# 611.

## REPORT OF THE COMMITTEE ON MATHEMATICAL TABLES:

CONSISTING OF PROFESSOR CAYLEY, F.R.S., PROFESSOR STOKES, F.R.S., PROFESSOR SIR W. THOMSON, F.R.S., PROFESSOR H. J. S. SMITH, F.R.S., AND J. W. L. GLAISHER, F.R.S.

[From the *Report of the British Association for the Advancement of Science* (1875), pp. 305—336.]

THE present Report (say Report 1875) is in continuation of that by Mr Glaisher, published in the volume for 1873, and here cited as Report 1873.

Report 1873 extends to all those tables which are at p. 3 (*l.c.*) included under the headings:—

A, auxiliary for non-logarithmic calculation, 1, 2, 3;

B, logarithmic and circular, 4, 5, 6;

C, exponential, 7, 8 (but only partially to C. 8), other than those tables of C referred to as "$\text{h}.\text{l}\tan(45^\circ+\frac{1}{2}\phi)$"; and also partially (see Art. 24, pp. 81—83) to the tables included under the heading "E. 11, transcendental constants $\epsilon$, $\pi$, $\gamma$, &c., and their powers and functions."

A future Report will comprise the tables, or further tables, included under the headings:—

C. 8. Hyperbolic antilogarithms ($e^x$) and $\text{h}.\text{l}\tan(45^\circ+\frac{1}{2}\phi)$, and hyperbolic sines, cosines, &c.

D. Algebraic constants.

9. Accurate integer or fractional values. Bernoulli's Numbers, $\Delta^n 0^m$, &c. Binomial coefficients.

10. Decimal values auxiliary to the calculation of series.

E. 11. Transcendental constants $\epsilon$, $\pi$, $\gamma$, &c., and their powers and functions.

www.rcin.org.pl

The present Report (1875) comprises the tables included under the headings:—

F. Arithmological.

12. Divisors and prime numbers. Prime roots. The Canon arithmeticus, &c.

13. The Pellian equation.

14. Partitions.

15. Quadratic forms $a^2 + b^2$, &c., and partitions of numbers into squares, cubes, and biquadrates.

16. Binary, ternary, &c., quadratic and higher forms.

17. Complex theories:

which divisions are herein referred to, for instance, as [F. 12. Divisors, &c.].

Report 1873 consists of six sections (§) divided into articles, which are separately numbered (see contents, p. 174); the present Report 1875 forms a single section (§ 7), divided in like manner into articles, which are separately numbered; but besides this the paragraphs are numbered, and that continuously, through the present Report 1875, so that any paragraph may be cited as Report 1875, No. — , as the case may be.

[F. 12. *Divisors, &c.*] *Divisors and Prime Numbers.* Art. I.

1. As to divisors and prime numbers see Report 1873, Art. 8 (Tables of Divisors—factor tables—and Tables of Primes), pp. 34—40. The tables there referred to, such as Chernac, Burckhardt, Dase, Dase and Rosenberg, are chiefly tables running up to very high numbers (the last of them the ninth million): wherein, to save space, multiples of 2, 3, 5 are frequently omitted, and in some of them only the least divisor is given. It would be for many purposes convenient to have a small table, going up say to 10,000, showing in every case all the prime factors of the number. Such a table might be arranged, 500 numbers in a page, in some such form as the following:—

Factor Table | 1 to 500 |

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 39 | 2.3.5.13 | 17.23 | $2^3.7^2$ | 3.131 | 2.197 | 5.79 | $2^2.3^2.11$ | 397* | 2.199 | 3.7.19 |

where the top line shows the units, and the left-hand column the remaining figures, viz. the specimen exhibits the composition of the several numbers from 390 to 399: a prime number, e.g. 397, would be sufficiently indicated by the absence of any decomposition, or it may be further indicated by an asterisk.

It may be noticed that, in the theory of numbers, the decomposition is specially required when the next following number is a prime, viz. that of $p-1$, $p$ being a

www.rcin.org.pl

prime: also, that this is given incidentally, for prime numbers $p$ up to 1000, in Jacobi's *Canon Arithmeticus, post*, No. 20, and up to 15,000 in Reuschle's Tables, V. (a, b, c) *post*, No. 22.

2. It may be proper to remark here that any table of a binary form is really a factor-table in the complex theory connected with such binary form. Thus in a table of the form $a^2+b^2$, a number of this form has a factor $a+bi$ ($i=\sqrt{-1}$ as usual); and the table, in fact, shows the complex factor $a+bi$ of the number in question: a well arranged table would give all the prime complex factors $a+bi$ of the number. But as to this more hereafter; at present, we are concerned with the real theory only, not with any complex theory.

3. Connected with a factor-table, we have (i) a Table of the number of less relative primes; viz. such a table would show, for every number, the number of inferior integers having no common factor with the number itself. The formula is a well-known one: for a number $N=a^\alpha b^\beta c^\gamma \ldots$, ($a, b, \ldots$ the distinct prime factors of $N$), the number of less relative primes is

$$\varpi(N), \ = a^{\alpha-1} b^{\beta-1} \ldots (a-1)(b-1) \ldots,$$

or, what is the same thing, $=N\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\ldots$ A small table ($N=1$ to 100), occupying half a page, is given by

**Euler,** *Op. Arith. Coll.* t. II. p. 128; viz. this is $\pi 1=0$, $\pi 2=1, \ldots$, $\pi 100=40$.

4. But it would be interesting to have such a table of the same extent with the proposed factor-table. The table might be of like form; for instance,

Number of less relative Primes Table | 1 to 500

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 29 | 112 | 192 | 144 | 292 | 84 | 232 | 144 | 198 | 148 | 264 |

It would be of still greater interest to have an inverse table showing the values of $N$ which belong to a given value of $\varpi(N)$; for instance,

| $\varpi=$ | $N=$ |
|---|---|
| 40 | 41, 55, 75, 82, 88, 100, 110, |
| 42 | 43, 49, 86, 98, |
| 44 | 69, 92, |
| 46 | 47, 94, |
| 48 | 65, 104, 105, 112, |
| ⋮ | |

where, observe, that $\varpi$ is of necessity even.

www.rcin.org.pl

5. Again, connected with a factor-table, we have (ii) a Table of the Sum of the divisors of a Number. The formula is also a well-known one; for a number $N = a^\alpha b^\beta \ldots$, ($a, b, \ldots$ the distinct prime factors of $N$), the required sum

$$\int N \text{ is } = (1 + a + \ldots + a^\alpha)(1 + b + \ldots + b^\beta) \ldots,$$

or, what is the same thing,

$$= \frac{a^{\alpha+1} - 1}{a - 1} \cdot \frac{b^{\beta+1} - 1}{b - 1} \ldots,$$

where, observe, that the number itself is reckoned as a divisor.

6. Such a table was required by Euler in his researches on Amicable Numbers (see *post*, No. 10), and he accordingly gives one of a considerable extent, viz.

**Euler,** *Op. Arith. Coll.* t. I. pp. 104—109.

It is to be remarked that, inasmuch as $\int N$ is obviously $= \int a^\alpha \int b^\beta \ldots$, the function need only be tabulated for the different integer powers $a^\alpha$ of each prime number $a$. The range of Euler's table is as follows:—

| $a =$ | $\alpha =$ |
|---|---|
| 2 | 1 to 36, |
| 3 | 1 „ 15, |
| 5 | 1 „ 9, |
| 7 | 1 „ 10, |
| 11 | 1 „ 9, |
| 13 | 1 „ 7, |
| 17 | 1 „ 5, |
| 19 | 1 „ 5, |
| 23 | 1 „ 4, |
| 29 to 997 | 1 „ 3, |

viz. for the several prime numbers from 29 to 997 the table gives $\int a$, $\int a^2$, and $\int a^3$. And it is to be noticed that the values of the sum are exhibited, decomposed into their prime factors: thus a specimen of the table is

| Num. | Summa Divisorum. |
|---|---|
| 139 | $2^2 . 5 . 7$ |
| $139^2$ | $3 . 13 . 499$ |
| $139^3$ | $2^3 . 5 . 7 . 9661$ |

www.rcin.org.pl

7. The form of the above table is adapted to its particular purpose (the theory of amicable numbers); but Euler gives also,

**Euler,** *Op. Arith. Coll.* t. I. p. 147—in the paper "Observatio de Summis Divisorum," (1752), pp. 146—154,—a short table of about half a page, $N=1$ to 100, of the form $\int 1=1$, $\int 2=3,\ldots,\int 100=217$. The paper contains interesting analytical researches on the subject of $\int N$ which connect themselves with the theory of the Partition of Numbers.

8. It would be interesting to carry the last-mentioned table to the same extent as the proposed factor-table; and to add to it an inverse table, as suggested in regard to the number of less relative primes table.

9. *Perfect Numbers.*—A perfect number is a number which is equal to the sum of its divisors, the number itself not being reckoned as a divisor; e.g.

$$6=1+2+3, \text{ and } 28=1+2+4+7+14.$$

Such numbers are indicated by a table of the sums of divisors $\int 6=12$, $\int 28=56$, these two being, as appears by the table, Art. 7, the only perfect numbers less than 100.

10. *Amicable Numbers.*—These are pairs of numbers such that each is equal to the sum of the divisors of the other, not reckoning the other number as a divisor; that is, each has the same sum of divisors, the number being here reckoned as a divisor; say $\int' A=B$, $\int' B=A$; or, what is the same thing, $\int A=\int B\,(=A+B)$. Thus for the numbers 220, 284,

$$\int' 220=(1+2+4)(1+5)(1+11)-220, =284,$$

$$\int' 284=(1+2+4)(1+71)-284, \qquad =220;$$

or, what is the same thing,

$$\int 220=(1+2+4)(1+5)(1+11)=504=(1+2+4)(1+71)=\int 284.$$

11. A catalogue of 61 pairs of numbers is given by

**Euler,** *Op. Arith. Coll.* t. I. pp. 144—145; it occupies about one page. The paper, "De Numeris Amicabilibus," pp. 102—145, contains an elaborate investigation of the theory, by means whereof all but two of the pairs of numbers are obtained. The first pair is the above-mentioned one, $2^2.5.11$ and $2^2.71$ (=220 and 284); and the fifty-ninth pair is the high numbers

$$3^5.7^2.13.19.53.6959 \text{ and } 3^5.7^2.13.19.179.2087.$$



www.rcin.org.pl

The last two pairs are referred to as "formæ diversæ a precedentibus;" viz. these are

$$\begin{cases} 2^3 . 19 . 41 \\ 2^5 . 199 \end{cases} \text{and} \begin{cases} 2^3 . 41 . 467 \\ 2^5 . 19 . 233. \end{cases}$$

12. A Table of the Frequency of Primes is given by

**Gauss,** Tafel der Frequenz der Primzahlen, *Werke,* t. II. pp. 436—443; viz. this extends to 3,000,000.

The first part, extending to 1,000,000, = 1000 thousand, shows how many primes there are in each thousand: a specimen is

1, 168:
2, 135:
3, 127:
4, 120:
5, 119:
&c.;

viz. in the first thousand there are 168 primes, in the second thousand 135 primes, and so on.

For the second and third millions the frequency is given for each ten thousand: a specimen is

1,000,000 to 1,100,000.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | | | | | | | | | | 1 |
| 2 | | 1 | | | | 1 | | 1 | 1 | | 4 |
| 3 | | 4 | 2 | 2 | 3 | 1 | 2 | 3 | 3 | 1 | 21 |
| 4 | 2 | 8 | 5 | 4 | 3 | 6 | 9 | 4 | 5 | 8 | 54 |
| 5 | 11 | 10 | 8 | 18 | 12 | 10 | 10 | 12 | 15 | 8 | 114 |
| 6 | 14 | 14 | 18 | 21 | 16 | 22 | 19 | 15 | 17 | 15 | 171 |
| 7 | 26 | 17 | 23 | 23 | 24 | 24 | 17 | 22 | 20 | 21 | 217 |
| 8 | 19 | 19 | 21 | 7 | 14 | 15 | 20 | 17 | 15 | 17 | 164 |
| 9 | 11 | 13 | 9 | 13 | 14 | 14 | 12 | 13 | 11 | 16 | 126 |
| 10 | 8 | 6 | 8 | 5 | 9 | 5 | 5 | 9 | 7 | 9 | 71 |
| 11 | 6 | 6 | 4 | 6 | 3 | 1 | 3 | 1 | 4 | 5 | 39 |
| 12 | 1 | 1 | 2 | 1 | 1 | 1 | 2 | 2 | 1 | | 12 |
| 13 | 1 | 1 | | | 1 | | 1 | 1 | 1 | | 6 |
| 14 | | | | | | | | | | | |
| 15 | | | | | | | | | | | |
| 16 | | | | | | | | | | | |
| | 752 | 719 | 732 | 700 | 731 | 698 | 713 | 722 | 706 | 737 | 7210, |

$$\int \frac{dx}{\log x} = 7212 \cdot 99;$$

www.rcin.org.pl

viz. in the interval 1,000,000 to 1,010,000, 100 hundreds, there is 1 hundred containing 1 prime, there are 2 hundreds each containing 4 primes, 11 hundreds each containing 5 primes,.., 1 hundred containing 13 primes, so that, as

$$\begin{array}{rcl} 1 \times & 1 = & 1, \\ 4 \times & 2 = & 8, \\ 5 \times & 11 = & 55, \\ \vdots & & \\ 13 \times & 1 = & 13, \\ \hline 100 & & 752, \end{array}$$

the whole 10,000 contains 752 primes; the next 10,000 contains 719 primes, and so on; the whole 100,000 thus containing $752 + 719 + \&c. \ldots = 7210$ primes, which number is at the foot compared with the theoretic approximate value

$$\int \frac{dx}{\log x} \text{ (limits 1,000,000 to 1,010,000)} = 7212{\cdot}99.$$

The integral in question is represented by the notation $\mathrm{Li}.\, x$ or $\mathrm{li}.\, x$.

p. 443. We have the like tables 1,000,000 to 2,000,000 and 2,000,000 to 3,000,000, showing for each 100,000 how many hundreds there are containing 0 prime, 1 prime, 2 primes, up to (the largest number) 17 primes.

13. It is noticed that

the 26,379th hundred contains no prime,

the 27,050th hundred contains 17 primes.

It may be observed that, if $N = 2 . 3 . 5 \ldots p$, the product of all the primes up to $p$, then each of the numbers $N + 1$ and $N + q$ (if $q$ be the prime next succeeding $p$) is or is not a prime; but the intermediate numbers $N + 2$, $N + 3, \ldots, N + q - 1$ are certainly composite; viz. we thus have at least $q - 2$ consecutive composites. To obtain in this manner 99 consecutive composites, the value of $N$ would be $= 2 . 3 . 5 \ldots 97$, viz. this is a number far exceeding 2,637,900; but, in fact, the hundred numbers 2,637,901 to 2,638,000 are all composite.

**Legendre,** in his *Essai sur la Théorie des Nombres* (1st edit., 1798; 2nd edit., 1808, supplement, 1816: references to this edition), gives for the number of primes inferior to a given limit $x$ the approximate formula

$$\frac{x}{\log x - 1{\cdot}08366};$$

and p. 394, and supplement, p. 62, he compares for each 10,000 up to 100,000, and for each 100,000 up to 1,000,000, the values as computed by this formula with the actual numbers of primes exhibited by the tables of Wega and Chernac. Thus for $x = 1{,}000{,}000$, the computed value is 78,543, the actual value 78,493.



www.rcin.org.pl

He shows, p. 414, that the number of integers, which are less than $n$ and are not divisible by any of the numbers $\theta$, $\lambda$, $\mu$, ..., is approximately

$$= n\left(1-\frac{1}{\theta}\right)\left(1-\frac{1}{\lambda}\right)\left(1-\frac{1}{\mu}\right)\dots;$$

and taking $\theta$, $\lambda$, $\mu$, ... the successive primes 3, 5, 7, ... he gives the values of the function in question, or, say, the function

$$\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7}\cdot\frac{10}{11}\cdots\frac{\omega-1}{\omega},$$

$\omega$ a prime, for the several prime values $\omega = 3$ to 1229 in the Table IX. (one page) at the end of the work.

14. A table of frequency is given by

**Glaisher,** J. W. L., *British Association Report* for 1872, p. 20. This gives for the second and the ninth millions, respectively divided into intervals of 50,000, the actual number of primes in each interval, as compared with the theoretic value $\mathrm{li}\,x' - \mathrm{li}\,x$; and also deduced therefrom, by the formula $\log \frac{1}{2}(x'+x)$, a table of the average interval between two consecutive primes; this average interval increases very slowly: at the beginning and the end of the second million the values are 13·76 and 14·58 (theoretic values 13·84 and 14·50); at the beginning and the end of the ninth million 16·02 and 15·95 (theoretic values 15·90 and 16·01).

15. Coming under the head of Divisor Tables, some tables by Reuschle and Gauss may be here referred to. These are:—

**Reuschle,** *Mathematische Abhandlung, zahlentheoretische Tabellen sammt einer dieselben treffenden Correspondenz mit der verewigten C. G. J. Jacobi*, 4°, pp. 1—61* (1856). The tables belonging to the present subject are

A. Tafeln zur Zerlegung von $a^n - 1$ (pp. 18—22).

I. Table of the prime factors of $10^n - 1$, viz.

(a. pp. 18—19.) Complete decomposition of $10^n - 1$, $n=1$ to 42: and $10^n+1$, $n=1$ to 21. Some values of $n$ are omitted.

A specimen is

$$10^{13} - 1 = 3^2 \,.\, 53 \,.\, 79 \,.\, 265371653,$$

$$10^{13} + 1 = 11 \,.\, 189 \,.\, 1058313049.$$

(b. p. 19.) List of the specific prime factors $f$ of $10^n - 1$, or the prime factors of the residue after separation of the analytical factors, for those values of $n$ for which the complete decomposition is unknown, and omitting those values for which no factor is known, $n = 25$ to 243.

* Titlepage missing in my copy; but I find from Prof. Kummer's notice of the work, *Crelle*, t. LIII. (1857), p. 379, that it appeared as a Programm of the Stuttgart Gymnasium, Michaelmas, 1856, and was separately printed by Liesching and Co., Stuttgart.

www.rcin.org.pl

A specimen is

| $n$ | $f$ |
|---|---|
| 25 | 21401. |

The meaning seems to be, residue of $10^{25}-1$ is $1+10^5+10^{10}+10^{15}+10^{20}$, and this contains the prime factor 21401; but it is not clear why this is the "specific prime factor."

II. Prime factors of $a^n-1$ for different values of $a$ and $n$.

(a. p. 20) gives for 41 values of $a$ (2, 3, &c. at intervals to 100) and for the following values of $n$ the decompositions of the residues or specific factors of $a^n-1$; viz. these are

$$\begin{aligned} n = {}& 1, \quad a-1: \\ ,, {}& 2, \quad a+1: \\ ,, {}& 3, \quad a^2+a+1: \\ ,, {}& 6, \quad a^2-a+1: \\ ,, {}& 4, \quad a^2+1: \\ ,, {}& 5, \quad a^4+a^3+a^2+a+1: \\ ,, {}& 10, \quad a^4-a^3+a^2-a+1: \\ ,, {}& 8, \quad a^4+1: \\ ,, {}& 12, \quad a^4-a^2+1. \end{aligned}$$

A specimen is

| $a$ | $a-1$ | $a^2-1$ | $a^3-1$ | $a^6-1$ | $a^4-1$ | $a^5-1$ | $a^{10}-1$ | $a^8-1$ | $a^{12}-1$ |
|---|---|---|---|---|---|---|---|---|---|
| 10 | $3^2$ | 11 | $3^3 . 37$ | 7 . 13 | 101 | 41 . 271 | 9091 | 73 . 137 | 9901 |

(b. p. 21.) Specific prime factors for the numbers 2, 3, 5, 6, 7, 10, (the powers 4, 8, 9 being omitted as coming under 2 and 3), for the exponents 1 to 42.

A specimen is

| $n$ | $2^n-1$ | $3^n-1$ | $5^n-1$ | $6^n-1$ | $7^n-1$ | $10^n-1$ |
|---|---|---|---|---|---|---|
| 19 | 524287 | 1597 . 363889 | 191 . $x$ | 191 . $x$ | 419 . $x$ | |

where the $x$ denotes that the other factor is not known to be prime. And so, where no number is given, as in $10^{19}-1$, it is not known whether the number $(=1+10^1+10^2+\ldots+10^{18})$ is or is not prime.

Addition, p. 22. For $a=2$, the complete decomposition of the prime factor of $2^n-1$ is given for values of $n$, $=44, 45, \ldots$ at intervals to 156.

A specimen is

| $n$ | $f$ |
|---|---|
| 44 | 397 . 2113, |

viz.

$$2^{20}-2^{18}+2^{16}-\ldots-2^2+1, =838861=397 . 2113.$$

$n=31$, Fermat's prime. $n=37$, the first case for which the decomposition is not given completely. $n=41$, the first case for which no factor is known.

www.rcin.org.pl

16. **Gauss,** Tafel zur Cyclotechnie, *Werke*, t. II. pp. 478—495, shows, for 2452 numbers of the several forms $a^2+1$, $a^2+4$, $a^2+9, \ldots, a^2+81$, the values of $a$ such that the number in question is a product of prime factors no one of which exceeds 200, and exhibits all the odd prime factors of each such number. The table is in nine parts, zerlegbare $a^2+1$, zerlegbare $a^2+4$, &c., with to each part a subsidiary table, as presently mentioned. Thus a specimen is

zerlegbare $a^2+9$.

| | |
|---|---|
| 1 | 5 |
| 2 | 13 |
| 4 | 5 . 5 |
| 5 | 17 |
| 7 | 29 |
| 8 | 73 |
| ⋮ | ⋮ |
| 1411168679 | 5 . 5 . 13 . 17 . 17 . 89 . 113 . 157 . 173 . 197 . 197 : |

viz.

$1^2+9$, odd prime factor is 5,

$2^2+9$, „ „ 13,

$4^2+9$, „ factors are 5, 5,

and so on.

And the subsidiary table is

| | |
|---|---|
| 5 | 1, 4, 79 |
| 13 | 2, 11, 41 |
| 17 | 5, 29, 46, 379, 1042 |
| ⋮ | ⋮ |

showing that the numbers $a$ for which the largest factor is 5 are 1, 4, 79; those for which it is 13 are 2, 11, 41; and so on.

The object of the table is explained in the *Bemerkungen*, (*l. c.*, p. 523), by Schering, the editor of the volume, viz. it is to facilitate the calculation of the circular arcs the cotangents of which are rational numbers. To take a simple example, it appears to be by means of it that Gauss obtained, among other formulæ, the following:

$$\frac{\pi}{4} = 12 \text{ arctan } \tfrac{1}{18} + 8 \text{ arctan } \tfrac{1}{57} - 5 \text{ arctan } \tfrac{1}{239},$$

and

$$= 12 \text{ arctan } \tfrac{1}{38} + 20 \text{ arctan } \tfrac{1}{57} + 7 \text{ arctan } \tfrac{1}{239} + 24 \text{ arctan } \tfrac{1}{268}.$$

www.rcin.org.pl

[F. 12. *Divisors, &c.*] *continued. Prime Roots. The Canon Arithmeticus, Quadratic residues.* Art. II.

17. *Prime Roots.*—Let $p$ be a prime number; then there exist $\varpi(p-1)$ inferior integers $g$, such that all the numbers $1, 2, \ldots, p-1$ are, to the modulus $p$,

$$\equiv 1,\ g,\ g^2, \ldots,\ g^{p-2}\ (g^{p-1} \text{ is of course } \equiv 1).$$

This being so, $g$ is said to be a prime root of $p$; and moreover the several numbers $g^\alpha$, where $\alpha$ is any number whatever less than and prime to $p-1$, constitute the series of the $\varpi(p-1)$ prime roots of $p$. It may be added that, if $\beta$ be an integer number less than $p-1$, and having with it a greatest common measure $=k$, so that

$$(g^\beta)^{\frac{p-1}{k}} \equiv g^{\frac{\beta}{k}(p-1)}, \equiv 1, \left(\text{since } \frac{\beta}{k} \text{ is an integer, and } g^{p-1} \equiv 1\right),$$

then $g^\beta$ has the indicatrix $\dfrac{p-1}{k}$: the prime roots are those numbers which have the indicatrix $p-1$.

The like theory exists as to any number $N$ of the form $p^m$ or $2p^m$. There are here $\varpi(N)$, $=N\left(1-\frac{1}{p}\right)$ or $\frac{1}{2}N\left(1-\frac{1}{p}\right)$, in the two cases respectively, numbers less than $N$ and prime to it; and we have then $\varpi(\varpi(N))$ numbers $g$ such that, to the modulus $N$, all these numbers are $\equiv 1, g, g^2 \ldots g^{\varpi(N)-1}$ ($g^{\varpi(N)}$ is of course $\equiv 1$). This being so, $g$ may be regarded as a prime root of $N$ ($=p^m$ or $2p^m$, as the case may be); and moreover the several numbers $g^\alpha$, where $\alpha$ is any number whatever less than and prime to $\varpi(N)$, constitute the series of the $\varpi(\varpi(N))$ prime roots of $N$. Thus $N=3^2=9$, $\varpi(N)=6$; we have

$$\begin{array}{llllll} 1, & 2^1, & 2^2, & 2^3, & 2^4, & 2^5, \\ \equiv 1, & 2, & 4, & 8, & 7, & 5, \text{ mod. } 9; \end{array}$$

or the prime roots of 9 are $2^1$ and $2^5$, $=2$ and 5.

So also $N=2.3^2=18$, $\varpi(N)=6$; we have

$$\begin{array}{llllll} 1, & 5^1, & 5^2, & 5^3, & 5^4, & 5^5, \\ \equiv 1, & 5, & 7, & 17, & 13, & 11, \text{ mod. } 18; \end{array}$$

and $5^1$ and $5^5$, $=5$ and 11 are the prime roots of 18.

18. A small table of prime roots, $p=3$ to 37, is given by

**Euler,** *Op. Arith. Coll.* t. I. pp. 525—526. The Memoir is entitled "Demonstrationes circa residua e divisione potestatum per numeros primos resultantia," pp. 516—537 (1772).

www.rcin.org.pl

19. A table, $p$ and $p^m$, 3 to 97, is given by

**Gauss,** "Disquisitiones Arithmeticæ," 1801, (*Werke,* t. I. p. 468). This gives in each case a prime root, and it shows the exponents in regard thereto of the several prime numbers less than $p$ or $p^m$. Thus a specimen is

| | | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 &c. |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 27 | 2 | 1 | * | 5 | 16 | 13 | 8 | 15 | 12 | 11 | |
| 29 | 10 | 11 | 27 | 18 | 20 | 23 | 2 | 7 | 15 | 24 | |

viz. for 27 we have 2 a prime root, and $2 \equiv 2^1$, $5 \equiv 2^5$, $7 \equiv 2^{16}$, $11 \equiv 2^{13}$, &c.; and so also for 29 we have 10 a prime root, and $2 \equiv 10^{11}$, $3 \equiv 10^{27}$, $5 \equiv 10^{18}$, &c.

20. Small tables are probably to be found in many other places; but the most extensive and convenient table is **Jacobi's** *Canon Arithmeticus,* the complete title of which is

*Canon Arithmeticus sive tabula quibus exhibentur pro singulis numeris primis vel primorum potestatibus infra* 1000 *numeri ad datos indices et indices ad datos numeros pertinentes.* Edidit C. G. J. Jacobi. Berolini, 1839. 4°.

The contents are as follows:—

| | Pages |
|---|---|
| Introductio . . . . . . . . . . . . | i to xl |
| Tabulæ numerorum ad indices datos pertinentium et indicum numero dato correspondentium pro modulis primis minoribus quam 1000 . . . . . . . . . . . . | 1—221 |
| Tabulæ residuorum et indicum sibi mutuo respondentium pro modulis minoribus quam 1000 qui sunt numerorum primorum potestates . . . . . . . . . . . . | 222—238 |
| Hujus tabula ea pars quæ pertinet ad modulos formæ $2^n$, invenitur | 239—240. |

The following is a specimen of the principal tables:—

$$p = 19,\ p - 1 = 2 \,.\, 3^2.$$

Numeri.

| *I* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 10 | 5 | 12 | 6 | 3 | 11 | 15 | 17 | 18 |
| | 9 | 14 | 7 | 13 | 16 | 8 | 4 | 2 | 1 | |

Indices.

| *N* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 18 | 17 | 5 | 16 | 2 | 4 | 12 | 15 | 10 |
| 1 | 1 | 6 | 3 | 13 | 11 | 7 | 14 | 8 | 9 | |

www.rcin.org.pl

where the first table gives the values of the powers of the prime root 10 (that 10 is the root appears by its index being given as $=1$) to the modulus 19, viz. $10^1 \equiv 10$, $10^2 \equiv 5$, $10^3 \equiv 12$, &c.; and the second table gives the index of the power to which the same prime root must be raised in order that it may be, to the modulus 19, congruent with a given number: thus $10^{18} \equiv 1$, $10^{17} \equiv 2$, $10^5 \equiv 3$, &c. The units of the index or number, as the case may be, are contained in the top line of the table, and the tens or hundreds and tens in the left-hand column.

21. There is given by

**Jacobi**, *Crelle*, t. XXX. (1846), pp. 181, 182, a table of $m'$ for the argument $m$, such that

$$1 + g^m \equiv g^{m'} \text{ (mod. } p), \quad p = 7 \text{ to } 103, \text{ and } m = 0 \text{ to } 102.$$

A specimen is

| $p$ | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 ... to 103 |
|---|---|---|---|---|---|---|---|---|---|
| $g$ | 3 | 2 | 6 | 10 | 10 | 10 | 10 | 17 | 5 |
| $m$ | | | | | | | | | |
| 11 | . | . | 6 | 4 | 7 | * | 27 | 21 | 34 |

for instance, $p = 19$, $1 + 10^{11} \equiv 10^7$ (mod. 19).

Jacobi remarks that this table was calculated for him by his class during the winter course of 1836—37; and that, by means of the *Canon Arithmeticus* since published (in 1839), the same might easily be extended to all primes under 1000. In fact, for any such number $p$, putting any number of the table "Indices" $= m$, the next following number of the table gives the value of $m'$.

22. We have next, in **Reuschle's** Memoir (*ante*, No. 15), the following relating to prime roots:—

C. Tafeln für primitive Wurzeln und Hauptexponenten, oder V. erweiterte und bereicherte Burkhardtsche Tafel, pp. 41—61, being divided into three parts; viz. these are

a. Table of the Hauptexponenten of the six roots 10, 5, 2, 6, 3, 7 for all prime numbers of the first 1000, together with the least primitive root of each of these numbers (pp. 42—46).

A specimen is as follows:—

| | | 10 | | 5 | | 2 | | 6 | | 3 | | 7 | | $w$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $p$ | $p-1$ | $e$ | $n$ | $e$ | $n$ | $e$ | $n$ | $e$ | $n$ | $e$ | $n$ | $e$ | $n$ | |
| 53 | $2^2.13$ | 13 | 4 | 52 | 1 | 52 | 1 | 26 | 2 | 52 | 1 | 26 | 2 | 2 |

where $e$ is the Hauptexponent or indicatrix of the root (10, 5, 2, 6, 3, 7, as the case may be), $n = \frac{p-1}{e}$, $w$ the least primitive root; thus

$$p = 53, \quad 10^{13} \equiv 1, \quad 5^{52} \equiv 1, \quad 2^{52} \equiv 1,$$



www.rcin.org.pl

(2 being accordingly the least prime root),

$$6^{26} \equiv 1, \quad 3^{52} \equiv 1, \quad 7^{26} \equiv 1.$$

The number $w$ of the last column is the least primitive root. It is, of course, not always (as in the present case) one of the numbers 10, 5, 2, 6, 3, 7 to which the table relates: the first exception is $p = 191$, $w = 19$: the highest value of $w$ is $w = 21$, corresponding to $p = 409$.

b. The like table for the roots 10 and 2 for all prime numbers from 1000 to 5000, together with as convenient as possible a prime root (and in some cases two prime roots) for each such number (pp. 47—53).

A specimen is:—

| | | 10 | | 2 | | |
|---|---|---|---|---|---|---|
| $p$ | $p-1$ | $e$ | $n$ | $e$ | $n$ | $w$ |
| 1289 | $2^3 . 7 . 23$ | 92 | 14 | 161 | 8 | 6, 11 |

viz. here, mod. 1289, $10^{92} \equiv 1$, $2^{161} \equiv 1$; and two prime roots are 6, 11. We have thus by the present tables a prime root for every prime number not exceeding 5000.

c. The like table for the root 10 for all prime numbers between 5000 and 15000, (no column for $w$, nor any prime root given), pp. 53—61.

A specimen is

| $p$ | $p-1$ | $e$ | $n$ |
|---|---|---|---|
| 9859 | $2.3.31.53$ | 3286 | 3: |

viz., mod. 9859, we have $10^{3286} \equiv 1$. But in a large number of cases we have $n = 1$, and therefore 10 a prime root. For example,

| | | | |
|---|---|---|---|
| 9887 | $2.4983$ | 9386 | 1. |

23. For a composite number $n$, if $N = \varpi(n)$ be the number of integers less than $n$ and prime to it, then if $x$ be any number less than $n$ and prime to it, we have $x^N \equiv 1$ (mod. $n$). But we have in this case no analogue of a prime root—there is no number $x$, such that its several powers $x^1, x^2, \ldots, x^{N-1}$ (mod. $n$) are all different from unity; or, what is the same thing, there is for each value of $x$ some submultiple of $N$, say $N'$, such that $x^{N'} \equiv 1$ (mod. $n$). And these several numbers $N'$ have a least common multiple $I$, which is not $= N$, but is a submultiple of $N$; and this being so, then for all the several values of $x$, $I$ is said to be the maximum indicator. For instance, $n = 12$, $N = \varpi(n)$; the numbers less than 12 and prime to it are 1, 5, 7, 11. We have, (mod. 12), $1^1 \equiv 1$, $5^2 \equiv 1$, $7^2 \equiv 1$, $11^2 = 1$, or the values of $N'$ are 1, 2, 2, 2; their least common multiple is 2, and we have accordingly $I = 2$: viz. $x^2 \equiv 1$ (mod. 12) has the $\varpi(12)$ roots 1, 5, 7, 11. So $n = 24$, $\varpi(n) = 8$; the maximum indicator $I$ is in this case also $= 2$.

www.rcin.org.pl

A table of the maximum indicator $n=1$ to 1000 is given by

**Cauchy,** *Exer. d'Analyse &c.*, t. II. (1841), pp. 36—40, contained in the "Mémoire sur la résolution des équations indéterminées du premier degré en nombres entiers," pp. 1—40.

24. It thus appears that for a composite number $n$, the $\varpi(n)$ numbers less than $n$ and prime to it cannot be expressed as $\equiv$ (mod. $n$) to the power of a single root; but for the expression of them it is necessary to employ two or more roots. A small table, $n=1$ to 50, is given by

**Cayley,** Specimen Table $M \equiv a^\alpha b^\beta$ (mod. $N$) for any prime or composite modulus; *Quart. Math. Journ.* vol. IX. (1868), pp. 95, 96, and folding sheet, [397].

A specimen is

| Nos. | 12 |
|---|---|
| roots | 5, 7 |
| Ind. | 2, 2 |
| M.I. | 2 |
| $\phi$ | 4 |
| 1 | 0, 0 |
| 2 | |
| 3 | |
| 4 | |
| 5 | 1, 0 |
| 6 | |
| 7 | 0, 1 |
| 8 | |
| 9 | |
| 10 | |
| 11 | 1, 1 |

viz. for the modulus 12 the roots are 5, 7, having respectively the indicators 2, 2, viz. $5^2 \equiv 1$ (mod. 12), $7^2 \equiv 1$ (mod. 12). Hence also the maximum indicator is $=2$. $\phi\,(=\varpi(n))=4$ is the number of integers less than 12 and prime to it, viz. these are 1, 5, 7, 11, which in terms of the roots 5, 7 and to mod. 12 are respectively $\equiv 5^0.7^0$, $5^1.7^0$, $5^0.7^1$, and $5^1.7^1$.

25. *Quadratic Residues.*—In regard to a given prime number $p$, a number $N$ is or is not a quadratic residue according as the index of $N$ is even or odd, viz. $g$ being a prime root and $N \equiv g^\alpha$, then $N$ is or is not a quadratic residue according as $\alpha$ is even or odd. But the quadratic residues can, of course, be obtained directly without the consideration of prime roots.

A small table, $p=3$ to 97 and $N=-1$ and (prime values) 3 to 97, is given by

**Gauss,** "Disquisitiones Arithmeticæ," 1801; Table II. (*Werke,* t. I. p. 469): I notice here a misprint in the top line of the original; it should be $-1, +2, +3$, &c., instead of

1, + 2, + 3, &c.; the $-1$ is printed correctly on p. 499 of the French translation *Recherches Arithmétiques*, Paris, 1807 and on p. 469 of vol. I. of *Werke*, (Göttingen, 1870).

A specimen is

| | $-1$ | $+2$ | $+3$ | $+5$ | $+7$ | $+11$ | $+13$ | $+17$ | $+19$ | $+23$ | &c. |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 19 | | | | $-$ | $-$ | $-$ | | $-$ | $-$ | $-$ | |

viz. $-1$, 2, 3, 13 are not, 5, 7, 11, 17 &c. are, quadratic residues of 19. The residues taken positively and less than 19 are, in fact, 1, 4, 5, 6, 7, 11, 16, 17.

The same table carried from $p = 3$ to 503, and prime values $N = 3$ to 997, is given by **Gauss,** *Werke*, t. II. pp. 400—409. A specimen is

| | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | &c.; |
|---|---|---|---|---|---|---|---|---|---|---|
| 19 | | | $-$ | $-$ | $-$ | | $-$ | $-$ | $-$ | |

viz. the arrangement is the same, except only that the $-1$ column is omitted.

26. We have also by **Gauss**

"Disquisitiones Arithmeticæ" Table III. (*Werke*, t. I. p. 470), for the conversion into decimals of a vulgar fraction, denominator $p$ or $p^\mu$, not exceeding 100. The explanation is given in Art. 314 *et seq.* of the same work.

But this table, carried to a greater extent, is given by **Gauss,** *Werke*, t. II. pp. 412—434, "Tafel zur Verwandlung gemeiner Brüche mit Nennern aus dem ersten Tausend in Decimalbrüche;" viz. the denominators are here primes or powers of primes, $p^\mu$ up to 997.

To explain the table, consider a modulus $p^\mu$ (where $\mu$ may be $=1$); if 10 is not a prime root of $p^\mu$, consider a prime root $r$, which is such that $r^e \equiv 10 \pmod{p^\mu}$, $e$ being a submultiple of $p^{\mu-1}(p-1)$; say we have $ef = p^{\mu-1}(p-1)$: then $10^f \equiv 1$ (mod. $p^\mu$). Consider any fraction $\frac{N}{p^\mu}$; then we may write $N \equiv r^{kl+l}$ (mod. $p^\mu$), $k$ from 0 to $f-1$ and $l$ from 0 to $e-1$, $\equiv 10^k r^l$, and consequently $\frac{N}{p^\mu}$ and $\frac{10^k r^l}{p^\mu}$ have the same mantissa (decimal part regarded as an integer); hence, in order to know the mantissa of every fraction whatever of $\frac{N}{p^\mu}$, it is sufficient to know the mantissa of $\frac{rl}{p^\mu}$, that is, the mantissæ of $\frac{1}{p^\mu}, \frac{r}{p^\mu}, \frac{r^2}{p^\mu}, \ldots, \frac{r^{e-1}}{p^\mu}$, or, what is the same thing, the mantissæ of $\frac{10}{p^\mu}, \frac{10r}{p^\mu}, \ldots, \frac{10r^{e-1}}{p^\mu}$.

For instance, $p^\mu = 11$, $10^2 \equiv 1$ (mod. 11), whence $f=2$, $e=5$; and taking $r=2$, we have $10 \equiv r^5$ (mod. 11).

www.rcin.org.pl

The required mantissæ, denoted in the table by

$$\begin{array}{ccccc} (0), & (1), & (2), & (3), & (4), \end{array}$$

are those of

$$\frac{10}{11},\ \frac{10\,.\,2}{11},\ \frac{10\,.\,2^2}{11},\ \frac{10\,.\,2^3}{11},\ \frac{10\,.\,2^4}{11},$$

viz. these fractions are respectively =

$$\begin{array}{ccccc} (0), & (1), & (2), & (3), & (4), \\ \cdot 9090\ldots, & 1\cdot 8181\ldots, & 3\cdot 6363\ldots, & 7\cdot 2727\ldots, & 14\cdot 5454\ldots; \end{array}$$

or their mantissæ are 90, 81, 63, 27, 54.

And we accordingly have as a specimen

$$11 \left|\ (1)\ldots 81,\ \ (2)\ldots 63,\ \ (3)\ldots 27,\ \ (4)\ldots 54,\ \ (0)\ldots 90.\right.$$

Or again, as another specimen, $r = 2$:—

$$27 \left|\ (1)\ldots 740,\ \ (2)\ldots 481,\ \ (3)\ldots 962,\ \ (4)\ldots 925,\ \ (5)\ldots 851,\ \ (0)\ldots 370.\right.$$

The table in this form extends to $p^\mu = 463$; the values of $r$ (not given in the body of the table) are annexed, p. 420.

In the latter part of the table $p^\mu = 467$ to 997, we have only the mantissæ of $\frac{100}{p^\mu}$. A specimen is

| | | | | |
|---|---|---|---|---|
| | 1828153564 | 8994515539 | 3053016453 | 3820840950 |
| 547 | 6398537477 | 1480804387 | 5685557586 | 8372943327 |
| | 2394881170 | 0182815356, | | |

viz. the fraction $\frac{100}{547} = \cdot 182815\ldots$ has a period of 91, $= \frac{1}{6}\,546$, figures.

[F. 13. *The Pellian Equation.*] Art. III.

27. The Pellian equation is $y^2 = ax^2 + 1$, $a$ being a given integer number, which is not a square (or rather, if it be, the only solution is $y = 1$, $x = 0$), and $x$, $y$ being numbers to be determined: what is required is the least values of $x$, $y$, since these, being known, all other values can be found. A small table $a = 2$ to 68 is given by

**Euler,** *Op. Arith. Coll.* t. I. p. 8. The Memoir is "Solutio problematum Diophanteorum per numeros integros," pp. 4—10, 1732—33. The form of the table is

| $a$ | $x\,(=p)$ | $y\,(=q)$ |
|---|---|---|
| 2 | 2 | 3 |
| 3 | 1 | 2 |
| 5 | 4 | 9 |
| ⋮ | ⋮ | ⋮ |
| 68 | 4 | 33. |

www.rcin.org.pl

Even here, for some of the values of $a$, the values of $x$, $y$ are extremely large; thus $a = 61$, $x = 226{,}153{,}980$, $y = 1{,}766{,}399{,}049$.

And probably tables of a like extent may be found elsewhere; in particular, a table of the solution of $y^2 = ax^2 \pm 1$ ($-$ when the value of $a$ is such that there is a solution of $y^2 = ax^2 - 1$, and $+$ for other values of $a$), $a = 2$ to 135, is given by **Legendre,** *Théorie des Nombres,* 2nd ed. 1808, in the Table X. (one page) at the end of the work. For the before-mentioned number 61, the equation is $y^2 = 61x^2 - 1$, and the values are $x = 3805$, $y = 29718$; much smaller than Euler's values for the equation $y^2 = 61x^2 + 1$.

28. The most extensive table, however, is given by

**Degen,** *Canon Pellianus, sive Tabula simplicissimam equationis celebratissimæ:* $y^2 = ax^2 + 1$, *solutionem, pro singulis numeri dati valoribus ab* 1 *usque ad* 1000 *in numeris rationalibus, iisdemque integris exhibens.* Auctore Carolo Ferdinando Degen. Hafn (Copenhagen) apud Gerhardum Bonnarum, 1817. 8vo. pp. iv to xxiv and 1 to 112.

The first table (pp. 3—106) is entitled as "Tabula I. Solutionem Equationis $y^2 - ax^2 - 1 = 0$ exhibens." It, in fact, also gives the expression of $\sqrt{a}$ as a continued fraction; thus a specimen is

| | | | | | |
|---|---|---|---|---|---|
| 209 | 14 | 2 | 5 | 3 | (2) |
| | 1 | 13 | 5 | 8 | 11 |
| | 3220 | | | | |
| | 46551 | | | | |

Here the first line gives the continued fraction, viz.

$$\sqrt{209} = 14 + \frac{1}{2} \, \frac{1}{+5} \, \frac{1}{+3} \, \frac{1}{+2} \, \frac{1}{+3} \, \frac{1}{+5} \, \frac{1}{+2} \, \frac{1}{+28} \, \frac{1}{+2} + \&c.,$$

the period being (2, 5, 3, 2, 3, 5, 2) indicated by 2, 5, 3 (2). [The number of terms in the period is here odd, but it may be even; for instance, the period (1, 1, 5, 5, 1, 1) is indicated by 1, 1 (5, 5).]

The second line contains auxiliary numbers presenting themselves in the process; thus, if $R^2 = 239$, we have $R = 14 + \frac{1}{\alpha}$,

$$\alpha = \frac{1}{R-14} = \frac{1\,(R+14)}{209-14^2} = \frac{R+14}{13} = 2 + \frac{1}{\beta},$$

$$\beta = \frac{13}{R-12} = \frac{13\,(R+12)}{209-12^2} = \frac{R+12}{5} = 5 + \frac{1}{\gamma},$$

$$\gamma = \frac{5}{R-13} = \frac{5\,(R+13)}{209-13^2} = \frac{R+13}{8} = 3 + \frac{1}{\delta},$$

&c.,

www.rcin.org.pl

where the second line 1, 13, 5,... shows the numerical factors of the third column. The value of this second line as a result is not very obvious.

The third line gives $x$, and the fourth line $y$.

29. The second table, pp. 109—112, is entitled "Tabula II. Solutionem æquationis $y^2 - ax^2 + 1 = 0$, quotiescunque valor ipsius $a$ talem admiserat, exhibens"; viz. it is remarked that this is only possible (but see *infrà*) for those values of $a$ which in Table I. correspond to a period of an even number of terms, as shown by two equal numbers in brackets; thus $a = 13$, the period of $\sqrt{13}$ given in Table I. is (1, 1, 1, 1) as shown by the top line 3, 1 (1, 1), and accordingly 13 is one of the numbers in Table II.; and we have there 13 $\begin{array}{|c}5\\18.\end{array}$

Or take another specimen, 241 $\begin{array}{|c}4574225\\71011068;\end{array}$ viz. the first line gives the value of $x$, and the second line the value of $y$ (least values), for which $y^2 - ax^2 = -1$.

It is to be noticed that $a = 2$ and $a = 5$, for which we have obviously the solutions ($x = 1$, $y = 1$) and ($x = 1$, $y = 2$) respectively, are exceptional numbers not satisfying the test above referred to; and (apparently for this reason) the values in question, 2 and 5, are omitted from the table.

30. **Cayley,** "Table des plus petites solutions impaires de l'équation $x^2 - Dy^2 = \pm 4$, $D \equiv 5$ (mod. 8)." *Crelle*, t. LIII. (1857), page 371 (one page), [231].

As regards the theory of quadratic forms, it is important to know whether for a given value of $D\,(\equiv 5$, mod. 8) there does or does not exist a solution, in odd numbers, of the equation $x^2 - Dy^2 = 4$. As remarked in the paper, "Note sur l'équation $x^2 - Dy^2 = \pm 4$, $D \equiv 5$ (mod. 8)," pp. 369—371, [231], this can be determined for values of $D$ of the form in question up to $D = 997$ by means of Degen's Table; and the solutions, when they exist, of the equation $x^2 - Dy^2 = 4$, as also of the equation $x^2 - Dy^2 = -4$, can be obtained up to the same value of $D$. Observe that when the equation $x^2 - Dy^2 = -4$ is possible, the equation $x^2 - Dy^2 = 4$ is also possible, and that its least solution is obtained very readily from that of the other equation; it is therefore sufficient to tabulate the solution of $x^2 - Dy^2 = \pm 4$, the sign being $-$ when the corresponding equation is possible, and being in other cases $+$. Hence the form of the Table: viz. as a specimen we have

| $D$ | $\pm$ | $x$ | $y$ |
|---|---|---|---|
| 757 | imposs. | | |
| 765 | + | 83 | 3 |
| 773 | − | 139 | 5 |
| 781 | imposs. | | |
| ⋮ | | | |

www.rcin.org.pl

that is, if $D=757$ or 781, there is no solution of either $x^2-Dy^2=+4$ or $=-4$; if $D=765$, there is a solution $x=83$, $y=3$ of $x^2-Dy^2=+4$, but none of $x^2-Dy^2=-4$; if $D=773$, there is a solution $x=139$, $y=5$ of $x^2-Dy^2=-4$, and therefore also a solution of $x^2-Dy^2=+4$; and so in other cases.

[F. 14. *Partitions.*] Art. IV.

31. The problem of Partitions is closely connected with that of Derivations. Thus if it be asked in how many ways can the number $n$ be expressed as a sum of three parts, the parts being 0, 1, 2, 3, and each part being repeatable an indefinite number of times, it is clear that $n$ is at most $=9$, and that for the values of $m$, $=0, 1, .., 9$ shown by the top line of the annexed table, the number of partitions has the values shown by the bottom line thereof:—

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| $a^3$ | $a^2b$ | $a^2c$ | $a^2d$ | $abd$ | $acd$ | $ad^2$ | $bd^2$ | $cd^2$ | $d^3$ |
| | | $ab^2$ | $abc$ | $ac^2$ | $b^2d$ | $bcd$ | $c^2d$ | | |
| | | | $b^3$ | $b^2c$ | $bc^2$ | $c^3$ | | | |
| 1 | 1 | 2 | 3 | 3 | 3 | 3 | 2 | 1 | 1 |

But taking $a$, $b$, $c$, $d$ to stand for 0, 1, 2, 3 respectively, the actual partitions of the required form are exhibited by the literal terms of the table (these being obtained, each column from the preceding one, by the method of derivations, or say by the rule of the last and last but one), and the numbers of the bottom line are simply the number of terms in the several columns respectively.

32. A set of such literal tables, say of tables $\begin{pmatrix} a, & b, & c, .., & k \\ =0, & 1, & 2, .., & m \end{pmatrix}^n$, for different values of $n$ and $m$ (where the number of letters is $=m+1$), would be extremely interesting and valuable. The tables for a given value of $m$ and for different values of $n$ are, it is clear, the proper foundation of the theory of the binary quantic $(a, b, c, .., k\between x, 1)^m$, which corresponds to such value of $m$. Prof. Cayley regrets that he has not in his covariant tables given in every case the complete series of literal terms; viz. the literal terms which have zero coefficients are, for the most part, though not always, omitted in the expressions of the several covariants.

33. But the question at present is as to the *number* of terms in a column, that is, as to the number of the partitions of a given form: the analytical theory has been investigated by Euler and others. The expression for the number of partitions is usually obtained as equal to the coefficient of $x^n$ in the development, in ascending powers of $x$, of a given rational function of $x$: for instance, if there is no limitation as to the number of the parts, but if the parts are 1, 2, 3, $m$ (viz. a part may have any value not exceeding $m$), each part being repeatable an indefinite number of times, then

www.rcin.org.pl

Number of partitions of $n =$ coefficient of $x^n$ in $\dfrac{1}{(1-x)(1-x^2)(1-x^3)\dots(1-x^m)}$,

and we can, by actual development, obtain for any given values of $m$, $n$ the number of partitions.

These have been tabulated $m = 1, 2, \dots, 20$, and $m = \infty$ (viz. there is in this case no limit as to the largest part), and $n = 1$ to 59, by

**Euler,** *Op. Arith. Coll.* t. I. pp. 97—101, given in the paper "De Partitione Numerorum," pp. 73—101, (1750); the heading is "Tabula indicans quot variis modis numerus $n$ e numeris 1, 2, 3, 4,.., $m$, per additionem exhibi potest, seu exhibens valores formulæ $n^{(m)}$." The successive lines are, in fact, the coefficients of the several powers $x^0, x^1, \dots, x^9$ in the expansions of the functions

$$\frac{1}{1-x}, \quad \frac{1}{1-x\,.\,1-x^2}, \dots, \frac{1}{1-x\,.\,1-x^2\dots 1-x^{20}}.$$

34. The generating function for any given value of $m$ is, it is clear, $= \dfrac{1}{1-x^m}$ multiplied by that for the next preceding value of $m$, and it thus appears how each line of the table is calculated from that which precedes it. The auxiliary numbers are *printed*; thus a specimen is

Valores numeri $n$.

| $m$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 1 | 2 | 3 | 5 | 6 | 9 | |
| 4 | 1 | 1 | 2 | 3 | 5 | 6 | 9 | 11 | 15 | 18 | 23 | |
| | | | | | | 1 | 1 | 2 | 3 | 5 | 7 | |
| 5 | 1 | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{5}$ | 7 | 10 | 13 | 18 | 23 | 30 | |

viz. suppose the numbers in the second 4-line known: then simply moving these each five steps onward we have the (auxiliary) numbers of the first 5-line; and thence by a mere addition the required series of numbers shown by the second 5-line. And similarly from this is obtained the second 6-line, and so on.

35. More extensive tables are contained in the memoir by

**Marsano,** *Sulle leggi delle derivate generali delle funzioni di funzioni et sulla teoria delle forme di partizione dei numeri intieri,* (4°. Genova, 1870), pp. 1—281; and three tables paged separately, described merely as "Tavole dei numeri $C_{q,r}$, $S_{q,e}$, $S'_{q,e}$ citate nel testo colle indicazioni di Tavole I., II., III., ai n[i] 77, 79, 81"; viz. the reader is referred to these articles for the explanations of what the tabulated functions are; and there is not even then any explicit statement, but the investigation itself has to be studied to make out what the tables are. It is, in fact, easier to make this out from the tables themselves; the explanation is as follows:—



www.rcin.org.pl

Table I. (16 pages) is, in fact, Euler's table, showing in how many ways the number $n$ can be made up with the parts 1, 2, 3,.., $m$; but the extent is greater, viz. $n$ is from 1 to 103, and $m$ from 1 to 102. The auxiliary numbers given in Euler's table are omitted, as also certain numbers which occur in each successive line; thus a specimen is

| $n=$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | &c. |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_{0,n}$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| $C_{1,n}$ | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | |
| $C_{2,n}$ | | | 2 | 2 | 3 | 3 | 4 | 4 | 5 | 5 | |
| $C_{3,n}$ | | | | 3 | 4 | 5 | 7 | 8 | 10 | 12 | |
| $C_{4,n}$ | | | | | 5 | 6 | 9 | 11 | 15 | 18 | |
| &c. | | | | | | | | | | | |

where the line $C_{4,n}$ (ways of making up $n-1$ with the parts 1, 2, 3, 4) is 1, 1, 2, 3, 5, 6, 9, 11, 15, 18, &c., viz. we read from the corner diagonally downwards as far as the 5, and then horizontally along the line: this saves a large number of figures. The table is printed in ordinary quarto pages, which are taken to come in in tiers of seven, five, and three pages one under the other, as shown by a prefixed diagram; and the necessity of a large folding plate is thus avoided.

The successive lines give, in fact, the coefficients in the expansions of

$$\frac{1}{1-x},\ \frac{1}{1-x\,.\,1-x^2},\ \frac{1}{1-x\,.\,1-x^2\,.\,1-x^3},\ldots,\ \frac{1}{1-x\,.\,1-x^2\ldots1-x^{102}},$$

each expanded as far as $x^{103}$.

Table II. (6 pages). The successive lines give the coefficients in the expansions of

$$S,\ \frac{S}{1-x},\ \frac{S}{1-x\,.\,1-x^2},\ldots,\ \frac{S}{1-x\,.\,1-x^2\ldots1-x^{35}},$$

where

$$S=\frac{1}{(1-x)(1-x^2)(1-x^3)}\ldots\text{ ad inf.},$$

each expanded as far as $x^{53}$, and further continued as regards the first ten lines, that is, the expansions of

$$S,\ \frac{S}{1-x},\ \frac{S}{1-x\,.\,1-x^2},\ldots,\ \frac{S}{1-x\,.\,1-x^2\ldots1-x^{9}},$$

each as far as $x^{107}$.

Table III. (2 pages). The successive lines give the coefficients in the expansions of

$$S^2,\ \frac{S^2}{1-x},\ \frac{S^2}{1-x\,.\,1-x^2},\ldots,\ \frac{S^2}{1-x\,.\,1-x^2\ldots1-x^{5}},$$

each expanded as far as $x^{55}$.

www.rcin.org.pl

36. As regards Tables II. and III., the analytical explanations have been given in the first instance; but it is easy to see that the tables give numbers of partitions. Thus, in Table II., the second line gives the coefficients in the development of

$$\frac{1}{(1-x)^2(1-x^2)(1-x^3)\dots};$$

viz. these are 1, 2, 4, 7 12, 19, 30, ..., being the number of ways in which the numbers 0, 1, 2, 3, 4, &c. respectively can be made up with the parts 1, 1′, 2, 3, 4, &c.; thus

| | Partitions. | No. = |
|---|---|---|
| 1 | 1 | 2 |
| | 1′ | |
| 2 | 2 | 4 |
| | 1, 1 | |
| | 1, 1′ | |
| | 1′, 1′ | |
| 3 | 3 | 7 |
| | 2, 1 | |
| | 2, 1′ | |
| | 1, 1, 1 | |
| | 1, 1, 1′ | |
| | 1, 1′, 1′ | |
| | 1′, 1′, 1′ | |
| | &c. | &c. |

Similarly, the third line shows the number of ways in which these numbers respectively can be made up with the parts 1, 1′, 2, 2′, 3, 4, 5, &c.; the fourth line with the parts 1, 1′, 2, 2′, 3, 3′, 4, 5, &c.; and so on.

And in like manner in Table III., the first line shows the number of ways when the parts are 1, 1′, 2, 2′, 3, 3′, ...; the second line when they are 1, 1′, 1″, 2, 2′, 3, 3′, &c.; the third when they are 1, 1′, 1″, 2, 2′, 2″, 3, 3′, &c.; and so on.

It is clear that the series of tables might be continued indefinitely, viz. there might be a Table IV. giving the developments of

$$S^3,\ \frac{S^3}{1-x},\ \frac{S^3}{1-x\,.\,1-x^2};\ \text{and so on.}$$

An interesting table would be one composed of the first lines of the above series, viz. a table giving in its successive lines the developments of $S$, $S^2$, $S^3$, $S^4$, &c.

There are throughout the work a large number of numerical results given in a quasi-tabular form; but the collection of these, with independent explanations of the significations of the tabulated numbers, would be a task of considerable labour.



www.rcin.org.pl

[F. 15. *Quadratic forms* $a^2+b^2$, *&c., and Partitions of Numbers into squares, cubes, and biquadrates.*] Art. V.

37. The forms here referred to present themselves in the various complex theories. Thus $N=a^2+b^2$, $=(a+bi)(a-bi)$; this means that, in the theory of the complex numbers $a+bi$ ($a$ and $b$ integers), $N$ is not a prime but a composite number. It is well known that an ordinary prime number $\equiv 3$, mod. 4, is not expressible as a sum $a^2+b^2$, being, in fact, a prime in the complex theory as well as in the ordinary one: but that an ordinary prime number $\equiv 1$, mod. 4, is (in one way only) $=a^2+b^2$; so that it is in the complex theory a composite number. A number whose prime factors are each of them $\equiv 1$, mod. 4, or which contains, if at all, an even number of times any prime factor $\equiv 3$, mod. 4, can be expressed in a variety of ways in the form $a^2+b^2$; but these are all easily deducible from the expressions in the form in question of its several factors $\equiv 1$, mod. 4, so that the required table is a table of the form $p=a^2+b^2$, $p$ an ordinary prime number $\equiv 1$, mod. 4: $a$ and $b$ are one of them odd, the other even; and to render the decomposition definite $a$ is taken to be odd.

$p=a^2+b^2$; viz. decomposition of the primes of the form $4n+1$ into the sum of two squares: a table extending from $p=5$ to 11981 (calculated by *Zornow*) is given by

**Jacobi,** *Crelle,* t. XXX. (1846), pp. 174—176.

This is carried by Reuschle, as presently mentioned, up to $p=24917$. Reuschle notices that $2713=3^2+52^2$ is omitted, also $6997=39^2+74^2$, and that 8609 should be $=47^2+80^2$.

38. Similarly, primes of the form $6n+1$ are expressible in the form $p=a^2+3b^2$. Observe that, $\omega$ being an imaginary cube root of unity, this is connected with $p'=(a+b\omega)(a+b\omega^2)$, $=a^2-ab+b^2$, viz. we have $4p'=(2a-b)^2+3b^2$; or the form $a^2+3b^2$ is connected with the theory of the complex numbers composed of the cube roots of unity.

$p=a^2+3b^2$; viz. decomposition of the primes of the form $6n+1$ into the form $a^2+3b^2$: a table extending from $p=7$ to 12007 (calculated also by *Zornow*) is given by

**Jacobi,** *Crelle,* t. XXX. (1846), *ut suprà,* pp. 177—179.

This is carried by Reuschle up to $p=13369$, and for certain higher numbers up to 49999, as presently mentioned. Reuschle observes that $6427=80^2+3.3^2$ is by accident omitted, and that 6481 should be $=41^2+3.40^2$.

39. Again, primes of the form $8n+1$ are expressible in the form $p=a^2+2b^2$ (or say $=c^2+2d^2$), the theory being connected with that of the complex numbers composed with the 8th roots of unity $\left(\text{fourth root of } -1, =\dfrac{1+i}{\sqrt{2}}\right)$.

$p=c^2+2d^2$; viz. decomposition of primes of the form $8n+1$ into the form $c^2+2d^2$:

www.rcin.org.pl

a table extending from $p = 16$ to 5943 (extracted from a MS. table calculated by *Struve*) is given by

**Jacobi,** *Crelle*, t. XXX. (1846), *ut suprà*, p. 180.

This is carried by Reuschle up to $p = 12377$, and for certain higher numbers up to 24889, as presently mentioned.

40. Reuschle's tables of the forms in question are contained in the work:—

**Reuschle,** *Mathematische Abhandlung*, &c. (see *ante* No. 15), under the heading "B. Tafeln zur Zerlegung der Primzahlen in Quadrate" (pp. 22—41). They are as follows:—

Table III. for the primes $6n + 1$.

The first part gives $p = A^2 + 3B^2$ and $4p = L^2 + 27M^2$, from $p = 7$ to 5743. The table gives $A$, $B$, $L$, $M$; those numbers which have 10 for a cubic residue are distinguished by an asterisk. A specimen is

| $p$ | $A$ | $B$ | $L$ | $M$ |
|---|---|---|---|---|
| 37* | 5 | 2 | 11 | 1 ; |

viz. $37 = 5^2 + 3 . 2^2$, $148 = 11^2 + 27 . 1^2$; the asterisk shows that $x^3 \equiv +10$ (mod. 37) is possible: in fact $34^3 \equiv 10$ (mod. 37).

The second part gives $p = A^2 + 3B^2$ only, from $p = 5749$ to 13669. The table gives $A$, $B$; and the asterisk implies the same property as before.

The third part gives $p = A^2 + 3B^2$, but only for those values of $p$ which have 10 for a cubic residue, viz. for which $x^3 \equiv 10$ (mod. $p$) is possible, from $p = 13689$ to 49999. The table gives $A$, $B$; the asterisk, as being unnecessary, is not inserted.

Table IV. for the primes $4n + 1$ in the form $A^2 + B^2$, and for those which are also $8n + 1$ in the form $C^2 + 2D^2$.

The first part gives $p = A^2 + B^2$, $= C^2 + 2D^2$, from $p = 5$ to 12377. The table gives $A$, $B$, $C$, $D$; those numbers which have 10 for a biquadratic residue, viz. for which $x^4 \equiv 10$ (mod. $p$) is possible, are distinguished by an asterisk; those which have also 10 for an octic residue, viz. for which $x^8 \equiv 10$ (mod. $p$) is possible, by a double asterisk. A specimen is

| $p$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|
| 229 | 15 | 2 | — | — |
| 233 | 13 | 8 | 15 | 2 |
| 241** | 15 | 4 | 13 | 6 |

The second part gives $p = A^2 + B^2$, from $p = 12401$ to 24917 for all those values of $p$ which have 10 for a biquadratic residue ($x^4 \equiv 10$ (mod. $p$) possible). The table gives $A$, $B$; those values of $p$ which have 10 for an octic residue, viz. for which $x^8 \equiv 10$ (mod. $p$) is possible, are distinguished by an asterisk.

www.rcin.org.pl

The third part gives $p=C^2+2D^2$, from $p=12641$ to 24889 for all those values of $p$ which have 10 for a biquadratic residue. The table gives $C$, $D$; those values of $p$ which have 10 as an octic residue are distinguished by an asterisk.

41. A table by **Zornow,** *Crelle,* t. XIV. (1835), pp. 279, 280 (belonging to the Memoir "De Compositione numerorum e Cubis integris positivis," pp. 276—280), shows for the numbers 1 to 3000 the least number of cubes into which each of these numbers can be decomposed. Waring gave, without demonstration, the theorem that every number can be expressed as the sum of at most 9 cubes. The present table seems to show that 23 is the only number for which the number of cubes is $=9\,(=2\,.\,2^3+7\,.\,1^3)$; that there are only fourteen numbers for which the number of cubes is $=8$, the largest of these being 454; and hence that every number greater than 454 can be expressed as a sum of at most 7 cubes; and further, that every number greater than 2183 can be expressed as a sum of at most 6 cubes. A small subsidiary table (p. 276) shows that the number of numbers requiring 6 cubes gradually diminishes—e.g. between $12^3$ and $13^3$ there are seventy-five such numbers, but between $13^3$ and $14^3$ only sixty-four such numbers; and the author conjectures "that for numbers beyond a certain limit every number can be expressed as a sum of at most 5 cubes."

42. For the decomposition of a number into biquadrates we have

**Bretschneider,** "Tafeln für die Zerlegung der Zahlen bis 4100 in Biquadrate," *Crelle,* t. XLVI. (1853), pp. 3—23.

Table I. gives the decompositions, thus:—

| $N$ | $1^4$, | $2^4$, | $3^4$, | $4^4$, | $5^4$, |
|---|---|---|---|---|---|
| 696 | 6 | 1 | 2 | 2 | |
| | 3 | 2 | 5 | 1 | |
| | 0 | 3 | 8 | | |

viz. $696=6\,.\,1^4+1\,.\,2^4+2\,.\,3^4+2\,.\,4^4$, &c.

And Table II. enumerates the numbers which are sums of at least 2, 3, 4,.., 19 biquadrates. There is at the end a summary showing for the first 4100 numbers how many numbers there are of these several forms respectively: 28 numbers are each of them a sum of 2 biquadrates, 75 a sum of 3,..., 7 a sum of 19 biquadrates. The seven numbers, each of them a sum of 19 biquadrates, are 79, 159, 239, 319, 399, 479, 559.

[F. 16. *Binary, Ternary, &c. quadratic and higher forms.*] Art. VI.

43. Euler worked with the quadratic forms $ax^2 \pm cy^2$ ($p$ and $q$ integers), particularly in regard to the forms of the divisors of such numbers. It will be sufficient to refer to his memoir:—

www.rcin.org.pl

**Euler,** "Theoremata circa divisores numerorum in hac forma $pa^2 \pm qb^2$ contentorum," (*Op. Arith. Coll.* pp. 35—61, 1744), containing fifty-nine theorems, exhibiting in a quasi-tabular form the linear forms of the divisors of such numbers. As a specimen:—

"Theorema 13. Numerorum in hac forma $a^2 + 76b^2$ contentorum divisores primi omnes sunt vel 2, vel 7, vel in una sex formularum

$$\begin{array}{ll} 28m+1, & 28m+11, \\ 28m+9, & 28m+15, \\ 28m+25, & 28m+23, \end{array}$$

seu in una harum trium

$$\begin{array}{l} 14m+1, \\ 14m+9, \\ 14m+11, \end{array}$$

sunt contenti"; viz. the forms are the three $14m+1$, $14m+9$, $14m+11$.

But Euler did not consider, or if at all very slightly, the trinomial forms $ax^2 + bxy + cy^2$, nor attempt the theory of the reduction of such forms. This was first done by Lagrange in the memoir

Lagrange, *Mém. de Berlin,* 1773. And the theory is reproduced by

Legendre, *Théorie des Nombres,* Paris, 1st ed. 1798; 2nd ed. 1808, § 8, "Réduction de la formule $Ly^2 + Myz + Nz^2$ à l'expression la plus simple," (2nd ed. pp. 61—67).

44. But the classification of quadratic forms, as established by Legendre, is defective as not taking account of the distinction between proper and improper equivalence; and the ulterior theory as to orders and genera, and the composition of forms (although in the meantime established by Gauss), are not therein taken into account; for this reason the **Legendre's** Tables I. to VIII. relating to quadratic forms, given after p. 480 (thirty-two pages not numbered), are of comparatively little value, and it is not necessary to refer to them in detail.

The complete theory was established by

Gauss, *Disquisitiones Arithmeticæ,* 1801.

It is convenient to refer also to the following memoir:

Lejeune Dirichlet, "Recherches sur diverses applications de l'Analyse à la théorie des Nombres," *Crelle,* t. XIX. (1839), p. 338, [*Ges. Werke,* t. I. p. 427], as giving a succinct statement of the principle of classification, and in particular a table of the characters of the genera of the properly primitive order, according to the four forms $D = PS^2$, $P \equiv 1$ or 3 (mod. 4), and $D \equiv 2PS^2$, $P \equiv 1$ or 3 (mod. 4), of the determinant.

45. Tables of quadratic forms arranged on the Gaussian principle are given by

**Cayley,** *Crelle,* t. LX. (1862), pp. 357—372, [335]; viz. the tables are—

Table I. des formes quadratiques binaires ayant pour déterminants les nombres négatifs depuis $D = -1$ jusqu'à $D = -100$. (Pp. 360—363: [*Coll. Math. Papers,* t. V. pp. 144—147].)

www.rcin.org.pl

A specimen is

| $D$ | Classes | $\alpha$ | $\beta$ | $\delta$ | $\epsilon$ | $\delta\epsilon$ | Cp |
|---|---|---|---|---|---|---|---|
| $=26$ | 1, 0, 26 | + | | | | + | 1 |
| | 3, −1, 9 | + | | | | + | $g^2$ |
| | 3, 1, 9 | + | | | | + | $g^4$ |
| | 5, 2, 6 | − | | | | − | $g$ |
| | 2, 0, 13 | − | | | | − | $g^3$ |
| | 5, −2, 6 | − | | | | − | $g^5$ |

where $\alpha$, $\beta$ denote, as there explained, the characters in regard to the odd prime factors of $D$; $\delta$, $\epsilon$, $\delta\epsilon$ those in regard to the numbers 4 and 8. The last column shows that the forms in the two genera respectively are 1, $g^2$, $g^4$ and $g$, $g^3$, $g^5$, where $g^6=1$, viz. the form $g$, six times compounded, gives the principal form (1, 0, 26).

Table II. des formes quadratiques binaires ayant pour déterminants les nombres positifs non-carrés depuis $D=2$ jusqu'à $D=99$. (Pp. 364—369: [*l.c.*, pp. 148—153].)

The arrangement is the same, except that there is a column "Périodes" showing, in an easily understood abbreviated form, the period of each form. Thus $D=7$, the period of the principal form (1, 0, −7), is given as 1, ₂, −3, ₁, 2, ₁, −3, ₂, 1, which represents the series of forms (1, 2, −3), (−3, 1, 2) (2, 1, −3), (−3, 2, 1).

Table III. des formes quadratiques binaires pour les treize déterminants négatifs irréguliers du premier millier. (Pp. 370—372: [*l.c.*, pp. 154—156].)

The arrangement is the same as in Table I. It may be mentioned that the thirteen numbers, and the forms for the principal genus for these numbers, respectively are:—

| $-D=$ | Principal genus |
|---|---|
| 576, 580, 820, 900 | $(1, e^2)(1, e_1^2)$ |
| 884 | $(1, e^2)(1, i^2, i^4, i^6)$ |
| 243, 307, 339, 459, 675, 891 | $(1, d, d^2)(1, d_1, d_1^2)$ |
| 755, 974 | $(1, d, d^2)(1, d_1, d_1^2)(1, e^2)$, |

where $d^3=d_1^3=1$, $e^4=e_1^4=1$, $i^8=1$, viz. $(1, e^2)(1, e_1^2)$ denotes four forms, $1, e^2, e_1^2, e^2e_1^2$; and so in the other cases.

46. **Gauss** must have computed quadratic forms to an enormous extent; but, for the reasons (rather amusing ones) mentioned in a letter of May 17, 1841, to Schumacher (quoted in Prof. Smith's Report on "The Theory of Numbers," *Brit. Assoc. Report* for 1862, p. 526, [and Smith's *Coll. Math. Papers*, t. I. p. 261]), he did not preserve his results in detail, but only in the form appearing in the

"Tafel der Anzahl der Classen binärer quadratischer Formen," *Werke*, t. II. pp. 449—476; see editor's remarks, pp. 521—523.

www.rcin.org.pl

This relates almost entirely to negative determinants, only three quarters of p. 475 and p. 476 to positive ones; for negative determinants, it gives the number of genera and classes, as also the index of irregularity for the determinants of the hundreds 1 to 30, 43, 51, 61, 62, 63, 91 to 100, 117 to 120; then, in a different arrangement, for the thousands 1, 3 and 10, for the first 800 numbers of the forms $-(15n+7)$ and $-(15n+13)$; also for some very large numbers, and for positive determinants of the hundreds 1, 2, 3, 9, 10, and for some others.

A specimen is

| | | | |
|---|---|---|---|
| | Centas I. | | |
| G II. | (58) ... (280) | | |
| 1. | 5, | 6, | 8, |
| | 9, | 10, | 12, |
| | 13, | 15, | 16, |
| | 18, | 22, | 25, |
| | 28, | 37, | 58, |
| 2. | 14, | 17, | 20, |
| | ................ | | |
| Summa | 233 ...... 477 | | |
| Irreg. | 0 Impr. 74; | | |

viz. this shows, as regards the negative determinants 1 to 100, that the determinants belonging to G II. 1, viz. those which have two genera each of one class, are 5, 6, 8, 9, &c., in all fifteen determinants; those belonging to G II. 2, viz. those which have two genera each of two classes, are 14, 17, 20, &c.; and so on. The head numbers (58) ... (280) show the number of determinants, each having two genera, and the number of classes; thus,

$$
\begin{array}{lrr}
\text{G II.} & 1\times 15 = & 15 \\
 & 2\times 17 = & 34 \\
 & 3\times 17 = & 51 \\
 & 4\times 6 = & 24 \\
 & 5\times 2 = & 10 \\
 & 6\times 1 = & 6 \\
 & \overline{58} & \overline{140} \\
 & & \times 2 \\
 & & = 280;
\end{array}
$$

and the bottom numbers show the total number of genera and of classes, thus

$$
\begin{array}{lrrr}
\text{G I.} & 17\times 1 = & 17 & 61 \\
\text{II.} & 58\times 2 = & 116 & 280 \\
\text{IV.} & 25\times 4 = & 100 & 136 \\
 & \overline{100} & \overline{233} & \overline{477};
\end{array}
$$

viz. seventeen determinants, each of one genus, and together of sixty-one classes; fifty-eight determinants, each of two genera, and together of 280 classes: and twenty-five determinants, each of four genera, and together 136 classes, give in all 233 genera and 477 classes. These are exclusive of 74 classes belonging to the improperly primitive order; and the number of irregular determinants (in the first hundred) is $=0$.

The irregular determinants are indicated thus:

243(*3*),
307(*3*), 339(*3*),
459(*),
576(*2*), 580(*2*),
675(*3*),
755(*3*),
891(*3*), 820(*2*), 900(*2*), 884(*2*), 974(*3*),
*3* 243, 307, 339, 459 ?, 675, 755, 891,
*2* 576, 589, 820, 884, 900, 974,

which is a notation not easily understood.

As regards the positive determinants, a specimen is

Centas I.
Excedunt determinantis
quadrati 10.

| | | | |
|---|---|---|---|
| G I. | | ... (12), | |
| 1. | 2, | 5, | 13, |
| | 17, | 29, | 41, |
| | 53, | 61, | 73, |
| | 89, | 97, | |
| 3. | 37; | | |

viz. in the first hundred, the positive determinants having one genus of one class are 2, 5, 13, &c.... (eleven in number); that having one genus of three classes is 37, (one in number); $11+1=12$. The irregular determinants, if any, are not distinguished.

47. *Binary cubic forms.*—The earliest table is given by

**Arndt,** "Tabelle der reducirten binären kubischen Formen und Klassen für alle negativen Determinanten $-D$ von $D=3$ bis $D=2000$," *Grunert's Archiv*, t. XXXI. 1858, pp. 369—448.

The memoir is a sequel to one in t. XVII. (1851). The binary cubic form $(a,\ b,\ c,\ d)$, of determinant $-D\left(=(bc-ad)^2-4(b^2-ac)(c^2-bd)\right)$, is said to be reduced when its characteristic $\phi,\ =(A,\ B,\ C),\ =\left(2(b^2-ac),\ bc-ad,\ 2(c^2-bd)\right)$, is a reduced quadratic form, that is, when in regard to absolute values $B$ is not $>\frac{1}{2}A$, $C$ not $<A$.

www.rcin.org.pl

A specimen is

| $D$ | Reduced forms, with characters | Classes |
|---|---|---|
| 44 | (0, 1, 0, −11) (1, −1, −2, 0)<br>(2, 0, 22 6, 2, 8) | (0, −1, 0, 11) (0, −2, ±1, 1) |

Two subsidiary tables are given, pp. 351, 352, and 353—368.

48. It appeared suitable to remodel a part of this table in the manner made use of for quadratic forms in my tables above referred to; and it is accordingly divided into the three tables given by

**Cayley,** *Quart. Math. Journ.* t. XI. (1871), where the notation &c. is explained, pp. 251—261, [496]; viz. these are:—

Table I. of the binary cubic forms, the determinants of which are the negative numbers $\equiv 0$ (mod. 4) from $-4$ to $-400$ (pp. 251—258; [*Coll. Math. Papers*, t. VIII., pp. 55—61]).

A specimen is

| Det. 4 × | Classes. | Order. | Charact. | Comp. |
|---|---|---|---|---|
| 11. | 0, −1, 0, 11 | on | 1, 0, 11 | 1 |
| | 0, −2, −1, 1 | *pp pp* | 3, 1, 4 | $d$ |
| | 0, −2, 1, 1 | | 3, −1, 4 | $d^2$. |

Table II. of the binary cubic forms the determinants of which (taken positively) are $\equiv 1$ (mod. 4) from $-3$ to $-99$, the original heading is here corrected, [*l.c.*, pp. 61, 62]; and

Table III. of the binary cubic forms the determinants of which are the negative numbers $-972$, $-1228$, $-1336$, $-1836$, and $-2700$, [*l.c.*, pp. 63, 64]; viz. $-972 = 4 \times -243, \ldots, -2700 = 4 \times -675$, where $-243, \ldots, -675$ are the first six irregular numbers for quadric forms.

$4 \times -675, = -2700$ is beyond the limits of Arndt's tables, and for this number the calculation had to be made anew; the table gives nine classes $(1, d, d^2)$ $(1, d_1, d_1^2)$ of the order *ip* on *pp*, but it is remarked that there may possibly be other cubic classes based on a non-primitive characteristic; the point was left unascertained.

49. The theory of ternary quadratic forms was discussed and partially established by Gauss in the *Disquisitiones Arithmeticæ*. It is proper to recall that a ternary quadratic form is either determinate, viz. always positive, such as $x^2+y^2+z^2$, or always negative, such as $-x^2-y^2-z^2$; or else it is indeterminate, such as $x^2+y^2-z^2$. But as regards determinate forms, the negative ones are derived from the positive ones by simply reversing the signs of all the coefficients, so that it is sufficient to attend to the positive forms; and practically the two cases are positive forms (meaning thereby positive determinate forms) and indeterminate forms; but the theory for positive forms was first established completely, and so as to enable the formation of tables, in the work

**Seeber,** *Ueber die Eigenschaften der positiven ternären quadratischen Formen*, (4to. Freiburg, 1831),



www.rcin.org.pl

which is reviewed by Gauss in the *Gött. Gelehrte Anzeigen,* 1831, July 9 (see Gauss, *Werke,* t. II. pp. 188—193). The author gives (pp. 220—243) tables "of the classes of positive ternary forms represented by means of the corresponding reduced forms" for the determinants 1 to 100. A specimen is

$$\text{Det. } 6 \quad \begin{pmatrix} 1, & 1, & 2 \\ 0, & 0, & -1 \end{pmatrix}, \begin{pmatrix} 1, & 1, & 2 \\ -1, & -1, & 0 \end{pmatrix},$$

$$\begin{matrix}\text{Zugeordnete}\\ \text{Formen}\end{matrix} \begin{pmatrix} 8, & 8, & 3 \\ 0, & 0, & 8 \end{pmatrix}, \begin{pmatrix} 7, & 7, & 4 \\ 4, & 4, & 2 \end{pmatrix},$$

where it is to be observed that Seeber admits odd coefficients for the terms in $yz$, $zx$, $xy$; viz. his symbol $\begin{pmatrix} a, & b, & c \\ f, & g, & h \end{pmatrix}$ denotes

$$ax^2 + by^2 + cz^2 + fyz + gzx + hxy,$$

and his determinant is

$$4abc - af^2 - bg^2 - ch^2 + fgh.$$

Also his adjoint form is

$$\begin{pmatrix} 4bc - f^2, & 4ca - g^2, & 4ab - h^2 \\ 2gh - 4af, & 2hf - 4bg, & 2fg - 4ch \end{pmatrix}, = (4bc - f^2)\,x^2 + \ldots + (2gh - 4af)\,yz + \ldots$$

In the notation of the *Disquisitiones Arithmeticæ,* followed by Eisenstein and others, the symbol $\begin{pmatrix} a, & b, & c \\ f, & g, & h \end{pmatrix}$ denotes

$$ax^2 + by^2 + cz^2 + 2fyz + 2gzx + 2hxy;$$

the determinant is

$$= -(abc - af^2 - bg^2 - ch^2 + 2fgh),$$

a positive form having thus always a negative determinant. And the adjoint form is

$$-\begin{pmatrix} bc - f^2, & ca - g^2, & ab - h^2 \\ gh - af, & hf - bg, & fg - ch \end{pmatrix}, = -(bc - f^2)\,x^2 - \ldots - 2\,(gh - af)\,yz - \ldots$$

Hence Seeber's determinant is $= -4$ multiplied by that of Gauss, and his tables really extend between the values $-1$ and $-25$ of the Gaussian determinant.

50. Tables of greater extent, and in the better form just referred to, are given by **Eisenstein,** *Crelle,* t. XLI. (1851), pp. 169—190; viz. these are

I. "Tabelle der eigentlich primitiven positiven ternären Formen für alle negativen Determinanten von $-1$ bis $-100$," (pp. 169—185).

A specimen is

| $D$ | Anzahl | Reducirte Formen für $-D$ |
|---|---|---|
| 10 | 3 | $\begin{pmatrix} 1, & 1, & 10 \\ 0, & 0, & 0 \end{pmatrix}, \begin{pmatrix} 1, & 2, & 5 \\ 0, & 0, & 0 \end{pmatrix}, \begin{pmatrix} 2, & 2, & 3 \\ 0, & -1, & 0 \end{pmatrix}.$ |
| | | $\delta = 8 \qquad \delta = 4 \qquad \delta = 4$ |

www.rcin.org.pl

II. "Tabelle der *uneigentlich* primitiven positiven ternären Formen für alle negativen Determinanten von $-2$ bis $-100$," (pp. 186—189).

A specimen is

| $D$ | Anzahl | Reducirte Formen für $-D$ |
|---|---|---|
| 10 | 1 | $\begin{pmatrix}2, & 2, & 4\\ 1, & 1, & 1\end{pmatrix}$. $\delta = 6$. |

And there is given (p. 190) a table of the reduced forms for the determinant $-385\,(=-5\,.\,7\,.\,11)$, selected merely as a largish number with three factors; viz. there are in all fifty-nine forms, corresponding to values 1, 2, 4, 6, 8 of $\delta$.

It may be remarked that $\delta$ denotes, for any given form, the number of ways in which this is linearly transformable into itself, this number being always 1, 2, 4, 6, 8, 12, or 24. The theory as to this and other points is explained in the memoir (pp. 141—168), and various subsidiary tables are contained therein and in the *Anhang* (pp. 227—242); and there is given a small table relating to *indeterminate forms*, viz. this is

"C. Versuch einer Tabelle der nicht äquivalenten unbestimmten (indifferenten) ternären quadratischen Formen für die Determinanten ohne quadratischen Theiler unter 20," (pp. 239, 240).

A specimen is

| $D$ | Indifferente ternäre quadratische Formen |
|---|---|
| 10 | $\begin{pmatrix}0, & 1, & 10\\ 0, & 0, & 1\end{pmatrix}$, $\begin{pmatrix}1, & 2, & -5\\ 0, & 0, & 0\end{pmatrix}$, |
| | $\begin{pmatrix}0, & 0, & 10\\ 0, & 0, & 1\end{pmatrix}$, |

where, when the determinant is even, the forms in the second line are always improperly primitive forms.

[F. 17. *Complex Theories.*] Art. VII.

51. The theory of binary quadratic forms $(a, b, c)$, with complex coefficients of the form $\alpha+\beta i$, $(i=\sqrt{-1}$ as usual, $\alpha$ and $\beta$ integers), has been studied by Lejeune Dirichlet, Prof. H. J. S. Smith, and possibly others; but no tables have, it is believed, been calculated. The calculations would be laborious; but tables of a small extent only would be a sufficient illustration of the theory, and would, it is thought, be of great interest.

www.rcin.org.pl

The theory of complex numbers of the last-mentioned form $\alpha+\beta i$, or say of the numbers formed with the fourth root of unity, had previously been studied by Gauss; and the theory of the numbers formed with the cube roots of unity ($\alpha+\beta\omega$, $\omega^2+\omega+1=0$, $\alpha$ and $\beta$ integers) was studied by Eisenstein; but the general theory of the numbers involving the $n$th roots of unity ($n$ an odd prime) was first studied by Kummer. It will be sufficient to refer to his memoir,

Kummer, "Zur Theorie der complexen Zahlen," *Berl. Monatsb.*, March, 1845; and *Crelle*, t. XXXV. (1847), pp. 319—326; also "Ueber die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren," same volume, pp. 327—367, where the astonishing theory of "Ideal Complex Numbers" is established.

52. It may be recalled that, $p$ being an odd prime, and $\rho$ denoting a root of the equation $\rho^{p-1}+\rho^{p-2}+\ldots+\rho+1=0$, then the numbers in question are those of the form $a+b\rho+\ldots+k\rho^{n-2}$, where $(a, b, .., k)$ are integers; or (what is in one point of view more, and in another less, general) if $\eta, \eta_1, .., \eta_{e-1}$ are "periods" composed with the powers of $\rho$ ($e$ any factor of $p-1$), then the form considered is $a\eta+b\eta_1+\ldots+h\eta_{e-1}$. For any value of $p$ or $e$ there is a corresponding complex theory. A number (real or complex) is in the complex theory prime or composite, according as it does not, or does, break up into factors of the form under consideration. For $p$ a prime number under 23, if in the complex theory $N$ is a prime, then any power of $N$ (to fix the ideas say $N^3$) has no other factors than $N$ or $N^2$; but if $p=23$ (and similarly for higher values of $p$), then $N$ may be such that, for instance, $N^3$ has complex factors other than $N$ or $N^2$ (for $p=23$, $N=47$ is the first value of $N$, viz. $47^3$ has factors other than 47 and $47^2$); say $N^3$ has a complex prime factor $A$, or we have $\sqrt[3]{A}$ as an ideal complex factor of $N$. Observe that by hypothesis $N$ is not a perfect cube, viz. there is no complex number whose cube is $=A$. In the foregoing general statement, made by way of illustration only, all reference to the complex factors of unity is purposely omitted, and the statement must be understood as being subject to correction on this account.

What precedes is by way of introduction to the account of **Reuschle's** Tables (*Berliner Monatsberichte*, 1859—60), which give in the different complex theories $p=5$, 7, 11, 13, 17, 19, 23, 29 the complex factors of the decomposable real primes up to in some cases 1000.

It should be remarked that the form of a prime factor is to a certain extent indeterminate, as the factor can without injury be modified by affecting it with a complex factor of unity; but in the tables the choice of the representative form is made according to definite rules, which are fully explained, and which need not be here referred to.

www.rcin.org.pl

53. The following synopsis is convenient:—

| | Theory of the $p$th roots | Form of real prime to mod. $p \equiv$ | No. of factors in complex theory | Extent of table; all primes under | Equation of periods |
|---|---|---|---|---|---|
| 1859. pp. 488–491. | 5 | 1 | 4 | 2500 | $\alpha^4 + \ldots + \alpha + 1 = 0.$ |
| | | 4 | 2 (not tabulated) | | $y^2 + y - 1 = 0.$ |
| | | 2, 3 | prime. | | |
| 694–697. | 7 | 1 | 6 | 1000 | $\alpha^6 + \ldots + \alpha + 1 = 0.$ |
| | | 6 | 3 | | $y^3 + y^2 - 2y - 1 = 0.$ |
| | | 2, 4 | 2 | | $y^2 + y + 2 = 0.$ |
| | | 3, 5 | prime. | | |
| 1860. pp. 190–194. | 11 | 1 | 10 | 1000 | $\alpha^{10} + \ldots + \alpha + 1 = 0.$ |
| | | 10 | 5 | | $y^5 + y^4 - 4y^3 - 3y^2 + 3y + 1 = 0.$ |
| | | 3, 4, 5, 9 | 2 | | $y^2 + y + 3 = 0.$ |
| | | 2, 6, 7, 8 | 1 | | |
| 194–199. | 13 | 1 | 12 | 1000 | $\alpha^{12} + \ldots + \alpha + 1 = 0.$ |
| | | 12 | 6 | | $y^6 + y^5 - 5y^4 - 4y^3 + 6y^2 + 3y - 1 = 0.$ |
| | | 3, 9 | 4 | | $y^4 + y^3 + 2y^2 - 4y + 3 = 0.$ |
| | | 5, 8 | 3 | | $y^3 + y^2 - 4y + 1 = 0.$ |
| | | 4, 10 | 2 | | $y^2 + y - 3 = 0.$ |
| | | 2, 6, 7, 11 | prime. | | |
| 714–719. | 17 | 1 | 16 | 1000 | $\alpha^{16} + \ldots + \alpha + 1 = 0.$ |
| | | 16 | 8 | | $y^8 + y^7 - 7y^6 - 6y^5 + 15y^4 + 10y^3 - 10y^2 - 4y + 1 = 0.$ |
| | | 4, 13 | 4 | | $y^4 + y^3 - 6y^2 + 1 = 0.$ |
| | | 2, 8, 9, 15 | 2 | | $y^2 + y - 4 = 0.$ |
| | | 3, 5, 6, 7, 11, 12, 14 | prime. | | |
| 719–725. | 19 | 1 | 18 | 1000 | $\alpha^{18} + \ldots + \alpha + 1 = 0.$ |
| | | 18 | 9 | | $y^9 + y^8 - 8y^7 - 7y^6 + 21y^5 + 15y^4 - 20y^3 - 10y^2 + 5y + 1 = 0.$ |
| | | 7, 11 | 6 | | $y^6 + y^5 + 2y^4 - 8y^3 - y^2 + 5y + 7 = 0.$ |
| | | 8, 12 | 3 | | $y^3 + y^2 - 6y - 7 = 0.$ |
| | | 4, 5, 6, 9, 13, 17 | 2 | | $y^2 + y + 5 = 0.$ |
| | | 2, 3, 10, 13, 14, 15 | prime. | | |
| 725–729. | 23 | 1 | 22 | 1000 | $\alpha^{22} + \ldots + \alpha + 1 = 0.$ |
| | | 22 | 11 | | $y^{11} + y^{10} - 10y^9 - 9y^8 + 36y^7 + 28y^6 - 56y^5 - 35y^4 + 35y^3 + 15y^2 - 6y - 1 = 0.$ |
| | | 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 | 2 | | $y^2 + y + 6 = 0.$ |
| | | ?5, 7, 10, 11, 14, 15, 17, 19, 20, 21 | prime. | | |
| 729–734. | 29 | 1 | 28 | 1000 | $\alpha^{28} + \ldots + \alpha + 1 = 0.$ |
| | | 28 | 14 | | $y^{14} + y^{13} - 13y^{12} - 12y^{11} + 66y^{10} + 55y^9 - 165y^8 - 120y^7 + 210y^6 + 126y^5 - 126y^4 - 56y^3 + 28y^2 + 7y - 1 = 0.$ |
| | | 12, 17 | 7 | | $y^7 + y^6 - 12y^5 - 7y^4 + 28y^3 + 14y^2 - 9y + 1 = 0.$ |
| | | 7, 16, 20, 23, 24, 25 | 4 | | $y^4 + y^3 + 4y^2 + 20y + 23 = 0.$ |
| | | 4, 5, 6, 9, 13, 22 | 2 | | $y^2 + y - 7 = 0.$ |
| | | 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27 | prime. | | |

The foregoing synopsis of Reuschle's tables in the *Berliner Monatsberichte* was written previous to the publication of Reuschle's far more extensive work. It is

www.rcin.org.pl

allowed to remain, but some explanations which were given have been struck out, and were instead given in reference to the larger work, which is

**Reuschle,** *Tafeln complexer Primzahlen, welche aus Wurzeln der Einheit gebildet sind.* Berlin, 4° (1875), pp. iii—vi and 1—671.

This work (the mass of calculation is perfectly wonderful) relates to the roots of unity, the degree being any prime or composite number, as presently mentioned, having all the values up to and a few exceeding 100; viz. the work is in five divisions, relating to the cases:

I. (pp. 1—171), degree any odd prime of the first 100, viz. 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97;

II. (pp. 173—192), degree the power of an odd prime 9, 25, 27, 49, 81;

III. (pp. 193—440), degree a product of two or more odd primes or their powers, viz. 15, 21, 33, 35, 39, 45, 51, 55, 57, 63, 65, 69, 75, 77, 85, 87, 91, 93, 95, 99, 105;

IV. (pp. 441—466), degree an even power of 2, viz. 4, 8, 16, 32, 64, 128;

V. (pp. 467—671), degree divisible by 4, viz. 12, 20, 24, 28, 36, 40, 44, 48, 52, 56, 60, 68, 72, 76, 80, 84, 88, 92, 96, 100, 120;

the only excluded degrees being those which are the double of an odd prime, these, in fact, coming under the case where the degree is the odd prime itself.

It would be somewhat long to explain the specialities which belong to degrees of the forms II., III., IV., V.; and what follows refers only to Division I., degree an odd prime.

For instance, if $\lambda = 7$, $\lambda - 1 = 2 . 3$; the factors of 6 being 6, 3, 2, 1, there are accordingly four divisions, viz.

I. $\alpha$ a prime seventh root, that is, a root of $\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$;

II. $\eta_0 = \alpha + \alpha^{-1}$, $\eta_1 = \alpha^2 + \alpha^{-2}$, $\eta_2 = \alpha^3 + \alpha^{-3}$, or $\eta$ a root of $\eta^3 + \eta^2 - 2\eta - 1 = 0$, $\left\{\begin{array}{l} \eta_0^2 = 2 + \eta_1,\ \eta_1^2 = 2 + \eta_2,\ \text{\&c.} \\ \eta_0\eta_1 = \eta_0 + \eta_2,\ \text{\&c.} \\ \eta_0\eta_2 = \eta_1 + \eta_2,\ \text{\&c.}; \end{array}\right.$

III. $\eta_0 = \alpha + \alpha^2 + \alpha^4$, $\eta_1 = \alpha^3 + \alpha^5 + \alpha^6$, or $\eta$ a root of $\eta^2 + \eta + 2 = 0$;

IV. Real numbers.

I. $p = 7m + 1$. First, it gives for the several prime numbers of this form 29, 43, .., 967 the congruence roots, mod. $p$; for instance,

| $p$ | $\alpha$ | $\alpha^2$ | $\alpha^3$ | $\alpha^4$ | $\alpha^5$ | $\alpha^6$ |
|---|---|---|---|---|---|---|
| 29 | − 5 | − 4 | − 9 | − 13 | + 7 | − 6 |
| 43 | + 11 | − 8 | − 2 | + 21 | + 16 | + 4. |
| ⋮ | | | | | | |

www.rcin.org.pl

This means that, if $\alpha \equiv -5$ (mod. 29), then $\alpha^2 \equiv 25$, $\equiv -4$, $\alpha^3 \equiv 20$, $\equiv -9$, &c., values which satisfy the congruence $\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 \equiv 0$ (mod. 29).

Secondly, it gives, under the simple and the primary forms, the prime factors $f(\alpha)$ of these same numbers 29, 43,.., 967; for instance,

| $p$ | $f(\alpha)$ simple. | $f(\alpha)$ primary. |
|---|---|---|
| 29 | $\alpha + \alpha^2 - \alpha^3$ | $2 + 3\alpha - \alpha^2 + 5\alpha^3 - 2\alpha^4 + 4\alpha^5$ |
| 43 | $\alpha^2 + 2\alpha^6$ | $2\alpha - 2\alpha^2 + 4\alpha^4 - \alpha^5 - 5\alpha^6$. |

The definition of a primary form is a form for which $f(\alpha) f(\alpha^{-1}) \equiv f(1)^2$ mod. $\lambda$, and $f(\alpha) \equiv f(1)$ mod. $(1-\alpha)^2$. The simple forms are also chosen so as to satisfy this *last* condition; thus $f(\alpha) = \alpha + \alpha^2 - \alpha^3$, then $f(1) - f(\alpha) = 1 - \alpha - \alpha^2 + \alpha^3 = (1-\alpha)^2 (1+\alpha)$, $\equiv 0$ mod. $(1-\alpha)^2$.

II. $p = 7m - 1$. First, it gives for the several prime numbers of this form 13, 41,.., 937 the congruence roots, mod. $p$; for instance,

| $p$ | $\eta_0$ | $\eta_1$ | $\eta_2$ |
|---|---|---|---|
| 13 | $-3$ | $-6$ | $-5$ |
| 41 | $-4$ | $+14$ | $-11$; |
| ⋮ | | | |

and secondly, it gives, under the simple and the primary forms, the prime factors $f(\eta)$ of these same numbers 13, 41,.., 937; for instance,

| $p$ | $f(\eta)$ simple. | $f(\eta)$ primary. |
|---|---|---|
| 13 | $\eta_0 + 2\eta_2$ | $3 + 7\eta_1$ |
| 41 | $4 + \eta_0$ | $-11 + 7\eta_1 - 7\eta_2$. |
| ⋮ | | |

Thus $13 = (\eta_0 + 2\eta_2)(\eta_1 + 2\eta_0)(\eta_2 + 2\eta_1)$, as is easily verified; the product of first and second factors is $= 4 + 3\eta_0 + 8\eta_1 + 5\eta_2$, and then multiplying by the third factor, the result is $42 + 29(\eta_0 + \eta_2)$, $= 13$.

III. $p = 7m + 2$ or $7m + 4$. First, it gives for the several prime numbers of this form 2, 11,.., 991 the congruence roots, mod. $p$; for instance,

| $p$ | $\eta_0$ | $\eta_1$ |
|---|---|---|
| 2 | 0 | $-1$ |
| 11 | 4 | $-5$; |
| ⋮ | | |

and secondly, it gives the primary prime factors $f(\eta)$ of these same numbers; for instance,

| $p$ | $f(\eta)$ |
|---|---|
| 2 | $\eta_0$ |
| 11 | $1 - 2\eta_1$. |



www.rcin.org.pl

IV. $p = 7m + 3$ or $7m + 5$. The prime numbers of these forms, viz. 3, 5, 17, 19,.., 997, are primes in the complex theory, and are therefore simply enumerated.

The arrangement is the same for the higher prime numbers $\lambda = 23$, &c., for which ideal factors make their appearance; but it presents itself under a more complicated form. Thus $\lambda = 23$, $\lambda - 1 = 2 . 11$, and the factors of 22 are 22, 11, 2, 1. There are thus four sections.

I. $\alpha$ a prime root, or $\alpha^{22} + \alpha^{21} + \ldots + \alpha^2 + \alpha + 1 = 0$;

II. $\eta_0 = \alpha + \alpha^{-1}, \ldots, \eta_{10} = \alpha^{11} + \alpha^{-11}$, or $\eta$ a root of $\eta^{11} + \eta^{10} - 10\eta^9 + \ldots + 15\eta^2 - 6\eta - 1 = 0$;

III. $\eta_0 = \alpha + \alpha^2$, $\eta_1 = \alpha^{-1} + \alpha^{-2}$, or $\eta$ a root of $\eta^2 + \eta + 6 = 0$;

IV. Real numbers.

I. $p = 23m + 1$. First, it gives for the prime numbers of this form 47, 139,.., 967 congruence roots, mod. $p$, and *also* congruence roots, mod. $p^3$ *; these last in the form $a + bp + cp^2$, where $a$ is given in the former table; thus first table:—

| $p$ | $\alpha$ | $\alpha^2$ | $\alpha^3 \ldots$ | $\alpha^{22}$ |
|---|---|---|---|---|
| 47 | 6 | $-11$ | $-19\ldots$ | $+8$; |

and second table—

| $p$ | $\alpha$ | $\alpha^2$ | $\alpha^3 \quad \ldots$ | $\alpha^{22}$ |
|---|---|---|---|---|
| 47 | $+p-2p^2$ | $+13p-23p^2$ | $+19p-8p^2\ldots$ | $+22p+22p^2$. |

The meaning is that, $p = 47$, the roots of the congruence

$$\alpha^{22} + \alpha^{21} + \ldots + \alpha^2 + \alpha + 1 \equiv 0 \text{ (mod. } 47^3)$$

are

$$\alpha = 6 + p - 2p^2, \ \alpha^2 = -11 + 13p - 23p^2, \text{ \&c.}$$

Secondly, it then gives $f(\alpha)$, the actual ideal prime factor of these same primes 47, 139,.., 967; viz. the whole of this portion of the table $\lambda = 23$, I. (2) is,

having actual prime factors,

| $p$ | $f(\alpha)$ |
|---|---|
| 599 | $\alpha + \alpha^{16} - \alpha^{17}$ |
| 691 | $\alpha^3 + \alpha^{21} + \alpha^{22}$ |
| 829 | $\alpha^2 + \alpha^5 + \alpha^{46}$; |

having ideal factors, their third powers actual,

| $p$ | $f^3(\alpha)$ |
|---|---|
| 47 | $\alpha^4 + \alpha^5 + \alpha^9 + \alpha^{10} + \alpha^{16} - \alpha^{20} + \alpha^{22}$ |
| 139 | $1 - \alpha^3 - \alpha^7 + \alpha^9 + \alpha^{11} + \alpha^{14} + \alpha^{15} + \alpha^{17} + \alpha^{18} + \alpha^{20} + \alpha^{21}$ |
| 277 | $\alpha^2 - \alpha^4 - \alpha^6 + \alpha^7 - \alpha^{10} - \alpha^{15} - \alpha^{17} + \alpha^{21} + \alpha^{22}$ |
| 461 | $\alpha - \alpha^2 + \alpha^3 - \alpha^9 + \alpha^{14} - 2\alpha^{15}$ |
| 967 | $\alpha^2 - \alpha^3 - \alpha^5 + \alpha^{10} + \alpha^{15} - 2\alpha^{16} + \alpha^{17} + \alpha^{19}$. |

I repeat the explanation that, for the number 47, this means $f(\alpha) f(\alpha^2) \ldots f(\alpha^{22}) = 47^3$.

* Where, as presently appearing, 3 is the index of ideality or power to which the ideal factors have to be raised in order to become actual.

www.rcin.org.pl

And the like further complication presents itself in the part III. of the same table, $\lambda = 23$ (not, as it happens, in part II., nor of course in the concluding part IV., which is a mere enumeration of real primes). Thus III. (1), we have congruences, (mod. $p^3$),

$$p = 2, \quad \eta \equiv -2, \quad p = 3, \quad \eta_0 = +12, \text{ \&c.};$$

and having actual prime factors,

$$\begin{array}{ll} p & f(\eta) \\ 59 & 5 - 2\eta_1 \\ 101 & 1 - 4\eta_1\,; \\ \vdots & \end{array}$$

and having ideal prime factors, their third powers actual,

$$\begin{array}{ll} p & f^3(\eta) \\ 2 & 1 - \eta_1 \\ 3 & 1 - 2\eta_1\,; \\ \vdots & \end{array}$$

as regards these last the signification being

$$2^3 = (1 - \eta_0)(1 - \eta_1), \quad \eta_0 + \eta_1 = -1, \quad \eta_0\eta_1 = 6 \text{ (as is at once verified)},$$

$$3^3 = (1 - 2\eta_0)(1 - 2\eta_1)\,;$$

but the simple numbers 2, 3 are neither of them of the form $(a + b\eta_0)(a + b\eta_1)$.

## CONTENTS OF REPORT 1875 ON MATHEMATICAL TABLES.

§ 7. *Tables* F. *Arithmological.*





www.rcin.org.pl