9Y \equiv Y, \text{ mod } 4.$$

Now, if X, Y are both even, one of them is and the other is not divisible by 4. For, if both were divisible by 4, $X^2 - 5Y^2$ would be a multiple of 16, and if both were $\equiv 2, \text{ mod } 4$, $X^2 - 5Y^2$ would be a multiple of 8. Hence, if X, Y are even,

$$2X_1 = 3X + 5Y, \equiv 2, \text{ mod } 4,$$

$$2Y_1 \equiv X + 3Y, \equiv 2, \text{ mod } 4,$$

so that X_1, Y_1 are both odd. It follows that, if P is an "even" point, P_1 and P_2 are odd points (because if P_2 were an even point, P_3 would be odd, in contradiction with what was proved above). It is also seen that, if a point P_i have odd coordinates, one and only one of the points adjacent to P_i has even coordinates, viz., P_{i+1} if $X_i \equiv Y_i, \text{ mod } 4$, and P_{i-1} if $X_i + Y_i \equiv 0, \text{ mod } 4$.

Hence, referring to the figure of Art. 15, there will be one and only one even point on the arc terminated by Q_{-1}, Q_2 whose coordinates are $2\sqrt{5p}, \pm 4\sqrt{p/5}$. This gives some idea of the comparative facility of solution of the two equations

$$X^2 - 5Y^2 = 4p, \quad \xi^2 - 5\eta^2 = p.$$

To solve the latter, we have only to suppose

$$X = 2\xi, \quad Y = 2\eta.$$

The values of ξ extend from $\sqrt{p}$ to $\sqrt{5p}$ for a minimum solution; about five times the extent that has to be examined for X .

Fixing the Absolute Term (Arts. 25, 26).

25. Kummer's second condition for a primary number is

$$a\omega \equiv a(1), \text{ mod } (1-\omega)^2,$$

and this is applicable to all prime factors, not only those which are primary. For instance, Reuschle, in his *Tafeln*, expresses all the prime factors so as to satisfy this congruence. It is obvious that $1-\omega$ is a factor of

$$a\omega - a(1),$$

and $(1-\omega)^2$ will be a factor if

$$a' \cdot \omega \equiv 0,$$

when $\omega = 1$, and $a'\omega$ is the derived function of $a\omega$.

Expressing that the complex number

$$\omega^k \cdot a\omega$$

satisfies the condition, we obtain

$$a_0k + a_1(k+1) + a_2(k+2) + a_3(k+3) + a_4(k+4) \equiv 0;$$

$$\text{therefore} \quad k \cdot s + a_1 + 2a_2 + 3a_3 + 4a_4 \equiv 0;$$

$$\text{therefore} \quad k \equiv -s^3(a_1 + 2a_2 + 3a_3 + 4a_4),$$

since s is not a multiple of 5.

Thus k is uniquely determined, and the absolute term is fixed.

A change of ω to ω^h does not affect the condition. For, if $a\omega$ satisfies the condition, so that

$$a_1 + 2a_2 + 3a_3 + 4a_4 \equiv 0,$$

then, for $a\omega^h$, the condition becomes

$$h(a_1 + 2a_2 + 3a_3 + 4a_4) \equiv 0,$$

which must be satisfied if the former is so.

26. The specification of the standard form of

$$\pm \epsilon^i \omega^k a\omega^h + j\Omega$$

is now substantially complete. The determination of h is a matter of subordinate interest, for it only means selecting one of the four factors of the norm as a representative; and when any one factor

$$a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 + a_4\omega^4$$

is given, the others are written down by a cyclic transposition of the last four coordinates arranged as above with their subscripts in geometric progression.

Nevertheless it seems worth while to indicate another way of selecting h , k ; viz., so that the reciprocal factor of p in its standard form may be obtained from the prime factor with a minimum of correction. Kummer's condition is satisfied by adopting this course, which has the advantage of determining the residues, mod 5, of the coordinates of the prime factor, and so saving some labour in the calculation of the prime factors. At the same time attention is drawn to a certain number—denoted by Q —which is connected with p , and promises to be of some importance in the theory.

Reciprocal factors of p . Residues of coordinates of $a\omega$, mod. 5
(Arts. 27-36).

27. A reciprocal factor, $\psi\omega$, of p is a complex integer such that

$$\psi\omega \cdot \psi\omega^{-1} = p.$$

The earliest publication relative to these factors appears to be the notice in Legendre's *Théorie des Nombres*, 3rd ed., 1830 (Arts. 549-561). The factors are there symbolized by A, A', A'', A''' (Art. 550), the reciprocal property is verified in Art. 553, and in Art. 558 it is pointed out that the coordinate sum is -1 . They appear also in Jacobi's memoir "Ueber die Kreistheilung," 1837 (*Gesammelte Werke*, Bd. vi., pp. 254 &c.), and the mode of calculation (p. 259) fixes the absolute term. The properties of the numbers so calculated suggested to Kummer the definition of primary numbers (*Berlin Monatsberichte*, May, 1850, p. 157). The reciprocal factors for all primes of the form $10\mu + 1$, less than 1000, are given in a paper on the quinquisection of the binomial equation (*Proc. Lond. Math. Soc.*, Vol. xviii., p. 229, 1887). In this table the conditions imposed by Legendre and Jacobi are both satisfied, and the special form of the reciprocal factor is denoted by

$$q\omega, = q_0 + q_1\omega + q_2\omega^2 + q_3\omega^3 + q_4\omega^4.$$

It is seen that there are two very distinct sets of primes p . In one set, containing from 75 to 80 per cent. of the whole, it is found that

$$q_0 \equiv \mu - 1, \quad q_i \equiv \mu + i, \quad i = 1, 2, 3, 4.$$

The primes p which have reciprocal factors of this kind will provisionally be called *perissads*. The rest of the primes, which will be called *artiads*, have reciprocal factors in which

$$q_0 \equiv \mu - 1, \quad q_i \equiv \mu, \quad i = 1, 2, 3, 4.$$

28. Now the product $a\omega \cdot a\omega^2$ is a reciprocal factor of p , for

$$a\omega \cdot a\omega^2 \times a\omega^{-1} \cdot a\omega^{-2} = N \cdot a\omega = p.$$

But the coordinate sum of $a\omega \cdot a\omega^2$ is s^2 ; that is to say, either 4 or 1. In the former case the coordinate sum can be reduced to the proper value, -1 , by subtracting Ω ; in the latter case, by changing the sign of the product. The immediate problem then becomes the determination of $a\omega$, so that

$$a\omega \cdot a\omega^2 = q\omega + \Omega, \quad \text{when } s = 2,$$

or else

$$a\omega \cdot a\omega^2 = -q\omega, \quad \text{when } s = 1.$$

It will be understood that each of these equations implies five equations, namely, each of the five coordinates of the product on the left is equal to the corresponding coordinate on the right. Performing the multiplication, we obtain

$$\begin{aligned} a_i^2 + (a_{i-1} + a_{i+1})(a_{i-2} + a_{i+2}) &= q_{3i} + 1, & \text{when } s = 2, \\ &= -q_{3i}, & \text{when } s = 1, \\ (i = 0, 1, 2, 3, 4). \end{aligned}$$

29. In analysing these systems it is convenient to retain one equation of each system (viz., that for which $i = 0$) in the above form. The others are replaced by equations expressing that the difference between the left sides for two values of i is the same as the difference between the corresponding dexters. The former differences take a characteristic form. We have, for example, when $s = 2$, taking $i = 2, 4$,

$$\begin{aligned} q_1 - q_2 &= \{a_2^2 + (a_1 + a_3)(a_0 + a_4)\} - \{a_4^2 + (a_3 + a_0)(a_2 + a_1)\} \\ &= \{a_2^2 + (a_1 + a_3)a_4 + a_3a_0 + a_1a_0\} - \{a_4^2 + (a_3 + a_0)a_2 + a_3a_1 + a_0a_1\}, \end{aligned}$$

and this, on interchanging the second terms of the two brackets, and cancelling the common term a_1a_0 , becomes

$$\begin{aligned} &= \{a_2^2 - (a_3 + a_0)a_2 + a_3a_0\} - \{a_4^2 - (a_1 + a_3)a_4 + a_3a_1\} \\ &= (a_2 - a_3)(a_3 - a_0) - (a_4 - a_1)(a_4 - a_3); \end{aligned}$$

similarly, $q_3 - q_4 = (a_1 - a_4)(a_1 - a_3) - (a_3 - a_2)(a_3 - a_0)$.

30. Hence

$$\begin{aligned} q_1 - q_2 - q_3 + q_4 &= (a_2 - a_3)(a_3 - a_0) - (a_4 - a_1)(a_4 - a_3) \\ &\quad - (a_1 - a_4)(a_1 - a_3) + (a_3 - a_2)(a_3 - a_0) \\ &= (a_3 - a_2)(-a_2 + a_0 + a_3 - a_0) \\ &\quad - (a_4 - a_1)(a_4 - a_3 - a_1 + a_2) \\ &= (a_3 - a_2)^2 + (a_3 - a_2)(a_4 - a_1) - (a_4 - a_1)^2. \end{aligned}$$

When $s = 1$, $q_i + 1$ is replaced by $-q_i$, so that any difference $q_i - q_j$, expressed in terms of the a for which $s = 2$, is the same as $q_j - q_i$, expressed in terms of a for which $s = 1$. In particular

$$q_1 - q_2 - q_3 + q_4 = \pm \{(a_3 - a_2)^2 + (a_3 - a_2)(a_4 - a_1) - (a_4 - a_1)^2\},$$

according as $s = 2$ or 1 .

31. Now, from the known residues of q_i (Art. 27), it is seen that

$$q_1 - q_2 - q_3 + q_4 \equiv 0.$$

Hence $(a_3 - a_2)^2 + (a_3 - a_2)(a_4 - a_1) - (a_4 - a_1)^2 \equiv 0$;

therefore $\{a_3 - a_2 - 2(a_4 - a_1)\}^2 \equiv 0$.

Hence, if we write $a_4 = a_1 + \delta$,

we have also $a_3 \equiv a_2 + 2\delta$.

Using these values for a_3, a_4 , we find

$$\begin{aligned} s &\equiv a_0 + a_1 + a_2 + a_3 + 2\delta + a_1 + \delta \\ &\equiv a_0 + 2a_1 + 2a_2 + 3\delta, \end{aligned}$$

a congruence which may also be written in the equivalent forms

$$\begin{aligned} a_0 + 2a_1 + 2a_2 &\equiv s + 2\delta, \\ -2a_0 + a_1 + a_2 &\equiv 3s + \delta. \end{aligned}$$

32. Again, letting the upper and lower signs correspond to the two cases $s = 2, 1$, we find

$$\begin{aligned} \pm (q_0 - q_1) &= (a_0 - a_3)(a_0 - a_1) - (a_2 - a_1)(a_3 - a_4) \\ &\equiv (a_0 - a_2 - 2\delta)(a_0 - a_1) - (a_2 - a_1)(a_2 - a_1 - \delta) \\ &\equiv -(2a_0 - a_1 - a_2)^2 - (2a_0 - a_1 - a_2)\delta \\ &\equiv -(3s + \delta)3s \\ &\equiv s^3 + 2s\delta. \end{aligned}$$

Thus $q_0 - q_1 \equiv -1 - \delta$ when $s = 2$,
 $q_0 - q_1 \equiv -1 - 2\delta$ when $s = 1$.

For an artiad $q_0 - q_1 \equiv -1$ (Art. 27),

so that, whether $s = 2$ or 1 , $\delta \equiv 0$.

On the other hand, for a perissad, $q_0 - q_1 \equiv -2$, and thus

$$\delta \equiv 1 \text{ when } s = 2, \quad \delta \equiv 3 \text{ when } s = 1,$$

results which may be combined in the formula

$$\delta \equiv 3s.$$

The last congruence of Art. 31 then gives

$$\begin{aligned} a_1 + a_2 &\equiv 2a_0 + 3s && \text{when } p \text{ is an artiad,} \\ a_1 + a_2 &\equiv 2a_0 + s && \text{when } p \text{ is a perissad.} \end{aligned}$$

33. The difference $a_1 - a_2$ can be expressed by means of Y . We have, namely,

$$Y = a_0 a_2 + (a_2 a_1 + a_2 \delta) + (a_1^2 + a_1 \delta) + (a_1 a_2 + 2a_1 \delta) + (a_2 a_0 + 2a_0 \delta) \\ - a_0 a_1 - a_1 a_2 - (a_2^2 + 2a_2 \delta) - (a_2 a_1 + 2a_1 \delta + a_2 \delta + 2\delta^2) - (a_1 a_0 + a_0 \delta),$$

whence, after some reductions,

$$2Y \equiv s(a_1 - a_2 + 2\delta).$$

From which, since s is not a multiple of 5,

$$a_1 - a_2 \equiv 2Ys^3 \quad \text{when } p \text{ is artiad,}$$

$$a_1 - a_2 \equiv 2Ys^3 - s \quad \text{when } p \text{ is perissad.}$$

Combining these with previous results, it will be found that, when p is artiad,

$$a_1 \equiv a_0 + Ys^3 - s \equiv a_4, \quad a_2 \equiv a_0 - Ys^3 - s \equiv a_3,$$

and, when p is perissad,

$$a_1 \equiv a_0 + Ys^3, \quad a_2 \equiv a_0 - Ys^3 + s, \quad a_3 \equiv a_0 - Ys^3 + 2s, \quad a_4 \equiv a_0 + Ys^3 + 3s.$$

34. It only remains to determine the residue of a_0 , mod 5. For this purpose we use the expression

$$(\psi_0) \equiv a_0^2 + (a_1 + a_4)(a_2 + a_3),$$

which is equal to $q_0 + 1$ or $-q_0$, according as s is 2 or 1 (Art. 28).

$$\text{Observing that} \quad a_1 + a_4 \equiv 2a_0 + 2Ys^3 - 2s,$$

$$a_2 + a_3 \equiv 2a_0 - 2Ys^3 - 2s,$$

for all values of p , we have

$$\psi_0 \equiv a_0^2 - (a_0 - s)^2 + Y^2 s^3$$

$$\equiv 2a_0 s - s^2 + Y^2 s^3,$$

so that

$$a_0 \equiv 3s + 2Y^2 s + 3s^3 \cdot \psi_0.$$

Hence, when $s = 2$, so that

$$\psi_0 = q_0 + 1 \equiv \mu,$$

$$a_0 \equiv 1 - Y^2 - \mu \equiv -\mu - Y^2 + 1,$$

and when $s = 1$, so that

$$\psi_0 = -q_0 \equiv -\mu + 1,$$

$$a_0 \equiv 3 + 2Y^2 + 2\mu - 2 \equiv 2\mu + 2Y^2 + 1.$$

35. The following table includes a summary of the results, and gives, for a real prime p , the residues of the coordinates expressed in terms of Y and μ , $= (p-1)/10$. The multiple of $\mu + Y^2$ in the third column is a part of the residue of each of the coordinates on the same line,

p	s	a_0	a_1	a_2	a_3	a_4
artiad.....	2	$-\mu - Y^2 + ; 1, -2Y-1,$	$2Y-1,$	$2Y-1,$	$-2Y-1$	
perissad...	2	$-\mu - Y^2 + ; 1, -2Y+1,$	$2Y-2,$	$2Y,$	$-2Y+2$	
artiad.....	1	$2\mu + 2Y^2 + ; 1,$	$Y,$	$-Y,$	$-Y,$	Y
perissad...	1	$2\mu + 2Y^2 + ; 1,$	$Y+1,$	$-Y+2,$	$-Y-2,$	$Y-1$

36. For practical application it is convenient to have these worked out for the several residues of Y , as in the table given below.

		p artiad	p perissad	
$s = 2$ $X \equiv -2$	$Y \equiv 0$	$-\mu + ; 1, 4, 4, 4, 4$	$-\mu + ; 1, 1, 3, 0, 2$	6
	$Y \equiv 1$	$-\mu + ; 0, 1, 0, 0, 1$	$-\mu + ; 0, 3, 4, 1, 4$	2
	$Y \equiv -1$	$-\mu + ; 0, 0, 1, 1, 0$	$-\mu + ; 0, 2, 0, 2, 3$	10
	$Y \equiv 2$	$-\mu + ; 2, 1, 4, 4, 1$	$-\mu + ; 2, 3, 3, 0, 4$	8
	$Y \equiv -2$	$-\mu + ; 2, 4, 1, 1, 4$	$-\mu + ; 2, 1, 0, 2, 2$	4
$s = 1$ $X \equiv 2$	$Y \equiv 0$	$2\mu + ; 1, 0, 0, 0, 0$	$2\mu + ; 1, 1, 2, 3, 4$	1
	$Y \equiv 1$	$2\mu + ; 3, 3, 1, 1, 3$	$2\mu + ; 3, 4, 3, 4, 2$	5
	$Y \equiv -1$	$2\mu + ; 3, 1, 3, 3, 1$	$2\mu + ; 3, 2, 0, 1, 0$	7
	$Y \equiv 2$	$2\mu + ; 4, 0, 1, 1, 0$	$2\mu + ; 4, 1, 3, 4, 4$	9
	$Y \equiv -2$	$2\mu + ; 4, 1, 0, 0, 1$	$2\mu + ; 4, 2, 2, 3, 0$	3

The term in μ is common to all the coordinates in the same line, so that the first line, for instance, shows that in a primary prime factor (with coordinate sum 2) of an artiad p ,

$$a_0 \equiv -\mu + 1, \quad a_1 \equiv -\mu + 4, \quad a_2 \equiv a_3 \equiv a_4;$$

and for a perissad p the coordinates are

$$a_0 \equiv -\mu + 1 \equiv a_1, \quad a_2 \equiv -\mu + 3, \quad a_3 \equiv -\mu, \quad a_4 \equiv -\mu + 2.$$

R 2

The last column indicates the order in which the prime factors occur if, starting with any one, we multiply it by ϵ , ϵ^2 , &c. We pass from a primo factor marked i to one marked j by multiplying the former by ϵ^{j-i} , and correcting the coordinate-sum if necessary. This is easily verified directly, or, by observing that $s = 2, 1$ are tantamount to $X \equiv -2, 2$ respectively (for $2X = 5A_0 - s^2$, and therefore $X \equiv 2s^2$), so that we are in effect repeating the table of Art. 22.

Sign of Y and Q (Arts. 37, 38).

37. This will be a convenient place to give some account of the mode of fixing the sign of Y in the tables appended. When p is a perissad, there is no difficulty, for, as will be seen by a reference to Art. 35 or Art. 36, a change of the sign of Y gives a different set of residues for the coordinates, and even for a primary factor, namely when $X \equiv 0$, the sequence of the residues is altered. Consider, for instance, the perissad 811, for which $X = 57$, $Y = \pm 1$, $\mu \equiv 1$, $s = 1$. The coordinates must be $\equiv 0, 1, 0, 1, 4$ or $0, 4, 2, 3, 2$, according as Y is positive or negative. Now the coordinates are found to be $0, -1, 2, 3, -3$, which agree with the second, and, however they may be arranged, are incompatible with the first. Thus $Y = -1$.

It is different with an artiad. Take, for example, the artiad 211, for which $X = 32$, $Y = \pm 6$, $\mu \equiv 1$, $s = 1$. Now, when Y is positive, the coordinates must be $\equiv 0, 0, 3, 3, 0$; if negative, they are $\equiv 0, 3, 0, 0, 3$. The coordinates are found to be $0, 0, 0, -2, 3$. The primo factor may be written $3\omega^2 - 2\omega^3$ or $-2\omega^2 + 3\omega^3$ consistently with $Y = 6$; it may be written $3\omega - 2\omega^4$ or $-2\omega + 3\omega^4$ for $Y = -6$. The residues, in fact, give no help in fixing the sign of Y .

38. Under these circumstances we make use of a function already mentioned, in Art. 30, viz.,

$$Q = q_1 - q_2 - q_3 + q_4 \\ = (-1)^s \{ (a_3 - a_2)^2 + (a_3 - a_2)(a_4 - a_1) - (a_4 - a_1)^2 \}.*$$

In the first place it will be observed that when ω is changed to ω^2 in the prime factor or the reciprocal factor, the sign of Q is reversed. The same is true of Y (Art. 11). Hence, if we fix the sign of Q , the sign of Y is also fixed.

* The symbol $(-1)^s$ is used on the assumption that s is 1 or 2. If other values of s have to be considered, $(-1)^s$ must be replaced by the Legendrian symbol $(2s/5)$; for it is 1 when $s \equiv \pm 2$, and -1 if $s \equiv \pm 1$.

Now, making the substitutions (Art. 31)

$$a_4 - a_1 = \delta,$$

$$a_3 - a_2 - 2(a_4 - a_1) = 5\delta',$$

we have $Q = (-1)^s \{ 5\delta^2 + 25\delta\delta' + 25\delta'\delta' \}$

$$\equiv (-1)^s 5\delta^2, \text{ mod } 25,$$

$$\equiv 5, \text{ mod } 25, \text{ if } p \text{ is perissad ;}$$

since, by Art. 32, $\delta \equiv 3$ when $s = 1$, and $\delta \equiv 1$ when $s = 2$.

When p is artiad it will be found that

$$Q \equiv \pm 5^{m-1}, \text{ mod } 5^m.$$

The prime factors in the following tables have been arranged so that the upper sign is true, viz.,

$$Q \equiv 5^{m-1}, \text{ mod } 5^m,*$$

and the sign of Y thus becomes determinate.

Example of first process of calculation (Arts. 39-51).

39. Some account will now be given of the details of the calculation of the complex factors of a given prime, and, to illustrate the method, we take as example $p = 1671781$.

40. The first step is to solve the equation

$$X^2 - 5Y^2 = 6687124 (= 4p).$$

Since the terminal digits of $5Y^2$ are 80, 000, 500, or 20, for an even Y , and e05, 125, e45 for an odd Y (e being any even digit), it follows that X^2 must end in

$$04, 124, 624, 44; \quad o29, 249, o69,$$

where o stands for an odd digit. From Art. 16 it appears that the minimum value of X lies between 2585 ($< 2\sqrt{p}$) and 2892 ($> \sqrt{5p}$); but of the 306 integers between these limits only 54 give X^2 with a proper ending, so that at worst 54 trials have to be made. A convenient way of making a trial is to add $-4p$, in the form 7312876 or 6712876 or 6092876, to the tabulated values of X^2 . The sum,

* There are some developments in which a more convenient assumption would be

$$Q \equiv -(-5)^{m-1}, \text{ mod } 5^m;$$

but this question, and others relating to Q , I hope to consider in a separate note.

multiplied by 2, is an exact square, Y^2 , when the proper value of X is reached. In the present case it happens that the first trial succeeds, and the minimum solution is

$$X = 2587, \quad Y = \pm 33.$$

41. Hence, by Art. 9,

$$s = 1, \quad A_0 = 1035, \quad (A_2, A_1) = (-242, -275),$$

and A_0 is now to be expressed (Art. 6) as a sum of five squares

$$1035 = a^2 + b^2 + c^2 + d^2 + e^2.$$

In writing down these decompositions the signless roots are arranged in order of magnitude,

$$a \leq b \leq c \leq d \leq e.$$

The greatest value for a is 32, the integral part of $\sqrt{1035}$, and there are 200 decompositions, beginning with 32, 3, 1, 1, 0, and ending with 17, 16, 15, 12, 11. It is, however, needless to write out all these, and I have found it convenient to write down all the decompositions containing one value of a , and to examine these before proceeding to the next value of a . On this plan the decompositions noted did not extend very far beyond the one required; and, on the other hand, writing down a number of them at a time was almost mechanical and less liable to errors of omission.

42. The first test applied is the coordinato-sum. The values of a, b must be such that, on properly fixing the signs,

$$\pm a \pm b \pm c \pm d \pm e = s,$$

where s is known. Hence, if the sum of the terms, all taken positively, be S , the sum of the positive terms of a proper decomposition is $\frac{1}{2}(s+S)$, and that of the negative terms $\frac{1}{2}(s-S)$. If, then, we can express $\frac{1}{2}(S+s)-a$ as a sum of any of the elements b, c, d, e , these, with a , furnish the positive terms of a proper-signed decomposition. Or, again, if $\frac{1}{2}(S-s)-a$ can be similarly partitioned, these elements, with a , have the negative sign in another set of signed terms. If neither partition is possible, the set (a, b, c, d, e) fails.

An important case of failure is when $a-s > 2\sqrt{A_0-a^2}$. For we have

$$2\sqrt{A_0-a^2} = 2\sqrt{b^2+c^2+d^2+e^2} > b+c+d+e.$$

Hence

$$a-s > b+c+d+e,$$

that is to say

$$a-b-c-d-e > s.$$

From this it is seen that in general the greatest coordinate cannot be greater than $2\sqrt{A_0/5}$. In the numerical example, we find that the greatest value of a , according to this formula, is 28, and, by putting 29 for a in the inequality above, it is verified that 29 is an impossible value. Thus the decompositions containing 32 or 31, or 30 or 29, are at once ruled out.

43. We have now to deal with signed sets of terms, and of course one decomposition into squares may give more than one set of signed terms. The second test is the table of Art. 36. In the example before us,

$$s = 1, \quad 2\mu \equiv 1, \quad Y \equiv \pm 2;$$

and the table shows that the coordinates of the prime factor sought must have the residues

$$0, 1, 2, 2, 1; \quad \text{or } 0, 2, 4, 0, 0; \quad \text{or } 0, 3, 3, 4, 1;$$

and a set of signed terms whose residues do not agree with one of these is not right. For example,

$$\pm 24, \mp 21, \mp 4, \pm 1, +1,$$

which gives the proper coordinate-sum when all the upper signs or when all the lower signs are taken, is excluded, for it contains no multiple of 5.

44. If a signed set of terms satisfies both tests, the values of A_1, A_2 are calculated, and if these have the required values, the required prime factor is found. The work is arranged thus

a	b	c	d	e
ab	ac	ad	ae	
	bc	bd	be	
		cd	ce	
			de	

where now $a, b, \dots e$ represent the terms, each with its proper sign. If $a, b, \dots e$ are in the right order (namely $a = a_0, b = a_1, \dots e = a_4$), then the sum of the four products in the diagonal line, and the product in the right-hand upper corner, is A_1 . The sum of the other five products is A_2 ; but it is unnecessary to calculate A_2 (save for verification) because $A_1 + A_2 = (A_0 - s^2)/2$ is the same for all sets which satisfy the first test.

45. In general there is ambiguity about the sequence of $a, b, \dots e$ (as in the instance worked below), and it is desirable to be able to find A_1, A_2 for every arrangement of the terms, without rewriting. This is done by means of the following diagrams, in which the two sets of five products each are denoted by crosses and noughts respectively.

$\times 0 0 \times$	$\times \times 0 0$	$\times 0 \times 0$	$\times \times 0 0$	$\times 0 0 \times$	$\times 0 \times 0$
$\times 0 0$	0×0	$\times 0 0$	$0 0 \times$	0×0	$0 0 \times$
$\times 0$	$0 \times$	$0 \times$	$\times 0$	$\times \times$	$\times \times$
$\times$	$\times$	$\times$	$\times$	0	0
<i>abcde</i>	<i>abdec</i>	<i>abced</i>	<i>abedc</i>	<i>abdce</i>	<i>abecd</i>
<i>adbec</i>	<i>aebcd</i>	<i>aebdc</i>	<i>adbce</i>	<i>acbed</i>	<i>acbde</i>

Beneath each diagram two arrangements of the coordinates $abcde$ are shown. Each of these may be read backwards or forwards and may begin at any letter, so that to each diagram there are 20 arrangements (10 for each signature), and, since no arrangement is repeated, there are 120 in all, which is right. For the upper signatures, in which a, b are adjacent, A_1 is the sum of the $\times$, and A_2 of the 0. For the lower signatures, in which a, b are not adjacent, A_1 is the sum of the 0, and A_2 of the $\times$.

46. As an example of the use of these diagrams, take the set of signed terms 23, -21, +6, -5, -2, the residues of which are 3, 4, 1, 0, 3, agreeing with the third set named in Art. 43, viz., 0, 3, 3, 4, 1. It is seen that two arrangements of the terms under trial are available. We try

-5	-2	23	-21	6
<hr/>				
	10	-115	105	-30
		-46	42	-12
			-483	138
				-126

The principal diagram fails to give $(A_1, A_2) = (-242, -275)$. In fact it is visible, without doing the addition, that

$$A_1 (= 10 - 46 - 483 - 126 - 30) \text{ is } < -600;$$

and that A_2 is positive. Either of these results shows that a, b, c, d, e is not right. The other arrangement, consonant with the second

test, is a, c, b, d, e , the lower signature of the last diagram. A_1 (given by the 0 of that diagram) $= -275$; $A_2 = -242$. Hence

$$Y = A_2 - A_1 = 33,$$

and this agrees with the indication, in the table of Art. 36, that $Y \equiv -2$ for the residues 0, 3, 3, 4, 1. We find, then, that the simplest prime factor of 1671781 is

$$-5 + 23\omega - 2\omega^2 - 21\omega^3 + 6\omega^4.$$

47. Two other methods of reducing the work may be noted. As soon as the residues of a trial-set are written down, the value of Y is known, and therefore also the values of A_2, A_1 separately. These two values do not end in the same digit, unless the simplest prime factor is primary.* Therefore we can, by working with the final digits only of the products ab , &c., at once exclude several—in the long run one-half—of the failures. Secondly, it is obvious that two or more trial sets, which differ only by their signs, can be tested in one multiplication scheme, by putting two or more rows of signs before the products.

48. In calculating the prime factor written above, it was necessary to write down 103 five-square expressions for A_0 , beginning with $a = 28$. Of these 43 were excluded by the first test ($s = 1$), and 17 were not examined, as they came after the solution was obtained. On the other hand, 13 satisfied this test doubly. The "second test" excluded 6 single and 2 double cases; and the values of A_2, A_1 were examined in 24 single and $10\frac{1}{2}$ double cases (the solution being the first of a double case), so that in all 35 multiplication schemes like that in Art. 46 were formed.

49. To obtain the simplest primary factor, we note that, since $X \equiv 2$ and $Y \equiv -2$, $3XY \equiv -2$; and the primary factor is $\epsilon_2^2 \cdot a\omega$, where

$$a\omega = -5 + 23\omega - 2\omega^2 - 21\omega^3 + 6\omega^4.$$

Now, multiplying by ϵ_2 means replacing each coordinate (a_i) by the sum of the two opposite coordinates ($a_{i+2} + a_{i-2}$), just as multiplying by ϵ means replacing each coordinate (a_i) by the sum of the two

* When $Y \equiv 0$ there is a simplification in the work, as the "second test" gives only two sets of residues instead of three. The symmetry of this case, and the ease of the computations, suggested this condition as proper for a canonical form of a prime factor, before I found—with no small pleasure—that it was Kummer's first condition for a primary number.

adjacent coordinates ($a_{i+1} + a_{i-1}$). In multiplying by ϵ_2^3 , the coordinate-sum becomes $4s$ (that is to say, in the present case, 4), and the coordinate-sum is corrected by subtracting each of the coordinates in the product from unity. The work can be done in three lines, thus :

$$\begin{array}{rcccccc} a\omega & = & -5 & 23 & -2 & -21 & 6 \\ \epsilon_2 a\omega & = & -23 & -15 & 1 & 18 & 21 \\ \epsilon_2^2 a\omega & = & 19 & 39 & -2 & -38 & -14 \end{array}$$

and the simplest primary factor ($= \Omega - \epsilon_2^2 a\omega$) is

$$-18 - 38\omega + 3\omega^2 + 39\omega^3 + 15\omega^4.$$

50. The product $a\omega \cdot a\omega^3$, corrected for coordinate-sum, is the reciprocal factor ; and $a\omega$ may be replaced by the primary factor or any other prime factor. The coefficient of ω^{3i} in the product is

$$a_i^2 + (a_{i+1} + a_{i-1})(a_{i+2} + a_{i-2}),$$

and this suggests a convenient arrangement of the work, which makes it possible indeed to write down the coordinates of the reciprocal factor at once for moderate values of p . Having written down the coordinates of $a\omega^3$, place under each of them (1) its square, (2) the product of the adjacent sum and the opposite sum (where "adjacent sum" means the sum of the two coordinates adjacent to the one treated, and similarly for the "opposite sum"). The sum of the square and product is the coordinate of $a\omega \cdot a\omega^3$, in its proper place. For example, taking $a\omega$ to be the simplest prime factor obtained in Art. 46, we have

$a\omega^3,$	-5	-2	6	23	-21
square	25	4	36	529	441
product	-23·29	1·2	-21·26	15·7	18·4
$a\omega \cdot a\omega^3 =$	-642	+ 6\omega	- 510\omega^2	+ 634\omega^3	- 513\omega^4

Hence the reciprocal factor is

$$q\omega = 642 - 6\omega + 510\omega^2 - 634\omega^3 - 513\omega^4,$$

and from this the cyclotomic of the fifth degree can be formed by

the formulæ in the paper (*Proc. Lond. Math. Soc.*, Vol. XVIII.) already cited.*

51. The value of Q is

$$-6-510+634-513 = -395 \equiv 5, \text{ mod } 25,$$

as it should be.

When p is artiad, the sign of Y is undetermined until this stage. The convenient course is to assume one sign for Y , and if this leads to $Q \equiv -5^m, \text{ mod } 5^{m+1}$, it is only necessary to replace $a\omega$ and $q\omega$ by $a\omega^3, q\omega^3$ respectively.

Second process (Arts. 52-54).

52. In the above process there is a considerable amount of labour wasted in making trials which fail, and it is clear that much of the waste work might be utilized for the factorization of other primes. This remark suggests a second mode of attacking the problem. Instead of seeking the complex factors of a given prime, we may seek all the primes that belong to a given A_0 . Of the decompositions

$$A_0 = a^2 + b^2 + c^2 + d^2 + e^2,$$

we select those which make $s = 1$ if A_0 is odd, or $s = 2$ if A_0 is even. Any set of signed terms which does not satisfy this test can [by adding any (the same) integer to each term and reversing the sign if necessary] be reduced to a set in which the "first test" is satisfied, but with a different A_0 . By this exclusion we do not miss any primes, but merely avoid repetitions of the same prime under a different A_0 .

For the same reason it is desirable to use only those signed terms which belong to reduced solutions; the excluded cases occur as reduced solutions for a smaller A_0 .

53. When a set of signed terms is selected, the multiplication scheme of Art. 44 is formed; and then, by using the diagrams of Art. 45, we compute six pairs of product-sums (A_2, A_1) which reduce however to three pairs when there are two equal terms, to two pairs

* An unchecked calculation gives the following values for the coefficients of the cyclotomic $\eta^5 + \eta^4 + P_2\eta^3 + P_3\eta^2 + P_4\eta + P_5$ in this case :—

$$P_2 = -668712, P_3 = -216124779, P_4 = -28654017881, \\ P_5 = 1685462024703.$$

if there are two pairs of equal terms, and to one pair if three of the terms are equal.

It is sufficient to record one product-sum of each pair, the other being given by the equation

$$A_1 + A_2 = -\frac{1}{2}(A_0 - s^2).$$

For this we choose the greater of the pair, and calling it A_2 we shall have Y positive. It will be observed that A_2 is numerically less than A_1 , and that the entry corresponds to a reduced or an unreduced solution according as it is ≤ 0 or > 0 . The upper signature of the diagram (Art. 45) is proper when A_2 is the sum of the "noughts," the lower when it is the sum of the crosses. If this signature does not agree with the table of Art. 36, we must interchange A_2 , A_1 and replace Y , ω by $-Y$, ω^2 .

54. Consider, for example, the scheme of Art. 46, which gives the product-sums

$$158, \quad -51 \times, \quad 81 \times, \quad 209, \quad -194, \quad -242 \times,$$

those marked $\times$ being the sums of the crosses. The first, third and fourth are not reduced, and the sixth has been worked out. The second, taking $A_2 = -51$, gives $A_1 = -466$ and $Y = 415, \equiv 0$.

Hence, $N \cdot a\omega = (A_0 - A_1)(A_0 - A_2) - (A_1 - A_2)^2 = 1457861$,

for which $2\mu \equiv 2$. The table of Art. 36 gives a choice of residues 3, 2, 2, 2, 2 or 3, 3, 4, 0, 5; and the lower signature of the second diagram (Art. 45), namely, $a e b c d$, becomes $-5, 6, -2, 23, -21$. This agrees with the 3, 3, 4, 0, 5, if we begin with -2 , and go forwards. Thus the assumption as to the sign of Y was correct, and the complex factor of 1457861 in the standard form is

$$-2 + 23\omega - 21\omega^2 - 5\omega^3 + 6\omega^4,$$

and

$$(2587)^2 - 5(415)^2 = 4 \times 1457861.$$

Similarly, from the fifth entry, it will be found that 1652341 is the norm of $6 - 5\omega - 2\omega^2 - 21\omega^3 + 23\omega^4$ and $Y = 129$.

Conditions that $a\omega$ should be a complex prime (Arts. 55, 56).

55. When a table of primes is at hand it can be determined by inspection whether the norms obtained are or are not primes; in other words, whether $a\omega$ is or is not a complex prime. This can also be determined, without using a table of primes, in the following way.

The real factors of a norm of a complex integer are of three kinds. First we have primes of the form $10\mu+1$ (say $p_1, p_2, \dots$); next, primes of the form $10\mu-1$ (say $q_1, q_2, \dots$), which must appear as powers q^{2t} , t being an integer; lastly, there are primes of the form $10\mu \pm 3$ and 2 (say $r_1, r_2, \dots$), which appear as powers r^{4t} .

Now, if $N\omega$ contain r as a factor, r will be a factor of all the differences of the coordinates of $a\omega$, and can be immediately detected.

If $N\omega$ contain a prime, q , as a factor, this prime will be a factor of all the differences of the coordinates of the "reciprocal factor" $a\omega \cdot a\omega^2$.

The presence of two primes $p_1 \cdot p_2$, or of a square p^2 , as factors of $N\omega$, can be recognized in two ways, when each of the p is of the form $10\mu+1$.

The first way depends on the fact that there are two integer points in the reduced half-segment AQ_1 (see figure to Art. 15).^{*} If there are more than two p -factors, there will be more than two integer points, but the number depends upon how many of the p are equal. To detect these it will be needful to examine the suitable values of X between $2\sqrt{N}$ and $\sqrt{5N}$, where N represents $N\omega$.

The second way depends on the fact that, corresponding to any one integer point, there will be two (or more) different sets of coordinates; that is to say, there will be two or more complex numbers which have the same X, Y (and therefore the same A_0, A_1, A_2 , and s), and may be taken to have the proper absolute terms, and yet are not included in one formula $a\omega^h$. The existence of such numbers is indicated by the same product-sum occurring in two different multiplication schemes belonging to one square-sum.

56. The former process is the easier when we are dealing with an isolated complex number. For instance, when $N\omega = 1652341$, there are four integer points on the reduced half-segment, viz., (2587, 129), (2613, 209), (2817, 515), (2847, 547); and, in fact,

$$1652341 = 41 \times 191 \times 211.$$

The other method is better if we are examining all the complex numbers that belong to a given square-sum. If a product-sum occurs only in connexion with one complex number, and the norm of this number is free from q and r factors, then the complex integer is

^{*} This theorem is due to Tchébicheff, and is quoted in Prof. Mathews' admirable text-book on the *Theory of Numbers*, Pt. I., p. 270.

a complex prime and its norm is a real prime. For instance, if $A_0 = 39$, there are five sets of signed terms

$$\begin{array}{l} 5 \ -3 \ -2 \ +1, \quad -5 \ +3 \ +2 \ +1, \quad 4 \ +3 \ -3 \ -2 \ -1, \\ 4 \ -3 \ -3 \ +2 \ +1, \quad -4 \ +3 \ +3 \ -2 \ +1, \end{array}$$

which may be distinguished as a, b, c, d, e respectively. Then it is found that -8 is a product-sum peculiar to a ; $-9, -5$ to b ; 0 to c , and -3 to d (noting only those which belong to reduced solutions). These answer to the norms 2341; 2351, 2251; 1901; and 2141 respectively. It is easily verified that there are no q, r factors, and we conclude that they are all prime. On the other hand, -4 , which gives the norm $(39+4)(39+15)-(15-4)^2 = 2201$, is common to a and e . This norm therefore contains two p factors; and, in fact,

$$2201 = 31 \times 71.$$

The analysis by which we justify this mode of discriminating a complex prime from other complex integers is a straightforward application of the methods and results of Arts. 8 and 29.*

Tables.

The tables which follow give the prime and reciprocal factors of every prime p , of the form $10\mu + 1$, less than 10000, and of a few larger primes. They are arranged in seven columns. The first contains the value of p . The second contains the minimum values of X, Y which satisfy the equation

$$X^2 - 5Y^2 = 4p,$$

the sign of Y being fixed as explained in Art. 38. The third column contains the minimum residue of $3XY$, mod 5, and shows by what power of $\omega + \omega^{-1}$ the simplest prime factor must be multiplied to obtain the simplest primary factor. The next two columns contain the coordinates of the simplest prime factor and the simplest primary prime factor, arranged in the order

$$a_0, a_1, a_2, a_3, a_4.$$

It may be noted that in a former paper (*Proc. Lond. Math. Soc.*, Vol. xviii., p. 229) the coordinates were tabulated with the indices in, geometric, not arithmetic, progression $a_1, a_2, a_3, a_4; a_0$. The arith-

[* The question is the subject of a supplementary note which follows. But the discussion is not quite on the lines suggested above, for it was found convenient to consider the factors of $a\omega$ itself rather than the factors of the norm.]

metic order is here adopted as being more adapted for calculations. Whenever the simplest prime factor is itself primary ($Y \equiv 0$) the entry in the fifth column is merely $a\omega$.

The sixth column, except when p is less than 1000, contains the reciprocal factor of p ; and the last column shows

$$Q = q_1 - q_2 - q_3 + q_4;$$

q_1 , &c. being the coordinates entered in the sixth column, omitting the first entry, q_0 .

For primes less than 1000 the reciprocal factors have been tabulated in the paper cited above, and it seemed useless to repeat them. The space thus saved has been used to give the prime factors published by Reuschle in his *Tafeln*, page 3. They are here expressed in terms of $a\omega$ the simplest prime factor of these tables, and $b\omega$ the simplest primary prime factor. The first entry is the "einfach," and the second is the "primär" of Reuschle. But when the primary factor is sufficiently simple, Reuschle does not give any entry under the *einfach*. In this column ϵ stands for $\omega + \omega^{-1}$, ϵ_2 for $\omega^2 + \omega^{-2}$, and Ω for $1 + \omega + \omega^2 + \omega^3 + \omega^4$. For example, $p = 11$, Reuschle's *einfach* factor

$$\begin{aligned} &= -\epsilon \cdot a\omega^3 + \Omega \\ &= -(\omega + \omega^{-1})(\omega^3 + \omega^0 - \omega^3) + \Omega \\ &= -\omega^3 - \omega^3 + \omega^4 - \omega - 1 + \omega^3 + \Omega \\ &= \omega^3 + 2\omega^4; \end{aligned}$$

and the primary factor is $= -b\omega^3$

$$= \omega - \omega^3 - 2\omega^4.$$

It will be observed that, disregarding some misprints and neglecting the terms in Ω , Reuschle always gives the simplest primary prime factor. The *einfach* are the simplest factors for about half of the primes, but in some cases (241, 431) the primary factor is simpler than the *einfach*. I find four misprints.

$p = 601.$	<i>einfach.</i>	$-a^2$	is printed instead of	$-a^3$.
$p = 751.$	<i>primär.</i>	$5a^2$	" "	$8a^2$.
$p = 821.$	<i>primär.</i>	$4 + 4a$	&c. " "	$1 + 4a$ - &c.
$p = 881.$	<i>primär.</i>	$-5a$	" "	$-5a^2$.

[To ensure the accuracy of the tables, as far as practicable, the proof-sheets have been systematically tested and every entry has been checked at least once. Negative numbers are denoted by dots placed over them, a method which has the authority of Prof. Sylvester's example. Thus for $p = 211$, $Y = -6$, $a\omega = 3\omega - 2\omega^4$.]

p	X, Y	$3XY$	Prime Factors.		Reuschlo's Factors.	Q
			Simplest, $=a\omega$.	Simplest primary $b\omega$		
11	7, 1	1	0, 1, 0, 1, 1	0, 0, 2, 1, 1	$-\epsilon a\omega^2 + \Omega, -b\omega^3$	5
31	12, 2	2	0, 2, 1, 0, 0	2, 3, 3, 1, 0	$a\omega^3, -b\omega^3 + 3\Omega$	5
41	13, 1	1	1, 1, 0, 2, 0	1, 1, 0, 1, 2	$\dots, b\omega^{-1} + \Omega$	5
61	17, 3	2	1, 2, 0, 1, 1	2, 3, 1, 0, 1	$-a\omega + \Omega, -b\omega + \Omega$	5
71	17, 1	1	2, 1, 1, 0, 1	1, 1, 1, 3, 0	$-\epsilon a\omega^{-1} + \Omega, b\omega^{-1} + \Omega$	5
101	22, 4	1	2, 2, 0, 1, 0	1, 1, 2, 0, 2	$\dots, b\omega^{-1} - \Omega$	5
31	23, 1	1	2, 0, 1, 2, 1	2, 2, 2, 1, 0	$a\omega^3 - \Omega, -b\omega^3 + 2\Omega$	5
51	27, 5	0	1, 1, 2, 2, 1	$a\omega$	$\dots, -a\omega^2 + \Omega$	20
81	27, 1	1	1, 0, 1, 0, 3	3, 2, 0, 2, 1	$\epsilon a\omega^3 + \Omega, b\omega^3 - 2\Omega$	5
91	28, 2	2	3, 1, 1, 1, 0	3, 2, 4, 1, 2	$a\omega + \Omega, -b\omega - 2\Omega$	5
* 211	32, 6	1	0, 3, 0, 0, 2	0, 2, 2, 3, 3	$-a\omega^3, b\omega^3 + 2\Omega$	25
41	33, 5	0	2, 2, 1, 1, 2	$a\omega$	$\epsilon a\omega^2, -a\omega^2 + 2\Omega$	20
51	32, 2	2	1, 2, 2, 2, 0	1, 4, 3, 3, 4	$-\epsilon_3 a\omega^3 + 2\Omega, b\omega^3 + 3\Omega$	20
71	33, 1	1	2, 0, 3, 0, 1	0, 0, 1, 3, 3	$\dots, b\omega^{-1}$	5
* 81	37, 7	2	0, 3, 1, 1, 2	2, 6, 1, 4, 4	$-a\omega^{-1} + \Omega, b\omega^{-1} + 4\Omega$	25
311	37, 5	0	3, 2, 1, 0, 1	$a\omega$	$\dots, a\omega^{-1} + 2\Omega$	5
31	37, 3	2	0, 3, 2, 1, 1	3, 3, 3, 4, 0	$-\epsilon a\omega^3 + \Omega, b\omega^3 + 3\Omega$	5
401	43, 7	2	2, 1, 0, 3, 2	1, 1, 2, 5, 3	$\epsilon_2 a\omega^3 - 2\Omega, -b\omega^3 + \Omega$	5
* 21	42, 4	1	2, 3, 0, 0, 2	1, 2, 3, 2, 2	$\dots, -b\omega^{-1} + 2\Omega$	25
31	43, 5	0	2, 3, 0, 2, 1	$a\omega$	$\epsilon_2 a\omega^{-1} - \Omega, -a\omega^{-1} + 3\Omega$	20
* 61	43, 1	1	1, 0, 4, 1, 0	2, 2, 2, 2, 3	$\dots, -b\omega^3 + 2\Omega$	25
91	47, 7	2	2, 1, 1, 3, 2	1, 4, 5, 6, 3	$-a\omega^3 + 2\Omega, -b\omega^3 + 6\Omega$	5
* 521	47, 5	0	0, 4, 1, 1, 1	$a\omega$	$\dots, a\omega^2 + \Omega$	25
41	47, 3	2	3, 0, 0, 1, 3	4, 4, 0, 4, 3	$-a\omega^{-1}, -b\omega^{-1} + 4\Omega$	5
71	48, 2	2	0, 1, 1, 3, 3	4, 1, 4, 2, 5	$-a\omega^2 + \Omega, b\omega^3 + 4\Omega$	20
601	53, 9	1	0, 2, 0, 3, 3	4, 1, 2, 2, 4	$-\epsilon_2 a\omega^{-1} + 2\Omega, -b\omega^{-1} + \Omega$	5
31	52, 6	1	4, 0, 1, 0, 2	2, 3, 0, 3, 4	$a\omega^2, -b\omega^3$	5
41	53, 7	2	2, 2, 1, 3, 2	2, 3, 4, 4, 3	$-a\omega^3 + 3\Omega, b\omega^3 + 4\Omega$	20
61	57, 11	1	0, 1, 3, 3, 2	0, 5, 2, 1, 4	$-\epsilon_2 a\omega^2 + 2\Omega, -b\omega^3 + 2\Omega$	45
* 91	53, 3	2	3, 0, 3, 2, 0	3, 0, 5, 5, 5	$a\omega^{-1}, -b\omega^{-1} + 5\Omega$	25
701	53, 1	1	0, 2, 4, 1, 1	4, 1, 2, 3, 1	$-a\omega^3 + \Omega, -b\omega^3 + 3\Omega$	5
51	57, 7	2	1, 1, 2, 1, 4	6, 4, 2, 3, 6	$-\epsilon_2 a\omega - \Omega, b\omega + 6\Omega$	5
61	58, 8	2	1, 2, 3, 1, 3	5, 0, 7, 4, 4	$\epsilon a\omega^{-1}, -b\omega^{-1}$	5
811	57, 1	1	0, 1, 2, 3, 3	5, 0, 3, 1, 1	$\dots, b\omega^{-1}$	5
21	58, 4	1	3, 1, 2, 1, 3	0, 5, 1, 3, 2	$-\epsilon_2 a\omega^2, -b\omega^3 + \Omega$	5
* 81	62, 8	2	0, 1, 2, 2, 4	3, 1, 1, 4, 6	$-a\omega^3 + 2\Omega, -b\omega^3 + \Omega$	25
911	67, 13	2	1, 3, 0, 4, 1	3, 2, 1, 5, 4	$-a\omega^3 + \Omega, -b\omega^3 + 5\Omega$	20
41	62, 4	1	4, 2, 1, 2, 0	2, 3, 4, 1, 2	$-a\omega^2 + 2\Omega, -b\omega^3 + 4\Omega$	5
71	67, 11	1	3, 3, 2, 2, 1	4, 1, 1, 3, 5	$\epsilon_2 a\omega^{-1}, b\omega^{-1} + \Omega$	20
* 91	63, 1	1	1, 2, 1, 4, 2	4, 3, 2, 2, 2	$\dots, b\omega^{-1} + 2\Omega$	25

p	X, Y	$3XY$	Prime Factors.		Reciprocal Factor.	Q
			Simplest, $=a\omega$.	Simplest primary.		
1021	67, 9	1	2, 2, 3, 3, 1	1, 1, 1, 2, 5	4, 12, 24, 0, 9	45
* 31	68, 10	0	3, 1, 1, 4, 1	$a\omega$	2, 12, 2, 12, 23	25
51	72, 14	1	2, 1, 2, 4, 2	1, 4, 3, 0, 2	6, 4, 2, 23, 16	45
61	67, 7	2	1, 4, 1, 0, 3	2, 7, 1, 5, 6	0, 7, 12, 16, 20	55
91	67, 5	0	1, 4, 0, 1, 3	$a\omega$	2, 20, 9, 18, 8	55
*1151	68, 2	2	3, 1, 4, 1, 1	6, 1, 6, 1, 4	14, 15, 20, 0, 10	25
71	72, 10	0	0, 0, 4, 2, 3	$a\omega$	6, 22, 1, 20, 4	45
81	73, 11	1	2, 4, 3, 1, 0	3, 2, 2, 4, 0	13, 14, 0, 16, 18	20
1201	77, 15	0	1, 1, 3, 2, 4	$a\omega$	24, 4, 18, 3, 6	5
31	73, 9	1	2, 1, 3, 4, 0	2, 2, 2, 4, 5	2, 14, 25, 4, 12	55
91	72, 2	2	2, 0, 0, 4, 3	6, 1, 5, 6, 3	8, 20, 9, 2, 22	5
1301	73, 5	0	4, 1, 3, 0, 2	$a\omega$	24, 6, 13, 2, 16	5
21	73, 3	2	0, 1, 2, 5, 0	1, 1, 6, 7, 5	4, 3, 16, 10, 26	55
61	82, 16	1	0, 1, 0, 4, 4	5, 0, 3, 4, 4	20, 12, 12, 1, 20	5
81	77, 9	1	4, 2, 1, 3, 1	2, 2, 5, 2, 1	18, 24, 0, 6, 13	5
1451	77, 5	0	1, 4, 2, 3, 1	$a\omega$	24, 4, 7, 22, 6	5
71	77, 3	2	2, 0, 3, 3, 3	5, 5, 6, 3, 2	4, 12, 6, 30, 9	45
81	77, 1	1	1, 5, 1, 0, 2	3, 2, 5, 3, 1	2, 14, 0, 29, 12	55
*1511	83, 13	2	1, 2, 5, 0, 2	5, 8, 7, 3, 3	20, 26, 6, 9, 4	25
31	87, 17	2	5, 2, 2, 1, 1	8, 2, 8, 4, 5	28, 14, 15, 4, 2	5
71	83, 11	1	2, 1, 3, 4, 2	0, 5, 1, 2, 3	6, 8, 1, 30, 16	55
*1601	82, 8	2	4, 1, 0, 0, 4	4, 5, 0, 5, 5	16, 0, 20, 15, 20	25
21	83, 9	1	3, 0, 3, 0, 4	5, 5, 1, 2, 2	4, 8, 24, 25, 4	5
1721	83, 1	1	2, 0, 2, 5, 1	0, 5, 4, 2, 2	6, 2, 6, 25, 26	55
41	87, 11	1	1, 5, 2, 1, 2	3, 3, 1, 6, 3	8, 0, 4, 28, 23	55
1801	93, 17	2	2, 2, 2, 5, 1	1, 6, 3, 5, 3	6, 6, 28, 3, 24	55
11	88, 10	0	0, 5, 3, 1, 1	$a\omega$	25, 12, 2, 24, 10	20
31	87, 7	2	5, 3, 1, 0, 0	8, 7, 2, 1, 5	28, 14, 20, 9, 2	5
61	87, 5	0	3, 3, 1, 0, 4	$a\omega$	10, 2, 22, 1, 30	55
* 71	92, 14	1	2, 0, 2, 2, 5	4, 3, 3, 2, 2	16, 2, 33, 12, 2	25
1901	97, 19	1	3, 4, 2, 1, 3	1, 1, 3, 5, 2	6, 4, 13, 12, 34	55
31	88, 2	2	1, 5, 0, 3, 1	2, 7, 0, 7, 4	18, 1, 20, 26, 12	5
* 51	93, 13	2	2, 4, 1, 4, 1	1, 9, 4, 6, 6	6, 0, 30, 20, 15	25
2011	93, 11	1	4, 4, 1, 1, 2	3, 2, 4, 0, 4	15, 18, 22, 24, 0	20
81	98, 16	1	3, 5, 1, 2, 1	2, 2, 3, 1, 5	2, 6, 30, 26, 7	5
2111	92, 2	2	4, 1, 4, 0, 2	8, 3, 6, 5, 1	20, 18, 8, 1, 30	5
31	93, 5	0	3, 2, 0, 3, 4	$a\omega$	2, 36, 15, 6, 12	45
41	97, 13	2	3, 4, 1, 2, 3	4, 6, 5, 4, 2	12, 35, 4, 18, 2	55
61	93, 1	1	1, 4, 4, 1, 2	3, 2, 4, 5, 1	10, 12, 3, 14, 30	45
*2221	98, 12	2	5, 1, 2, 3, 1	6, 3, 2, 7, 2	26, 13, 2, 28, 12	25
51	97, 9	1	3, 2, 0, 1, 5	1, 4, 2, 5, 2	6, 6, 33, 8, 24	55
81	102, 16	1	4, 2, 4, 2, 1	2, 3, 5, 2, 6	18, 16, 35, 4, 2	45
2311	107, 21	1	5, 1, 0, 1, 4	5, 5, 2, 4, 4	30, 2, 12, 24, 15	5
41	97, 3	2	3, 5, 0, 1, 2	4, 6, 5, 1, 7	12, 30, 6, 28, 3	55
51	97, 1	1	3, 2, 5, 1, 0	4, 1, 3, 5, 3	1, 31, 12, 2, 24	20

<i>p</i>	<i>X, Y</i>	<i>3XY</i>	Prime Factors.		Reciprocal Factor.	<i>Q</i>
			Simplest, = <i>aw</i> .	Simplest primary.		
2371	103, 15	0	1, 1, 6, 2, 0	<i>aw</i>	4, 38, 16, 10, 9	55
81	98, 4	1	2, 5, 1, 3, 1	3, 3, 2, 4, 5	13, 6, 20, 36, 2	20
2411	107, 19	1	5, 1, 2, 2, 3	0, 5, 2, 4, 1	25, 2, 12, 34, 0	20
41	103, 13	2	2, 1, 1, 6, 0	7, 7, 1, 9, 2	2, 10, 9, 18, 38	55
2521	102, 8	2	2, 1, 4, 2, 4	0, 5, 6, 3, 7	6, 22, 16, 35, 4	45
31	112, 22	2	0, 2, 2, 1, 6	3, 7, 8, 1, 10	12, 14, 40, 6, 7	55
51	103, 9	1	0, 2, 5, 2, 3	4, 6, 3, 3, 1	10, 36, 2, 22, 1	55
* 91	103, 7	2	2, 5, 2, 3, 0	7, 5, 0, 5, 5	2, 1, 36, 24, 14	25
2621	103, 5	0	4, 1, 4, 3, 0	<i>aw</i>	16, 23, 36, 0, 4	55
71	108, 14	1	3, 0, 3, 5, 1	0, 5, 6, 3, 3	6, 12, 6, 25, 36	55
2711	107, 11	1	0, 4, 5, 1, 1	5, 5, 3, 4, 1	30, 28, 2, 16, 15	5
31	112, 18	2	5, 2, 4, 0, 0	7, 3, 2, 4, 5	33, 6, 30, 4, 12	20
41	113, 19	1	6, 2, 1, 2, 1	4, 6, 5, 1, 3	38, 20, 4, 18, 3	5
91	108, 10	0	3, 3, 4, 1, 3	<i>aw</i>	8, 15, 6, 12, 42	45
2801	107, 7	2	1, 6, 2, 1, 1	6, 9, 7, 2, 1	14, 6, 7, 42, 14	55
51	107, 3	2	4, 3, 3, 3, 0	4, 6, 7, 2, 6	16, 9, 42, 12, 6	45
61	107, 1	1	0, 1, 5, 4, 1	0, 5, 3, 4, 4	0, 28, 23, 24, 20	95
2971	117, 19	1	3, 6, 1, 0, 1	1, 1, 4, 3, 5	4, 23, 14, 40, 6	55
*3001	122, 24	1	2, 1, 2, 2, 6	4, 4, 4, 1, 1	24, 0, 40, 15, 0	25
11	112, 10	0	2, 2, 1, 0, 6	<i>aw</i>	0, 7, 42, 14, 20	55
41	113, 11	1	1, 3, 4, 2, 4	6, 4, 0, 1, 2	42, 20, 16, 2, 3	5
61	117, 17	2	1, 4, 1, 5, 2	7, 7, 4, 10, 1	35, 2, 8, 16, 30	20
3121	123, 23	2	0, 1, 6, 2, 3	4, 6, 9, 3, 10	9, 38, 6, 30, 6	80
81	113, 3	2	1, 5, 0, 2, 4	3, 7, 5, 2, 9	2, 36, 20, 26, 13	95
91	113, 1	1	1, 4, 0, 2, 5	1, 4, 5, 4, 3	2, 25, 36, 12, 22	95
3221	122, 20	0	5, 0, 4, 2, 2	<i>aw</i>	26, 22, 24, 0, 26	20
* 51	127, 25	0	1, 0, 5, 5, 0	<i>aw</i>	1, 20, 20, 30, 30	100
71	117, 11	1	2, 1, 1, 5, 4	6, 1, 6, 3, 0	26, 23, 16, 0, 34	5
3301	118, 12	2	2, 1, 5, 3, 3	4, 6, 7, 5, 2	1, 26, 2, 42, 14	80
31	123, 19	1	2, 5, 4, 2, 1	7, 2, 2, 6, 0	33, 24, 0, 26, 18	20
61	117, 7	2	1, 2, 5, 1, 4	7, 8, 6, 0, 6	35, 28, 22, 14, 0	20
91	117, 5	0	1, 1, 0, 6, 3	<i>aw</i>	23, 20, 4, 2, 42	20
3461	118, 4	1	1, 6, 1, 1, 3	2, 3, 6, 5, 1	0, 28, 8, 39, 20	95
91	128, 22	2	3, 1, 4, 1, 5	2, 3, 6, 1, 8	22, 15, 36, 28, 2	5
3511	132, 26	1	0, 6, 2, 3, 2	5, 5, 2, 6, 4	20, 2, 8, 46, 15	55
41	122, 12	2	3, 0, 0, 6, 2	9, 4, 5, 9, 2	3, 30, 4, 12, 42	20
* 71	123, 13	2	5, 2, 4, 1, 2	9, 3, 3, 7, 8	36, 12, 33, 2, 18	25
81	127, 19	1	4, 5, 1, 0, 3	2, 3, 5, 2, 4	18, 34, 15, 31, 2	55
3631	123, 11	1	3, 0, 6, 2, 1	3, 2, 3, 4, 5	12, 39, 30, 4, 18	55
71	127, 17	2	2, 6, 1, 3, 1	0, 10, 4, 7, 8	6, 8, 34, 40, 9	5
91	128, 18	2	3, 1, 1, 4, 5	8, 2, 9, 6, 7	12, 40, 26, 2, 23	45
3701	122, 4	1	2, 2, 5, 4, 0	1, 4, 2, 0, 7	6, 29, 42, 8, 16	95
61	133, 23	2	6, 2, 3, 1, 2	10, 5, 7, 9, 1	35, 12, 2, 6, 40	20
3821	127, 13	2	3, 4, 1, 3, 4	5, 5, 6, 2, 7	9, 48, 16, 20, 4	80
* 51	128, 14	1	5, 1, 0, 5, 1	4, 5, 5, 5, 0	34, 25, 0, 30, 20	25

<i>p</i>	<i>X, Y</i>	<i>3XY</i>	Prime Factors.		Reciprocal Factor.	<i>Q</i>
			Simplest, = $a\omega$.	Simplest primary.		
3881	127, 11	1	1, 5, 4, 0, 3	2, 3, 5, 7, 1	7, 6, 10, 34, 42	80
3911	137, 25	0	2, 3, 1, 5, 4	$a\omega$	0, 47, 22, 6, 20	55
31	127, 9	1	6, 3, 1, 2, 1	3, 3, 5, 3, 4	48, 24, 15, 6, 2	5
4001	127, 5	0	1, 1, 2, 3, 6	$a\omega$	24, 16, 48, 8, 1	55
* 21	127, 3	2	3, 1, 0, 5, 4	0, 4, 6, 9, 6	6, 42, 18, 2, 33	25
51	128, 6	1	5, 3, 0, 3, 3	1, 4, 7, 2, 1	24, 49, 2, 8, 14	45
91	128, 2	2	3, 4, 1, 1, 5	3, 8, 1, 6, 8	8, 10, 36, 7, 42	95
4111	132, 14	1	0, 4, 0, 6, 1	5, 0, 2, 1, 6	30, 2, 23, 16, 40	45
4201	143, 27	2	3, 4, 5, 2, 2	1, 6, 7, 5, 3	6, 26, 2, 23, 40	45
11	133, 13	2	4, 0, 1, 1, 6	10, 5, 2, 4, 9	15, 2, 38, 36, 20	20
31	132, 10	0	2, 2, 3, 6, 0	$a\omega$	2, 1, 20, 26, 48	95
41	137, 16	1	1, 2, 4, 3, 5	7, 3, 1, 1, 2	48, 10, 29, 2, 12	5
61	138, 20	0	5, 5, 2, 1, 1	$a\omega$	30, 13, 42, 24, 0	5
71	133, 11	1	3, 5, 2, 0, 4	0, 0, 4, 7, 2	6, 2, 24, 20, 49	95
*4391	133, 5	0	2, 0, 5, 0, 5	$a\omega$	22, 24, 34, 36, 1	25
4421	133, 1	1	3, 1, 2, 6, 2	5, 5, 4, 3, 2	4, 22, 6, 20, 51	55
* 41	138, 16	1	1, 3, 1, 6, 3	6, 2, 3, 3, 3	42, 6, 6, 14, 39	25
51	143, 23	2	2, 3, 2, 5, 4	9, 4, 8, 10, 3	46, 9, 12, 8, 34	5
* 81	137, 13	2	5, 2, 4, 1, 3	8, 4, 6, 6, 1	28, 22, 3, 2, 48	25
4561	143, 21	1	6, 2, 3, 0, 3	2, 2, 4, 5, 4	50, 2, 22, 6, 25	5
91	137, 9	1	1, 5, 3, 4, 2	7, 2, 1, 4, 2	48, 10, 6, 33, 12	5
*4621	147, 25	0	5, 4, 1, 4, 1	$a\omega$	34, 47, 2, 2, 18	25
* 51	152, 30	0	6, 5, 0, 0, 0	$a\omega$	36, 30, 30, 25, 0	25
* 91	137, 1	1	6, 4, 1, 1, 1	3, 5, 5, 0, 5	42, 34, 24, 16, 1	25
4721	142, 16	1	2, 1, 4, 0, 6	4, 6, 4, 3, 5	16, 12, 46, 35, 6	5
* 51	143, 17	2	2, 6, 1, 1, 4	4, 9, 6, 4, 1	1, 30, 0, 50, 20	100
4801	153, 26	1	5, 2, 1, 4, 4	6, 1, 8, 2, 4	14, 51, 12, 3, 24	45
31	143, 15	0	3, 3, 0, 2, 6	$a\omega$	2, 16, 50, 4, 33	95
61	142, 12	2	1, 2, 0, 4, 6	3, 3, 6, 10, 9	15, 42, 42, 6, 10	80
* 71	148, 22	2	0, 7, 1, 1, 3	4, 8, 7, 3, 2	6, 18, 2, 52, 28	100
4931	152, 26	1	1, 2, 6, 2, 4	8, 2, 5, 3, 4	47, 36, 20, 6, 2	20
51	147, 19	1	2, 2, 5, 1, 5	4, 6, 3, 0, 3	24, 34, 28, 38, 1	45
5011	143, 9	1	1, 6, 1, 4, 2	7, 3, 1, 0, 6	40, 2, 22, 39, 20	5
21	142, 4	1	3, 4, 4, 0, 4	4, 4, 1, 7, 0	9, 12, 16, 20, 56	80
51	143, 7	2	7, 2, 2, 0, 1	6, 1, 8, 5, 3	54, 9, 28, 2, 16	5
* 81	143, 5	0	2, 1, 4, 1, 6	$a\omega$	18, 23, 38, 42, 2	25
5101	143, 3	2	3, 6, 0, 2, 3	6, 6, 8, 5, 2	14, 49, 2, 38, 6	95
71	152, 22	2	2, 4, 6, 2, 1	10, 5, 6, 8, 3	36, 42, 1, 20, 26	5
5231	148, 14	1	3, 5, 1, 3, 4	3, 2, 8, 1, 5	12, 56, 15, 26, 2	95
61	158, 28	2	1, 5, 6, 1, 1	5, 10, 12, 6, 1	36, 47, 2, 11, 36	5
* 81	162, 32	2	0, 4, 2, 3, 6	2, 6, 9, 11, 9	2, 38, 42, 22, 23	125
5351	148, 10	0	1, 4, 3, 5, 3	$a\omega$	56, 6, 2, 23, 24	5
* 81	157, 25	0	3, 1, 6, 4, 1	$a\omega$	13, 42, 48, 8, 2	100
5431	148, 6	1	3, 1, 7, 1, 0	2, 3, 3, 6, 5	2, 54, 25, 4, 28	55
41	163, 31	1	4, 3, 6, 2, 1	1, 1, 0, 4, 7	23, 30, 54, 2, 2	80

p	X, Y	$3XY$	Prime Factors.		Reciprocal Factor.	Q
			Simplest, = $a\omega$.	Simplest primary.		
5471	148, 2	2	0, 1, 3, 5, 5	0, 4, 1, 7, 10	49, 12, 34, 0, 26	20
5501	157, 23	2	1, 1, 3, 4, 0	4, 1, 2, 7, 9	34, 26, 48, 3, 16	55
21	158, 24	1	3, 6, 3, 1, 3	5, 5, 1, 8, 2	4, 8, 14, 35, 54	95
*	31	1	0, 4, 2, 2, 1	3, 4, 6, 1, 4	48, 38, 23, 12, 2	25
81	162, 28	2	5, 2, 6, 0, 0	3, 3, 8, 6, 5	13, 46, 20, 4, 42	20
*	91	1	1, 2, 6, 4, 3	1, 8, 3, 2, 7	2, 39, 16, 46, 24	125
*5641	153, 13	2	2, 3, 0, 0, 7	2, 10, 5, 5, 10	3, 16, 54, 6, 36	100
51	152, 10	0	4, 6, 2, 2, 1	$a\omega$	16, 16, 47, 42, 6	5
5701	153, 11	1	0, 3, 6, 1, 4	6, 4, 3, 2, 4	30, 51, 12, 22, 6	55
11	157, 19	1	5, 1, 0, 6, 1	0, 5, 7, 1, 1	25, 42, 2, 24, 40	20
41	158, 20	0	3, 7, 1, 1, 2	$a\omega$	8, 40, 9, 52, 12	95
91	153, 7	2	3, 4, 6, 1, 0	8, 3, 9, 6, 2	12, 50, 9, 12, 42	5
*5801	157, 17	2	6, 5, 1, 1, 0	11, 10, 5, 0, 5	46, 35, 30, 20, 0	25
21	153, 5	0	6, 4, 1, 3, 0	$a\omega$	51, 42, 16, 0, 6	20
51	153, 1	1	0, 3, 0, 7, 2	6, 1, 3, 3, 0	36, 9, 18, 8, 54	55
61	163, 25	0	0, 0, 7, 1, 4	$a\omega$	25, 52, 8, 36, 0	80
*	81	0	3, 1, 1, 6, 4	$a\omega$	12, 48, 22, 3, 42	25
5931	163, 23	2	1, 0, 5, 2, 6	2, 8, 10, 3, 11	18, 34, 30, 49, 2	55
*6011	157, 11	1	5, 3, 5, 0, 2	5, 2, 3, 8, 2	20, 34, 6, 9, 56	25
91	163, 21	1	1, 6, 5, 2, 0	6, 1, 0, 6, 2	42, 20, 4, 47, 22	45
*6101	157, 7	2	1, 0, 1, 6, 5	4, 0, 5, 10, 10	34, 35, 30, 0, 40	25
21	173, 33	2	5, 4, 4, 3, 2	6, 9, 11, 2, 10	26, 8, 61, 20, 6	55
31	157, 5	0	7, 3, 2, 1, 0	$a\omega$	58, 24, 30, 4, 7	5
51	157, 3	2	4, 1, 3, 1, 6	9, 6, 3, 2, 9	6, 9, 48, 48, 14	5
*6211	168, 26	1	1, 4, 5, 5, 1	2, 3, 2, 3, 7	0, 26, 54, 9, 36	125
21	158, 4	1	2, 5, 3, 5, 1	5, 0, 1, 3, 8	9, 8, 56, 20, 36	80
*	71	0	0, 4, 1, 4, 6	$a\omega$	6, 47, 48, 18, 12	125
6301	177, 35	0	1, 1, 2, 7, 4	$a\omega$	24, 26, 2, 8, 61	45
11	167, 23	2	4, 4, 1, 5, 3	8, 2, 6, 5, 6	20, 62, 12, 6, 25	55
61	163, 15	0	0, 5, 2, 6, 1	$a\omega$	25, 2, 42, 14, 50	80
6421	167, 21	1	3, 2, 7, 2, 1	1, 4, 4, 8, 5	4, 57, 24, 0, 36	45
51	168, 22	2	7, 1, 0, 3, 3	9, 6, 2, 0, 7	54, 9, 12, 42, 16	5
81	162, 8	2	0, 2, 6, 0, 5	7, 8, 8, 1, 5	42, 46, 25, 26, 2	45
*	91	1	6, 1, 2, 3, 4	4, 7, 3, 3, 2	38, 1, 24, 56, 6	25
6521	167, 19	1	2, 3, 2, 7, 1	4, 4, 4, 3, 5	16, 8, 24, 15, 64	95
51	172, 26	1	2, 4, 3, 6, 2	6, 1, 2, 5, 8	14, 9, 52, 12, 46	95
71	173, 27	2	0, 6, 3, 5, 0	6, 9, 4, 2, 5	49, 8, 16, 50, 6	20
81	163, 7	2	4, 0, 5, 3, 4	2, 7, 5, 7, 9	7, 24, 20, 64, 12	80
6661	182, 36	1	0, 1, 0, 6, 6	5, 0, 7, 6, 6	30, 42, 42, 1, 30	55
91	167, 15	0	4, 4, 5, 1, 3	$a\omega$	12, 30, 4, 18, 63	55
6701	173, 25	0	1, 6, 2, 5, 2	$a\omega$	56, 6, 13, 38, 24	5
61	167, 13	2	4, 1, 1, 0, 7	3, 8, 4, 5, 9	10, 2, 57, 34, 30	55
81	177, 29	1	1, 5, 4, 5, 2	7, 3, 0, 2, 4	62, 16, 0, 31, 13	5
91	172, 22	2	7, 0, 0, 4, 2	11, 6, 5, 11, 2	57, 20, 4, 42, 2	20
*6841	183, 35	0	7, 0, 5, 0, 0	$a\omega$	48, 24, 36, 1, 36	25

p	X, Y	$3XY$	Primo Factors.		Reciprocal Factor.	Q
			Simplest, $=a\omega$.	Simplest primary.		
*6871	167, 9	1	3, 0, 3, 7, 0	4, 7, 3, 3, 3	9, 12, 12, 42, 58	100
6911	167, 7	2	1, 1, 6, 5, 2	2, 8, 9, 5, 9	0, 48, 38, 34, 25	145
61	167, 3	2	1, 2, 5, 6, 1	2, 2, 9, 10, 6	0, 33, 48, 21, 40	145
71	167, 1	1	2, 7, 2, 3, 1	6, 4, 4, 3, 5	26, 8, 24, 65, 6	55
91	172, 18	2	2, 5, 0, 6, 2	4, 9, 0, 9, 3	38, 0, 36, 33, 42	45
7001	182, 32	2	4, 2, 2, 7, 0	9, 9, 2, 13, 4	6, 16, 12, 38, 61	95
7131	173, 17	2	5, 1, 6, 2, 2	9, 1, 9, 2, 5	36, 38, 46, 0, 20	55
51	172, 14	1	2, 2, 0, 6, 5	6, 1, 7, 0, 2	14, 56, 33, 2, 36	55
*7211	187, 35	0	2, 2, 3, 3, 7	$a\omega$	50, 4, 54, 16, 9	25
7321	183, 29	1	7, 1, 2, 4, 2	5, 5, 6, 7, 2	66, 22, 6, 30, 9	5
31	173, 11	1	7, 0, 1, 2, 4	2, 7, 2, 6, 0	52, 6, 20, 49, 18	5
51	172, 6	1	2, 7, 0, 4, 0	4, 4, 2, 5, 7	24, 6, 42, 57, 16	5
7411	192, 38	2	4, 4, 4, 5, 2	3, 7, 6, 5, 6	10, 18, 68, 16, 25	95
* 51	173, 5	0	1, 4, 1, 6, 4	$a\omega$	56, 10, 0, 15, 50	25
81	173, 1	1	2, 5, 1, 2, 6	2, 3, 7, 4, 5	2, 56, 35, 36, 18	145
7541	187, 31	1	6, 5, 2, 1, 3	3, 2, 9, 1, 7	42, 50, 26, 33, 2	55
61	182, 24	1	0, 6, 0, 1, 6	0, 0, 7, 6, 1	0, 42, 42, 36, 35	155
91	183, 25	0	2, 2, 4, 1, 7	$a\omega$	22, 0, 66, 33, 12	45
7621	177, 13	2	7, 1, 1, 2, 4	10, 5, 4, 8, 2	64, 8, 6, 35, 26	5
81	177, 11	1	1, 2, 4, 7, 1	3, 8, 0, 3, 6	2, 16, 35, 36, 58	145
91	187, 29	1	6, 2, 1, 3, 5	3, 7, 1, 4, 3	42, 0, 34, 52, 23	5
7741	178, 12	2	3, 2, 1, 7, 3	2, 2, 6, 11, 7	22, 30, 4, 13, 68	55
7841	178, 8	2	7, 2, 1, 3, 3	12, 8, 4, 1, 7	68, 20, 4, 33, 12	5
7901	178, 4	1	5, 3, 6, 1, 1	6, 1, 3, 7, 4	14, 51, 18, 8, 56	5
51	193, 33	2	2, 4, 0, 7, 3	9, 6, 3, 10, 12	46, 4, 28, 23, 54	55
*8011	183, 17	2	6, 0, 3, 2, 5	5, 7, 2, 8, 8	30, 6, 36, 61, 9	25
81	187, 23	2	0, 7, 1, 0, 5	2, 8, 8, 6, 5	2, 34, 25, 54, 42	155
8101	182, 12	2	6, 1, 2, 4, 4	11, 9, 7, 2, 6	46, 6, 18, 63, 6	45
11	193, 31	1	1, 4, 4, 6, 3	8, 2, 1, 0, 4	70, 7, 8, 24, 30	5
61	183, 13	2	4, 5, 4, 4, 1	10, 5, 3, 9, 9	15, 12, 72, 24, 20	80
* 71	197, 35	0	5, 1, 1, 6, 4	$a\omega$	4, 62, 18, 7, 48	25
91	187, 21	1	1, 5, 2, 6, 3	8, 3, 4, 6, 3	63, 0, 6, 28, 42	20
8221	183, 11	1	2, 4, 2, 1, 7	0, 5, 4, 7, 3	6, 22, 54, 15, 54	145
31	188, 22	2	1, 0, 5, 7, 1	3, 8, 5, 8, 6	2, 24, 30, 49, 52	155
91	187, 19	1	1, 7, 4, 3, 0	7, 3, 4, 4, 2	48, 20, 6, 58, 23	55
8311	183, 7	2	1, 2, 2, 4, 7	5, 5, 8, 1, 11	30, 33, 68, 6, 0	95
8431	188, 18	2	1, 8, 3, 1, 1	8, 12, 10, 3, 1	28, 6, 10, 71, 28	95
61	187, 15	0	3, 2, 1, 5, 6	$a\omega$	15, 62, 42, 6, 30	80
8501	197, 31	1	7, 4, 3, 1, 2	6, 4, 3, 5, 8	61, 6, 52, 12, 14	20
21	198, 32	2	5, 1, 2, 5, 5	9, 6, 6, 2, 5	36, 3, 24, 70, 6	55
* 81	202, 36	1	4, 6, 2, 3, 4	2, 6, 9, 6, 1	18, 68, 12, 42, 3	125
8641	187, 9	1	1, 0, 3, 4, 7	7, 3, 6, 1, 3	48, 15, 61, 12, 12	55
81	187, 7	2	5, 3, 4, 0, 5	7, 2, 7, 9, 10	33, 16, 20, 4, 72	80
8731	187, 3	2	0, 3, 4, 5, 5	8, 7, 2, 6, 10	72, 6, 30, 9, 28	5
41	187, 1	1	1, 3, 4, 7, 0	3, 3, 4, 4, 8	8, 20, 56, 12, 57	145

<i>p</i>	<i>X, Y</i>	<i>3XY</i>	Prime Factors.		Reciprocal Factor.	<i>Q</i>
			Simplest, = $a\omega$.	Simplest primary.		
8761	193, 21	1	0, 2, 2, 5, 3	2, 7, 4, 5, 1	50, 18, 8, 01, 20	55
8821	198, 28	2	5, 1, 1, 7, 2	11, 0, 6, 13, 0	6, 42, 1, 30, 66	55
* 31	188, 2	2	4, 3, 1, 1, 7	2, 9, 4, 6, 11	7, 12, 68, 22, 42	100
* 61	193, 10	1	1, 5, 4, 0, 0	3, 7, 2, 3, 8	10, 16, 04, 6, 51	125
8941	203, 33	2	8, 1, 1, 4, 0	13, 3, 9, 11, 2	68, 40, 9, 28, 8	5
51	193, 17	2	2, 7, 3, 0, 4	1, 11, 3, 5, 8	0, 34, 7, 68, 30	145
71	192, 14	1	2, 6, 0, 0, 1	0, 1, 1, 8, 0	26, 42, 1, 40, 56	55
9001	207, 37	2	4, 1, 7, 4, 1	4, 4, 12, 12, 9	10, 64, 47, 8, 24	95
* 11	208, 38	2	1, 5, 3, 7, 0	5, 12, 2, 13, 8	20, 6, 49, 4, 66	125
41	197, 23	2	3, 1, 4, 2, 7	9, 0, 5, 1, 8	3, 20, 54, 62, 8	20
* 91	192, 10	0	1, 2, 8, 2, 2	$a\omega$	23, 70, 14, 24, 14	100
9151	197, 21	1	2, 7, 0, 1, 5	1, 4, 7, 5, 7	0, 56, 18, 57, 24	155
61	193, 11	1	0, 1, 1, 6, 2	2, 8, 0, 0, 1	50, 28, 3, 50, 30	55
81	207, 35	0	2, 7, 2, 1, 5	$a\omega$	2, 14, 30, 40, 62	155
9221	202, 28	2	8, 0, 3, 2, 2	10, 5, 1, 3, 8	74, 3, 14, 20, 36	5
* 41	213, 41	1	4, 7, 1, 4, 2	4, 3, 3, 2, 7	12, 0, 01, 54, 24	25
81	193, 5	0	8, 2, 0, 3, 1	$a\omega$	72, 30, 10, 20, 2	5
9311	193, 1	1	1, 3, 8, 0, 2	7, 3, 4, 5, 4	40, 72, 2, 0, 25	55
41	197, 17	2	2, 5, 0, 1, 7	1, 11, 5, 6, 12	2, 30, 61, 13, 48	155
* 71	208, 34	1	7, 3, 4, 1, 3	5, 4, 1, 0, 9	66, 7, 48, 2, 28	25
91	203, 27	2	3, 1, 0, 6, 0	3, 7, 9, 4, 7	8, 50, 64, 18, 23	155
9421	197, 15	0	0, 5, 1, 7, 2	$a\omega$	56, 3, 24, 30, 54	45
* 31	212, 38	2	5, 2, 6, 4, 2	7, 4, 9, 1, 6	33, 42, 68, 2, 8	100
61	217, 43	2	1, 7, 0, 6, 1	7, 8, 1, 5, 6	35, 2, 48, 50, 30	20
91	197, 13	2	3, 1, 4, 7, 2	4, 0, 10, 9, 2	12, 10, 16, 62, 57	145
9511	207, 31	1	5, 0, 3, 3, 2	0, 5, 7, 1, 0	25, 12, 68, 46, 10	20
21	203, 25	0	4, 1, 6, 2, 5	$a\omega$	9, 38, 34, 70, 6	80
51	197, 11	1	8, 1, 2, 1, 3	4, 6, 2, 5, 7	70, 6, 12, 23, 34	5
9601	197, 9	1	3, 3, 5, 6, 0	1, 6, 3, 0, 8	0, 34, 72, 3, 30	145
31	213, 37	2	4, 5, 5, 2, 4	7, 7, 5, 7, 4	12, 24, 15, 26, 78	95
* 61	207, 29	1	0, 7, 5, 0, 3	5, 3, 3, 7, 2	20, 4, 0, 01, 56	125
9721	198, 8	2	5, 6, 1, 3, 3	9, 0, 9, 2, 10	36, 72, 0, 35, 6	95
81	198, 4	1	2, 1, 7, 1, 5	7, 8, 3, 1, 0	33, 54, 30, 54, 2	80
91	212, 34	1	4, 0, 2, 1, 8	3, 7, 4, 4, 2	8, 0, 74, 42, 23	55
9811	213, 35	0	5, 5, 2, 4, 4	$a\omega$	30, 78, 8, 24, 15	95
51	203, 19	1	5, 7, 0, 2, 2	4, 6, 8, 3, 4	34, 64, 18, 48, 1	95
71	217, 39	1	7, 3, 3, 2, 4	1, 4, 1, 7, 5	54, 12, 10, 15, 66	55
* 9901	222, 44	1	2, 8, 1, 4, 2	6, 1, 4, 1, 6	14, 15, 50, 70, 10	25
* 31	207, 25	0	7, 1, 4, 1, 4	$a\omega$	58, 22, 8, 8, 63	25
* 41	203, 17	2	2, 2, 5, 0, 7	3, 5, 10, 0, 10	42, 34, 54, 40, 1	25
98801	653, 79	1	10, 3, 10, 7, 2	6, 1, 3, 13, 16	114, 131, 218, 8, 30	305
* 98911	637, 45	0	12, 3, 7, 2, 7	$a\omega$	180, 54, 0, 36, 206	125
98981	662, 92	2	10, 2, 6, 5, 10	22, 18, 13, 1, 15	88, 30, 120, 236, 7	145
1562051	2552, 230	0	14, 4, 13, 8, 24	$a\omega$	90, 209, 678, 848, 134	245
1671781	2587, 33	2	5, 23, 2, 21, 6	18, 38, 3, 39, 15	642, 0, 510, 034, 513	305