SOME CRITERIA FOR THE RESIDUES OF EIGHTH AND OTHER POWERS

By A. E. WESTERN.

[Received August 9th, 1910.—Read April 22nd, 1909.]

TABLE OF CONTENTS.

	Introduction	§§ 1–3
Part I.	Expressions for $\{q/\pi\}_8$ in terms of a, b and c, d; also in terms of π ...	4–15
II.	Expressions for $\{q/\pi\}_8$ in terms of a, b and e, f	16–18
III.	Expressions for $\{q/\pi\}_{16}$, where $q = 3$ or 5	19–24
IV.	Expressions for $\{q/\pi\}_9$, where $q = 2$ or 5	25–26
V.	Expressions for $\{q/\pi\}_8$ in terms of a, b and x, y, where $p = x^2-(-1)^{\frac{1}{2}(q-1)}qy^2$. The quartic field $k(\omega, \theta)$	27–34
VI.	Expressions for $\{q/\pi\}_8$ in terms of a, b and x', y', where $p=x'^2+(-1)^{\frac{1}{2}(q-1)}qy'^2$. The quartic field $k(\iota, \theta)$	35–37

1. This paper falls into two distinct portions, Parts I–IV and Parts V–VI. The object of the first four parts is to develop some of the practical consequences of the law of l^n-th reciprocity proved in my two papers entitled "An Extension of Eisenstein's Law of Reciprocity."* The notation used in the first four parts is as follows.

$p = ml^n+1$ is a rational prime number.

ζ is a primitive l^n-th root of 1.

The field of complex numbers defined by ζ is called $k(\zeta)$.

This paper is confined to the cases $l^n = 2^3$, 2^4, and 3^2.

Rational numbers are denoted by italic letters, and complex numbers of the field $k(\zeta)$ by Greek letters.

π is a prime factor of p in the field $k(\zeta)$.

q is a rational prime, different from l and p.

All congruences are to mod q, unless the contrary is stated.

E is the exponent to which q belongs, mod l^n, so that

$$q^E \equiv 1 \pmod{l^n}.$$

Q is written for $(q^E-1)\,l^{-n}$.

---

* *Proc. London Math. Soc.*, Ser. 2, Vol. 6, First Paper, p. 16; Second Paper, p. 265. These are hereafter cited as "first paper" and "second paper."

F is defined by the following equations:—

when $l = 2$, $\qquad EF = 2^{n-2}$;

when $l \neq 2$, $\qquad EF = l^{n-1}(l-1)$.

ψ_g, where $g = 1, 2, \ldots, l^n - 2$, denotes the reciprocal factors of p, so called because of their property

$$\psi_g . \psi_g(\zeta^{-1}) = p.$$

In my first and second papers I have shewn how these reciprocal factors may be expressed in terms of π and its conjugates.

We know from Fermat's theorem that

$$q^{p-1} \equiv 1 \pmod{\pi},$$

and it follows from this that q^m, that is, $q^{(p-1)l^{-n}}$, is congruent, mod π, to some power of ζ. That power of ζ is denoted by $\{q/\pi\}_{l^n}$ or $\{q/\pi\}$, the suffix l^n being omitted when there can be no doubt which l^n is meant. In Parts I and II, $\{q/\pi\}$ means $\{q/\pi\}_8$; in Part III it means $\{q/\pi\}_{16}$; and in Part IV it means $\{q/\pi\}_9$.

When $\{q/\pi\} = 1$, then

$$q \equiv x^{l^n} \pmod{p};$$

and, conversely, $\{q/\pi\} = 1$ is the condition that q is the residue of the l^n-th power of some number, mod p.

If ν is composite, and its prime factors are $\pi, \pi', \ldots$, then $\{a/\nu\}$ is defined to mean $\{a/\pi\}\{a/\pi'\}\ldots$.

2. The general results proved in my first and second papers, which will be used in this paper, are as follows:—

$$\{q/\pi\}^q \equiv \psi_1 \psi_2 \ldots \psi_{q-1} \pmod{q}^*;$$

the law of reciprocity, namely,

$$\{q/\pi\} = \{\pi/q\},$$

where π is "primary" (in the sense defined in my papers) and, when $l = 2$, q is taken with such sign as to make

$$q \equiv 1 \pmod{4};^\dagger$$

---

* First paper, § 7; and second paper, § 19.

† First paper, § 19; second paper, § 23.

when $l = 2$, and $$q \not\equiv -1 \pmod{2^n},$$

$$\{\pi/q\} \equiv \Pi \pi_u^{Qr_{-u}} \pi_u^{\dagger -Qr_{-u}} \pmod{q} \quad (u = 0, 1, \ldots, F-1),$$

wherein r denotes 5 or some power of 5 chosen to satisfy

$$q \equiv \pm r^F \pmod{2^n}.$$

r_{-u} denotes the least positive residue of $r^{-u} \pmod{2^n}$,

π_u denotes $s^u\pi$, that is, $\pi(\zeta^{r^u})$,

s being the substitution which changes ζ into ζ^r, and $\pi_u^\dagger$ denotes $s^u t \pi$, that is, $\pi(\zeta^{-r^u})$,

t being the substitution which changes ζ into ζ^{-1};*

and lastly, when l is odd,

$$\{\pi/q\} \equiv \Pi \pi_u^{Qr_{-u}} \pmod{q} \quad (u = 0, 1, \ldots, F-1),$$

wherein r is a primitive root, mod l^n, chosen to satisfy

$$q \equiv r^F \pmod{l^n},$$

and π_u denotes $s^u\pi$, that is, $\pi(\zeta^{r^u})$,

s being the substitution which changes ζ into ζ^r.‡

3. In the first four parts of this paper, it is shewn how the general results mentioned in the previous paragraph may be simplified in the cases $l^n = 8$, 16, and 9, and how, for any given value of q, the value of $\{q/\pi\}$ may be calculated; and also the simplest expressions for $\{q/\pi\}$ are ascertained for certain small values of q. Some of these latter results have been enunciated by Bickmore§ and by Lt.-Col. A. Cunningham,‖ but it is believed that no proofs of them have hitherto been published.

In the paper just cited, Cunningham has also stated some other expressions for $\{q/\pi\}_8$, which he has discovered by induction from numerical results. In Parts V and VI the proofs of these expressions are obtained. I may refer to the first section of Part V for a general account of the subject-matter of Parts V and VI. In the theory of numbers important theorems have often (indeed, usually) been discovered by means of numerical instances, or, one may say, experimentally, and have afterwards been rigidly proved; while their existence would never have been suspected if the discoverer had not marshalled his columns of figures and observed the general law running through them. Cunningham's new expressions for $\{q/\pi\}_8$ form a remarkable instance of this tendency.

---

* Second paper, § 19; and below, § 15.

‡ First paper, § 5.

§ "On the Numerical Factors of a^n-1," *Messenger of Math.*, Vol. XXVI, p. 1.

‖ "On 8-vic, 16-ic, &c. Residuacity," *ante*, p. 1 of this volume.

PART I.

Criteria for the Value of $q^{\frac{1}{8}(p-1)} \pmod p$ *in Terms of the Prime Factors of* p *in the Field of* 8*-th Roots of* 1 *or of the Reciprocal Factors of* p *in that Field.*

4. It is convenient to begin with Gauss's law of quartic reciprocity for numbers in the field of 4-th roots of 1; this is included as a particular case in my second paper, Part II, and I shall deduce it from the general formulæ of §§ 19 and 23.

In the field of 4-th roots of 1, the primary prime factors of p are

$$\pi = a+b\iota \quad \text{and} \quad \pi^\dagger = a-b\iota,$$

where b is even, and $p = \pi\pi^\dagger = a^2+b^2$.

When $q = 4k+1$, $Q = \frac{1}{4}(q-1) = k$,

and so $\{q/\pi\}_4 = \{\pi/q\}_4 \equiv (\pi\pi^{\dagger -1})^k$.

And, when $q = 4k-1$, $Q = \frac{1}{4}(q^2-1) = k(q-1)$,

and $\pi' = (a+b\iota)' \equiv a+b\iota' \equiv \pi^\dagger$,

and then $\{-q/\pi\}_4 = \{\pi/q\}_4 \equiv \pi^Q$

$$\equiv (\pi\pi^{\dagger -1})^{-k};$$

if $(q/p) = 1$, $\{-q/\pi\}_4 = \pm 1$,

and then $\{-q/\pi\}_4 \equiv (\pi\pi^{\dagger -1})^k$.

And if $p = 8m+1$, $\{-q/\pi\}_4 = \{q/\pi\}_4$.

Assuming that $(q/p) = 1$ and $p = 8m+1$, we see that the two cases $q = 4k+1$ and $4k-1$ take the same form,

$$\{q/\pi\}_4 \equiv \left(\frac{a+b\iota}{a-b\iota}\right)^k.$$

5. The criterion for $\{q/\pi\}_4 = 1$ is now easily obtained for any given value of q. Let

$$(a+b\iota)^k = X+\iota X',$$

where X and X' are rational functions of a and b; then

$$(a-b\iota)^k = X-\iota X' \quad \text{and} \quad \{q/\pi\}_4 = 1$$

if, and only if, $X' \equiv 0$.

This is a congruence of degree k, and its solution gives as the criteria results of some of the forms

$$a \equiv 0, \qquad b \equiv 0, \qquad a \equiv \pm xb.$$

For all values of k, $b \equiv 0$ is one of the roots, and, when k is even, $a \equiv 0$ is also a root. Then $p = a^2+b^2 \equiv b^2$, a^2, or $(1+x^2)b^2$ respectively. Cunningham has calculated these criteria for all values of q up to 50.*

6. We now take the field of 8-th roots of 1; the notation to be used will be that of my second paper, § 29, namely,

$$\pi = a_0+a_1\xi+a_2\xi^2+a_3\xi^3,$$
$$\omega = \xi+\xi^3 = \sqrt{(-2)},$$
$$p = c^2+2d^2 = (c+d\omega)(c-d\omega),$$

s is here the substitution $(\xi : \xi^5)$, and t is $(\xi : \xi^{-1})$.

The values of the reciprocal factors in this field are given in my second paper, § 29, whence we obtain

$$\psi_1\psi_2 = (-1)^m(a-b\iota)(c-d\omega),$$
$$\psi_3\psi_4 = (-1)^m(c-d\omega)^2,$$
$$\psi_5\psi_6 = (-1)^m(a-b\iota)(c-d\omega),$$
$$\psi_7\psi_8 = (-1)^m p.$$

Also $$\psi_{x+8y} = \psi_x.$$

It should be remembered that the numbers $a+b\iota$ and $c+d\omega$ are defined in terms of π, which is a given primary prime factor of p in the field. It follows from this definition that $a \equiv c \pmod 4$; a and c are therefore not necessarily positive, but possess such sign as to satisfy this congruence. In order to fix the sign, I take

$$a \equiv c \equiv 1 \pmod 4.$$

Then, using the formula of the second paper, § 19,

$$\{q/\pi\}^q \equiv \psi_1 \dots \psi_{q-1},$$

and operating on it with st when $q \equiv 3 \pmod 8$, with s when $q \equiv 5 \pmod 8$, and with t when $q \equiv 7 \pmod 8$, we obtain

when $q \equiv 1 \pmod 8$, $\quad \{q/\pi\} \equiv p^{\frac{1}{8}(q-1)}(a-b\iota)^{\frac{1}{4}(q-1)}(c-d\omega)^{\frac{1}{4}(q-1)}$,

when $q \equiv 3 \pmod 8$, $\quad \{-q/\pi\} \equiv p^{\frac{1}{8}(q-3)}(a+b\iota)^{\frac{1}{4}(q+1)}(c-d\omega)^{\frac{1}{4}(q-1)}$,

when $q \equiv 5 \pmod 8$, $\quad \{q/\pi\} \equiv p^{\frac{1}{8}(q-5)}(a-b\iota)^{\frac{1}{4}(q-1)}(c+d\omega)^{\frac{1}{4}(q+1)}$,

when $q \equiv 7 \pmod 8$, $\quad \{-q/\pi\} \equiv p^{\frac{1}{8}(q-7)}(a+b\iota)^{\frac{1}{4}(q+1)}(c+d\omega)^{\frac{1}{4}(q+1)}$.

* Unpublished.

In the particular cases of $\{q/\pi\} = \pm 1$, the signs of ι and ω in these congruences are immaterial, for the substitutions s and t can be applied without altering $\{q/\pi\}$.

Assuming that $\{q/\pi\} = \pm 1$, we have, from § 5, $X' \equiv 0$, and so

$$(a+b\iota)^k \equiv X.$$

Writing k' for the index of $c+d\omega$, viz., $\frac{1}{2}(q-1)$ or $\frac{1}{2}(q+1)$, we have

$$(c+d\omega)^{k'} \equiv Y+Y'\omega,$$

where Y and Y' are functions of c and d.

Then, since $\{q/\pi\} \equiv \pm 1$, $Y' \equiv 0$, which gives as one root $d \equiv 0$; and, when k' is even, $c \equiv 0$ is another root; and the other roots are of the form

$$c \equiv \pm yd.$$

Then $p = c^2+2d^2 \equiv c^2,\ 2d^2,\ (2+y^2)d^2$ respectively.

Finally,

$$\{\pm q/\pi\} \equiv p^j XY,$$

where j is the index of p in the above congruences; and this is readily simplified for any given value of q, taking in turn the different roots of $X' \equiv 0$ and $Y' \equiv 0$.

I give the full results for $q = 3$ and 5, and the values of $\{q/\pi\}_8$, supposing that $\{q/\pi\}_4 = 1$, for $q = 7$, 11, and 13.

7. *The case* $q = 3$. Since $p = a^2+b^2 = c^2+2d^2$, when $p \equiv 1$, either a or $b \equiv 0$, and $d \equiv 0$; when $p \equiv -1$, $a \equiv \pm b$, and $c \equiv 0$. We then obtain, from the results of the previous paragraph:—

(i) When $p \equiv 1$ and $b \equiv 0$, $\{3/\pi\} \equiv (-1)^m ac$,

(ii) When $p \equiv 1$ and $a \equiv 0$, $\{3/\pi\} \equiv (-1)^m bc\iota$,

(iii) When $p \equiv -1$ and $a \equiv -b$, $\{3/\pi\} \equiv (-1)^m ad\zeta$,

(iv) When $p \equiv -1$ and $a \equiv b$, $\{3/\pi\} \equiv (-1)^m ad\zeta^3$.

The first of these results was discovered by Bickmore* by means of numerical induction, and it can be easily identified with Cunningham's criterion.† For, if his $a \equiv 0 \pmod 2$, my $a \equiv 1 \pmod 3$, and if his $a \equiv 1 \pmod 2$, my $a \equiv -1 \pmod 3$; that is, $a \equiv (-1)^\alpha \pmod 3$, and similarly $c \equiv (-1)^\gamma \pmod 3$; and so in case (i), when $\{3/\pi\}_4 = 1$,

$$\{3/\pi\} = (-1)^{m+\alpha+\gamma},$$

which is Cunningham's criterion.

---

* *Messenger of Math.*, Vol. XXVI, p. 15.

† *Ante*, p. 10 of this volume.

8. *The case* $q = 5$.

(i) When $p \equiv \pm 1$ and $b \equiv 0$,

(1) if $d \equiv 0$, $\{5/\pi\} \equiv pac$,

(2) if $d \equiv \pm 2c$, $\{5/\pi\} \equiv -2pac$.

(ii) When $p \equiv \pm 1$ and $a \equiv 0$,

(1) if $d \equiv 0$, $\{5/\pi\} \equiv -pbc\iota$,

(2) if $d \equiv \pm 2c$, $\{5/\pi\} \equiv 2pbc\iota$.

(iii) When $p \equiv \pm 2$ and $a \equiv b$,

(1) if $c \equiv 0$, $\{5/\pi\} \equiv -2pad\xi$,

(2) if $d \equiv \pm c$, $\{5/\pi\} \equiv -pad\xi$.

(iv) When $p \equiv \pm 2$ and $a \equiv -b$,

(1) if $c \equiv 0$, $\{5/\pi\} \equiv -2pad\xi^3$.

(2) if $d \equiv \pm c$, $\{5/\pi\} \equiv -pad\xi^3$.

The results of case (i) are due to Jacobi.* In order to deduce Cunningham's criterion from them, we need only the following:—

When $p \equiv 1$, $a \equiv (-1)^\alpha$, and $c \equiv (-1)^\gamma$ or $2(-1)^\gamma$, according as $d \equiv 0$ or not.

And, when $p \equiv -1$, $a \equiv 2(-1)^\alpha$; and $c \equiv 2(-1)^\gamma$ or $-(-1)^\gamma$, according as $d \equiv 0$ or not.

9. *The case* $q = 7$.

Assuming that $\{7/\pi\}_4 = 1$,

when $b \equiv 0$ and c or $d \equiv 0$, $\{7/\pi\} = (-1)^m$,

when $b \equiv 0$ and $c \equiv \pm 3d$, $\{7/\pi\} = (-1)^{m+1}$,

when $a \equiv 0$ and c or $d \equiv 0$, $\{7/\pi\} = (-1)^{m+1}$,

when $a \equiv 0$ and $c \equiv \pm 3d$, $\{7/\pi\} = (-1)^m$.

Cunningham's definition of α and γ in this case amount to this, that $\alpha \equiv 0 \pmod 2$ when $b \equiv 0$, and $\alpha \equiv 1 \pmod 2$ when $a \equiv 0$; that $\gamma \equiv 0 \pmod 2$ when $d \equiv 0$, and $\gamma \equiv 1 \pmod 2$ when $c \equiv \pm 3d$.

* Bickmore, *loc. cit.*, p. 15.

10. *The case* $q = 11$.

Assuming that $\{11/\pi\}_4 = 1$, and introducing for brevity the definition that $\kappa = 0$, when $d \equiv 0$ or $\pm c$, and $\kappa = 1$, when $d \equiv \pm 2c$, we obtain

$$\{11/\pi\} \equiv (-1)^{m+\kappa}(ac/11).$$

In this case, Cunningham's definitions of α and γ are, that

$$(-1)^{\alpha} = (a/11) \quad \text{and} \quad (-1)^{\gamma} = (c/11).$$

11. *The case* $q = 13$.

Assuming that $\{13/\pi\}_4 = 1$, $\{13/\pi\} = 1$ when

$$a \equiv c, \ -2c, \ -3c, \ -5c, \ 6c;$$

also, when $b \equiv 0$ and $a \equiv 4c$, and when $b \equiv \pm 4a$ and $a \equiv -4c$. And, if any of these congruences are true with the sign of c changed, then

$$\{13/\pi\} = -1.$$

12. From the value of $\{1+\iota/\pi\}_4$, one of the so-called supplementary laws in the field of 4-th roots of 1,* the value of $\{2/\pi\}$ may be easily deduced. For $2 = -\iota(1+\iota)^2$ and $b \equiv 0 \pmod 4$, and so

$$\begin{aligned}\{2/\pi\} &= \iota^{-m}\{1+\iota/\pi\}_4 \\ &= \iota^{-m+\frac{1}{2}(a-b-1)}.\end{aligned}$$

If $b \equiv 0 \pmod 8$, then $a \equiv 1-4m \pmod{16}$, and so

$$\{2/\pi\} = (-1)^{m+\frac{1}{8}b}.$$

And, if $b \equiv 4 \pmod 8$, then $a \equiv 1-4(m+2) \pmod{16}$, and so

$$\{2/\pi\} = \iota^{2m+2-\frac{1}{2}b}.$$

The former of these expressions for $\{2/\pi\}$ was stated by Reuschle, in 1856, in a slightly different form; he discovered it by induction from numerical instances.† It is remarkable that the proof of the criterion for $\{2/\pi\}$ should now be published apparently for the first time.

13. Combining the value of $\{2/\pi\}$ with that of $\{q/\pi\}$, we can easily find the value of $\{2q/\pi\}$, or, in particular, a criterion to decide whether it is ± 1. The results stated by Bickmore for $\{6/\pi\}$ and $\{10/\pi\}$ are thus

* Gauss, "Theoria Residuorum Biquad.," Comm. II (1831), *Werke*, Bd. II; and H. J. S. Smith, "Report on the Theory of Numbers," *Collected Papers*, Vol. I, p. 77.

† A. Cunningham, *Proc. London Math. Soc.*, Ser. 1, Vol. XXVII, p. 88.

verified. Similarly criteria may be derived for $\{qq'/\pi\}$, q and q' being different primes. Thus $\{15/\pi\} = 1$, when

$$\{3/\pi\} = \zeta^n, \qquad \{5/\pi\} = \zeta^{-n} \quad (n = 0, 1, \ldots, 7);$$

but the combinations of the different cases are too numerous to be set out. For any given value of π, it is simpler to calculate $\{q/\pi\}$ and $\{q'/\pi\}$ separately.

14. So far, the value of $\{q/\pi\}$ has been expressed in terms of the reciprocal factors of p, that is, $a+bi$ and $c+d\omega$. These expressions are convenient for numerical calculations, because there are extensive tables of a, b, c, and d.* Criteria for $\{q/\pi\}$ may, however, be also obtained in terms of π itself. For, if n be any prime or power of a prime, the law of reciprocity shews that the residues of π (mod q) are divisible into n sets, one of which contains the values of π such that $\{q/\pi\}_n = 1$, and the other $n-1$ of which correspond to the other values of $\{q/\pi\}_n$. A table, which for given values of n and q gives those residues of π (mod q) making $\{q/\pi\}_n = 1$ or any given power of ζ, would be a theoretically complete solution of the question. Legendre has given such a table as this for quadratic residues for all values of q not divisible by a square up to 79.† But in most of the cases considered in this paper, such a table would be of great size, and it must therefore suffice to state the conditions which π must satisfy in a more condensed form.

15. It should be observed that the expressions for $\{\nu/q\}$ given in my second paper, § 19, are not in general unique; when $q \equiv -1 \pmod 4$, but not $\equiv -1 \pmod{2^n}$, the factorising group§ of q, that is, the group of operations leaving $\mathfrak{q}$ (a prime factor of q) unaltered, is $\{s^F t\}$; consequently $s^F\mathfrak{q} = t\mathfrak{q}$, and the conjugates of $\mathfrak{q}$ may be written in the form

$$\mathfrak{q}_u = s^u\mathfrak{q} \quad \text{and} \quad \mathfrak{q}'_u = s^u t\mathfrak{q} \quad (u = 0, 1, \ldots, F-1).$$

In this case we obtain for $\{\nu/q\}$ the same expression as when $q \equiv 1 \pmod 4$,‖ and this will be found to be the best expression in practice. This argument does not hold when $q \equiv -1 \pmod{2^n}$, as then the factorising group is $\{t\}$.

---

* A. Cunningham, *Quadratic Partitions*, London, 1904.

† *Théorie des Nombres*, 3rd edition, Table III.

§ German, *Zerlegungsgruppe*.

‖ This is given in § 2 above.

The case $q = 3$.

Here $Q = \frac{1}{8}(3^2-1) = 1$, and

$$\{-3/\pi\} \equiv \pi\pi^{\dagger -1}.$$

Then $\{-3/\pi\} = 1$, if $\pi \equiv \pi^{\dagger}$,

which gives $a_2 \equiv 0$,

$$a_1+a_3 \equiv 0.$$

The case $q = 5$.

Here $Q = \frac{1}{8}(5^2-1) = 3$, and

$$\{5/\pi\} \equiv (\pi\pi^{\dagger -1})^3.$$

The solutions of $\kappa^3 \equiv 1$ are

$$\kappa \equiv 1,\ 2+\omega,\ 2-\omega.$$

Therefore, if $\{5/\pi\} = 1$,

$$\pi\pi^{\dagger -1} \equiv 1,\ 2+\omega,\ \text{or}\ 2-\omega \pmod{1+2\iota}.$$

The application of t shews that each of these congruences is true mod $1-2\iota$, so we get

$$\pi^{\dagger} \equiv \pi,\ (2+\omega)\pi \text{ or } (2-\omega)\pi;$$

and, conversely, each of these gives $\{5/\pi\} = 1$.

If $\pi^{\dagger} \equiv \pi$, then $a_2 \equiv 0$, $a_1+a_3 \equiv 0$.

If $\pi^{\dagger} \equiv (2+\omega)\pi$, then $a_0 \equiv a_1+a_3$, $2a_2 \equiv a_1-a_3$.

If $\pi^{\dagger} \equiv (2-\omega)\pi$, then $-a_0 \equiv a_1+a_3$, $-2a_2 \equiv a_1-a_3$.

The connection between these results and the criterion given before is as follows.

$$\{5/\pi\} \equiv \left(\frac{\pi}{\pi^{\dagger}}\right)^3 \equiv \frac{\pi_1\pi^{\dagger 2}}{\pi_1^{\dagger}\pi^2} \equiv \frac{\pi^{\dagger}}{\pi}\ \frac{c-d\omega}{c+d\omega};$$

so, assuming that $\{5/\pi\} = 1$,

when $\pi^{\dagger} \equiv \pi$, $d \equiv 0$,

when $\pi^{\dagger} \equiv (2+\omega)\pi$, $d \equiv 2c$,

when $\pi^{\dagger} \equiv (2-\omega)\pi$, $d \equiv -2c$.

In the first case, we get $a \equiv a_0^2-2a_1^2 \equiv c$.

In the other two cases, we get

$$a \equiv -a_0^2+2a_2^2 \equiv -2c.$$

PART II.

Criteria for the Value of $q^{\frac{1}{8}(p-1)} \pmod p$, *in Terms of* $a, b,$ *and* e, f.

16. Besides the two reciprocal factors of p in the field of 8-th roots of 1, which are defined in my second paper, § 29, there is one other way of pairing the conjugate prime factors of p, namely,

$$\pi\pi^\dagger = e+f\varpi,$$

where $\varpi = \zeta+\zeta^{-1}$ and $\varpi^2 = 2$.

We then have $p = e^2-2f^2$,

and $e = a_0^2+a_1^2+a_2^2+a_3^2$,

$$f = a_0a_1+a_1a_2+a_2a_3-a_3a_0.$$

As is well known, there is a singly infinite set of values of e, f, satisfying $p = e^2-2f^2$, which correspond to the set of prime factors of p, $\epsilon^x\pi$, ϵ being the fundamental unit $1+\varpi$. Assuming that π is canonical [*i.e.*, that $\pi \equiv 1 \pmod 2$], so also is $\epsilon^{2x}\pi$, for $\epsilon^2 = 3+2\varpi \equiv 1 \pmod 2$; and therefore for the present purpose we need only consider the e and f formed from π, and from $\pi' = \epsilon\pi$. Let

$$e'+f'\varpi = \pi'\pi'^\dagger = \epsilon^2(e+f\varpi);$$

then we find $e \equiv 1 \pmod 4$, and $f \equiv a_1+a_3 \equiv d \pmod 4$;

also $e' \equiv -1 \pmod 4$, and $f' \equiv d+2 \pmod 4$.

17. The formulæ for $\{q/\pi\}$ of § 6 can be transformed so as to eliminate $c \pm d\omega$, and to introduce $e \pm f\varpi$. First, let $q = 8x+1$; then since

$$a-b\iota = \pi^\dagger\pi_1^\dagger, \quad \text{and} \quad c-d\omega = \pi_1\pi^\dagger,$$

$$\begin{aligned}\{q/\pi\} &\equiv p^x(a-b\iota)^{2x}(c-d\omega)^{4x}\\ &\equiv p^x\pi^{\dagger 6x}\pi_1^{4x}\pi_1^{\dagger 2x}\\ &\equiv p^{-x}\pi^{2x}\pi^{\dagger 8x}\pi_1^{6x}\pi_1^{\dagger 4x},\end{aligned}$$

but $\pi^{\dagger 8x} = \pi^{\dagger q-1} \equiv 1$,

so $\{q/\pi\} \equiv p^{-x}\pi^{2x}\pi_1^{6x}\pi_1^{\dagger 4x}$

$$\equiv p^{-x}(a+b\iota)^{2x}(e-f\varpi)^{4x},$$

In a similar way we find

when $q = 8x+3$, $\{-q/\pi\} \equiv p^{-x-1}(a-b\iota)^{2x+1}(e+f\varpi)^{4x+2}$,

when $q = 8x+5$, $\{\ \ q/\pi\} \equiv p^{-x-1}(a+b\iota)^{2x+1}(e+f\varpi)^{4x+3}$,

when $q = 8x+7$, $\{-q/\pi\} \equiv p^{-x-1}(a-b\iota)^{2x+2}(e-f\varpi)^{4x+3}$.

If $q \equiv \pm 1 \pmod 8$, $\epsilon^{q-1} \equiv 1$,

and if $q \equiv \pm 3 \pmod 8$, $\epsilon^q \equiv \epsilon_1$, and $\epsilon^{q+1} \equiv -1$.

When therefore $\{\pm q/\pi\}$ is expressed in terms of $e' \pm f'\varpi$, the above formulæ remain true when $q \equiv \pm 1 \pmod 8$, but the sign of the right side is changed when $q = \pm 3 \pmod 8$.

These formulæ may now be reduced for any given value of q, and thus criteria for $\{q/\pi\}$ may be found in terms of a, b, and e, f. In the rest of this Part, it is assumed that $\{q/\pi\}_4 = 1$.

18. *The case* $q = 3$.

When $f \equiv 0$, $\{-3/\pi\} \equiv a$;

when $e \equiv 0$, $\{-3/\pi\} \equiv -a$.

The case $q = 5$.

When $f \equiv 0$, $\{5/\pi\} \equiv ae$;

when $e \equiv \pm f$, $\{5/\pi\} \equiv -2ae$.

The case $q = 7$.

When $b \equiv 0$ and $f \equiv 0$, $\{-7/\pi\} = (e/7)$,

when $b \equiv 0$ and $e \equiv \pm 2f$, $\{-7/\pi\} = -(e/7)$,

when $a \equiv 0$ and $f \equiv 0$, $\{-7/\pi\} = -(e/7)$,

when $a \equiv 0$ and $e \equiv \pm 2f$, $\{-7/\pi\} = (e/7)$.

The case $q = 11$.

When $f \equiv 0$ or $f \equiv \pm 2e$, $\{-11/\pi\} = (a/11)$,

when $e \equiv 0$ or $f \equiv \pm 3e$, $\{-11/\pi\} = -(a/11)$.

I have verified Cunningham's criteria in these cases, and find them correct both for e, f, and for e', f'.

PART III.

Criteria for 3 or 5 being a Residue of a 16-th Power.

19. As might be expected, the evaluation of $\{q/\pi\}_{16}$ is more troublesome than that of $\{q/\pi\}_8$, and, except when $q = 3$, the only practicable method seems to be that already employed in §§ 14 and 15.

In this part the notation is the same as in Part III of my second paper; π is assumed to be primary; by the use of the tables of primary residues given there, any prime factor of p can be made primary by multiplying it by a suitable power of ζ. It is assumed that

$$\{q/\pi\}_8 = 1, \quad \text{so that} \quad \{q/\pi\} = \pm 1.$$

20. *The case* $q = 3$.

Using the general formula of § 19 of my second paper, and substituting in it the values of ψ_1 and ψ_2 given in Part III of that paper, we find

$$\{3/\pi\}^3 \equiv (-1)^m t\Phi_1 . t\Phi_2;$$

or, since we suppose $\{3/\pi\}$ to be ± 1,

$$\{-3/\pi\} \equiv \Phi_1\Phi_2.$$

Now $$\Phi_1 . t\Phi_1 = p \equiv 1,$$

so $$\Phi_2 \equiv \{-3/\pi\}\, t\Phi_1,$$

that is, Φ_2 (mod 3) belongs to the sub-field $(\omega_1, \omega_2, \omega_3)$; and therefore

$$d_4 \equiv 0, \quad d_2 \equiv -d_6, \quad d_3 \equiv d_5, \quad d_1 \equiv d_7,$$

and $$\Phi_2 \equiv d_0 + d_1\omega_1 + d_2\omega_2 + d_3\omega_3.$$

Therefore $$\{-3/\pi\} \equiv \frac{d_0}{c_0} \equiv -\frac{d_1}{c_1} \equiv \frac{d_2}{c_2} \equiv -\frac{d_3}{c_3}.$$

It may be proved that $c_0 \not\equiv 0$, and so we find that

$$\{-3/\pi\} \equiv c_0 d_0, \quad \text{and} \quad \{3/\pi\} \equiv (-1)^m c_0 d_0.$$

21. A criterion for $\{3/\pi\}$ may also be found in terms of π. The prime factors of 3 are $1-\omega$ and $1+\omega$, and its factorising group is $\{st\}$; also

$$Q = \tfrac{1}{16}(3^4-1) = 5,$$

and so $$\{-3/\pi\} \equiv (\pi\pi'^{-1})^5.$$

The norm of $1-\omega$ is 3^4, and so the number of incongruent residues of π prime to 3 is $(3^4-1)^2$, and the number of residues of π satisfying $\{-3/\pi\} = 1$ is one-sixteenth of this number, *i.e.*, 400.

Any residue of $1-\omega$ may be written in the form

$$\lambda \equiv x+y\omega_1+z\omega_2+w\omega_3 \pmod{1-\omega}.$$

Since s^2t leaves λ unaltered, and changes $1-\omega$ into $1+\omega$, we see that any congruence (mod $1-\omega$) in the field $(\omega_1, \omega_2, \omega_3)$ is also true mod 3.

If $\{-3/\pi\} = 1$, we must have

$$\pi' \equiv \lambda\pi \pmod{1-\omega},$$

where λ satisfies

$$\lambda^5 \equiv 1 \pmod 3.$$

Now κ being any number of the field $k(\xi)$,

$$\kappa^3 \equiv \kappa(\xi^3) \equiv \kappa_3';$$

therefore $\lambda^3 \equiv \lambda_3' \equiv \lambda_1$, $\lambda^4 \equiv \lambda_2$, $\lambda\lambda_2 \equiv 1$, $\lambda^2 \equiv \lambda_3$,

and the roots of $\lambda^5 \equiv 1$ are

$$1, \quad \lambda, \quad \lambda_1, \quad \lambda_2, \quad \lambda_3.$$

By trial, values of x, y, z, and w are found which satisfy $\lambda^2 \equiv \lambda_3$, and thus we get

$$\lambda \equiv -1-\omega_1-\omega_2+\omega_3.$$

Now, since

$$\pi' \equiv \lambda\pi \pmod{1-\omega},$$

applying t,

$$\pi \equiv \lambda_2\pi' \pmod{1+\omega},$$

that is,

$$\pi' \equiv \lambda_2^{-1}\pi \equiv \lambda\pi \pmod{1+\omega},$$

and therefore

$$\pi' \equiv \lambda\pi \pmod 3.$$

Therefore the complete solution of $\{-3/\pi\} = 1$ is

$$\pi' \equiv \pi, \quad \lambda\pi, \quad \lambda_1\pi, \quad \lambda_2\pi, \quad \text{or} \quad \lambda_3\pi \pmod 3;$$

and when $m \equiv 1 \pmod 2$, $\{3/\pi\} = -\{-3/\pi\}$,

and then the solution of $\{3/\pi\} = 1$ is

$$-\pi' \equiv \pi, \quad \lambda\pi, \quad \lambda_1\pi, \quad \lambda_2\pi, \quad \text{or} \quad \lambda_3\pi.$$

Each value of $\pi\pi'^{-1}$ corresponds to 3^4-1 values of π; for instance, $\pi \equiv \pi'$ gives

$$\pi \equiv b_0+b_1\varpi_1+b_2\varpi_2+b_3\varpi_3,$$

where b_0, b_1, ... may have any values.

22. Yet another criterion for $\{-3/\pi\}$ may be derived from the results of the last paragraph; for, if

$$\pi^{\dagger} \equiv \lambda^{x}\pi,$$

then $$\Phi_2 \equiv \pi\pi_1\pi_2\pi_3\lambda_1^{x},$$

but $$\pi\pi_1\pi_2\pi_3 = a+b\iota \equiv a,$$

so $$\Phi_2 \equiv a\lambda^{3x};$$

and conversely, if $\Phi_2 \equiv a\lambda^{u}$, and $\{3/\pi\}_4 = 1$,

then $$\pi^{\dagger} \equiv \lambda^{2u}\pi,$$

and so $$\{-3/\pi\} = 1;$$

and if $\Phi_2 \equiv -a\lambda^{u}$, $\{-3/\pi\} = -1$.

23. *The case* $q = 5$.

Here $$Q = \tfrac{1}{16}(5^4-1) = 39,$$

and $$\{5/\pi\} \equiv (\pi\pi^{\dagger -1})^{39}.$$

As in the case of $q = 3$, any residue mod $1+2\iota$ may be written in the form

$$x+y\omega_1+z\omega_2+w\omega_3,$$

and it only remains to find the solutions of

$$\kappa^{39} \equiv 1.$$

Now, if $\lambda^{13} \equiv 1$, and $\mu^3 \equiv 1$,

$$\kappa \equiv \lambda^{x}\mu^{y} \quad (x = 0, \ldots, 12;\ y = 0, 1, 2).$$

Then $\lambda^5 \equiv \lambda_1$, $\lambda^{25} \equiv \lambda_2$, $\lambda^{125} \equiv \lambda_3$,

and so $\lambda\lambda_2 \equiv 1$, and $\lambda^3 \equiv \lambda_3^2$.

A value of λ satisfying the latter congruence is found by trial to be

$$\lambda \equiv 1+\omega_1-2\omega_2,$$

whence $$\lambda^2 \equiv 2+\omega_1+2\omega_2+\omega_3,$$

and $$\lambda^4 \equiv -2-\omega_1+\omega_2+2\omega_3;$$

and the other roots, besides 1, are λ_u, λ_u^2, λ_u^4 $(u = 1, 2, 3)$.

We have seen in § 15 that a root of $\mu^3 \equiv 1$ is $2+\omega$; for the present purpose it is better to take μ in the same field as λ, and we find

$$\mu \equiv 1, \quad 2+2\omega_2, \quad 2-2\omega_2.$$

Finally, as in the case of $q = 3$, we find that

$$\{5/\pi\} = 1,$$

when $$\pi' \equiv \lambda^x \mu^y \pi.$$

Also, as before, $$\{5/\pi\} = 1,$$

when $$\Phi_2 \equiv a\lambda^x\mu^y, \quad \text{and} \quad \{5/\pi\}_4 = 1,$$

and $$\{5/\pi\} = -1,$$

when $$\Phi_2 \equiv -a\lambda^x\mu^y, \quad \text{and} \quad \{5/\pi\}_4 = 1.$$

The curious result follows from this, that whenever $\{5/\pi\}_8 = 1$, $\Phi_2 \pmod 5$ belongs to the sub-field $(\omega_1, \omega_2, \omega_3)$.

24. Throughout this part, it should be observed that $a+b\iota$, Φ_1 and Φ_2 are defined as products of π and its conjugates; for instance,

$$a+b\iota = \pi\pi_1\pi_2\pi_3.$$

The result of substituting $\epsilon_1\pi$ for π in any of these products is to multiply it by the norm of ϵ_1 in the field of $k(\zeta+\zeta^{-1})$, that is, by -1. Accordingly if π is in one of the eight primary forms $\{\epsilon_1^2, \epsilon_3, \gamma\}$,* we have

$$a \equiv 1 \pmod 8, \quad c_0 \equiv 1 \pmod 8, \quad \text{and} \quad d_0 \equiv 1+\tfrac{1}{2}b \pmod 4,$$

as in §§ 32 and 33 of my second paper; but if π is in one of the other eight primary forms,* then

$$a \equiv -1 \pmod 8, \quad c_0 \equiv -1 \pmod 8, \quad \text{and} \quad d_0 \equiv -1-\tfrac{1}{2}b \pmod 4.$$

It will be seen that the only formulæ of this part that are affected by this are those of the last two sections containing Φ_2.

* Tables of these are given in my second paper, §§ 31 and 36.

PART IV.

Criteria for 2 or 5 being a Residue of a 9-th Power.

25. In this part, the notation is the same as in Part IV of my second paper. It is assumed that π is primary, and that $\{q/\pi\}_3 = 1$, so that $\{q/\pi\} = 1$, ρ, or ρ^2.

The case $q = 2$.

As before, the general formulæ of my second paper give

$$\{2/\pi\} \equiv \phi,$$

and also

$$\{2/\pi\} \equiv \pi_3 \pi^{-1}.$$

We infer that for every π, $\quad \phi \equiv \xi^x \pmod 2$.

The condition that $\{2/\pi\}_3 = 1$ is $a' \equiv 0$, and hence the interesting connection between $\pi^* = a + a'\rho$ and ϕ, namely, that when $a' \equiv 0$, then

$$c_1 \equiv c_2 \equiv c_7 \equiv c_8 \equiv 0.$$

We also see that the criterion for $\{2/\pi\} = 1$ is that

$$c_3 \equiv 0,$$

or that

$$\pi \equiv \pi_3.$$

The latter criterion gives

$$b_3 \equiv 0, \quad b_1 \equiv b_8, \quad b_2 \equiv b_7,$$

and so

$$\pi \equiv b_0 + b_1(\xi + \xi^{-1}) + b_2(\xi^2 + \xi^{-2}).$$

26. *The case* $q = 5$.

5 is a prime in the field of 9-th roots of 1.

$\pi^* = \pi\pi_2\pi_4 = a + a'\rho$ being a factor of p in the field of third roots of 1, the condition that $\{5/\pi\}_3 = 1$ is known to be :—

when $p \equiv \pm 1$, $\quad \pi^* \equiv \pi_1^*$, that is, $a' \equiv 0$;

when $p \equiv \pm 2$, $\quad \pi^* \equiv -\pi_1^*$, that is, $2a - a' \equiv 0$.

Now $\pi^5 \equiv \pi_5$, $\quad \pi^{5^2} \equiv \pi_4$, and generally $\pi^5 \equiv \pi_{6-n}$,

and so from $$\pi^* \equiv \pm \pi_1^*,$$

that is, $$\pi\pi_2\pi_4 \equiv \pm \pi_1\pi_3\pi_5,$$

we deduce $$\pi^{5^4+5^2+1} \equiv \pm \pi_3^{5^4+5^2+1}.$$

The reciprocity law gives at once

$$\{5/\pi\} = \{\pi/5\} \equiv \pi^{\frac{1}{8}(5^6-1)}$$
$$\equiv \pi^{14(5^3-1)}$$
$$\equiv (\pi_3\pi^{-1})^{14}.$$

So if $\{5/\pi\} = 1$, $$\pi^{14} \equiv \pi_3^{14}.$$

Since $$5^4+5^2+1 = 3.7.31,$$

we find that when $p \equiv \pm 1$, $\{5/\pi\} = 1$, when $\pi^7 \equiv \pi_3^7$,

and that when $p \equiv \pm 2$, $\{5/\pi\} = 1$, when $\pi^7 \equiv -\pi_3^7$.

We have now only to solve $\lambda^7 \equiv 1$.

The simplest equivalent congruence is $\lambda^2 \equiv \lambda_2$, and this can be solved by trial. The table at the end of this part gives the six solutions of $\lambda^7 \equiv 1$ other than 1.

As in Part III, the criterion for $\{5/\pi\} = 1$ may be expressed in terms of the reciprocal factor

$$\phi = \pi\pi_1\pi_2.$$

First, when $p \equiv \pm 1$, $$\pi^* \equiv a,$$

that is, $$\pi_4\phi \equiv a\pi_1,$$

and so $$\phi \equiv a\lambda_x.$$

Secondly, when $p \equiv \pm 2$, $$\pi^* \equiv -\pi_1^*,$$

that is, $$\pi_4^2\phi \equiv -\pi_1^2\phi_3,$$

or $$\pi_4^2\phi^2 \equiv -\pi_1^2 p.$$

Now in this case

$$p \equiv -2a^2 \quad \text{and} \quad (1+2\rho)^2 \equiv 2,$$

and so $$\phi \equiv \pm(1+2\rho)\,a\lambda_x.$$

The Solutions of $\lambda^7 \equiv 1 \pmod 5$.

	1	ζ	ζ^2	ζ^3	ζ^7	ζ^8
λ	2	1	−1	1	−2	0
$\lambda_1 \equiv \lambda^3$	1	1	−2	−1	1	2
$\lambda_2 \equiv \lambda^2$	2	2	0	1	−1	−1
$\lambda_3 \equiv \lambda^6$	1	0	−2	−1	−1	1
$\lambda_4 \equiv \lambda^4$	2	2	1	1	−2	1
$\lambda_5 \equiv \lambda^5$	1	−1	−1	−1	0	2

PART V.

The Quartic Field $k(\omega, \theta)$, *where*

$$\omega = \sqrt{(-2)}, \quad \textit{and} \quad \theta = \tfrac{1}{2}\{-1+\sqrt{[(-1)^{\frac{1}{2}(q-1)}q]}\}.$$

27. Col. A. Cunningham has given in his paper* expressions for $\{q/\pi\}_8$ in terms of a, b, t, u, t', u', where

$$p = a^2+b^2 = t^2+qu^2 = t'^2-qu'^2,$$

and it is assumed that $\{q/\pi\} = 1$. When $q = 11$,

$$p = \tfrac{1}{4}(t^2+11u^2).$$

The object of Parts V and VI of this paper is to furnish proofs of these expressions. As $\{q/\pi\}$ has already been expressed in terms of a, b and c, d, these new results depend on certain congruences between a, b, c, d, t, u, t', u'. These congruences will be proved by the use of certain quartic fields of algebraic numbers, containing as sub-fields two or three of the quadratic fields $k(\iota)$, $k[\sqrt{(-2)}]$, $k(\sqrt{q})$, $k[\sqrt{(-q)}]$. Quartic fields containing a quadratic field have been studied by Hilbert† and Sommer,‡ and are called by Hilbert "Dirichlet's Biquadratic Fields," because Dirichlet was the first to investigate the theory of binary quadratic forms whose coefficients and variables belong to the field $k(\iota)$.

28. In this part I deal with the quartic field which contains $\omega = \sqrt{(-2)}$, and $\sqrt{(eq)}$, where $e = (-1)^{\frac{1}{2}(q-1)}$. A basis of the quadratic field defined

* *Ante*, p. 10 of this volume.

† *Bericht, Deutschen Math. Verein*, Bd. 4, 1897, § 87; and *Math. Annalen*, Bd. 45, p. 309.

‡ *Vorlesungen über Zahlentheorie*, 1907.

by ω is $(1, \omega)$, and its discriminant is 8; a basis of the quadratic field defined by $\sqrt{(eq)}$ is $(1, \theta)$, where

$$\theta = \tfrac{1}{2}[-1+\sqrt{(eq)}],$$

and its discriminant is eq.

I therefore call this quartic field $k(\omega, \theta)$.

Since these discriminants are prime to each other, the discriminant of $k(\omega, \theta)$ is 2^6q^2,* and a basis is

$$(1, \omega, \theta, \omega\theta).$$

Therefore every integer of $k(\omega, \theta)$ is of the form

$$d_0+d_1\omega+d_2\theta+d_3\omega\theta,$$

where d_0, d_1, d_2, d_3 are rational integers.

The field $k(\omega, \theta)$ is clearly a sub-field of the field of $8q$-th roots of 1, and this fact furnishes another proof that $(1, \omega, \theta, \omega\theta)$ is a basis of $k(\omega, \theta)$.

θ_1 means $\tfrac{1}{2}[-1-\sqrt{(eq)}]$,

k means $\tfrac{1}{4}(1-eq)$.

Then θ and θ_1 are the roots of $\theta^2+\theta+k = 0$.

$f(x, y)$ means $(x+\theta y)(x+\theta_1 y) = x^2-xy+ky^2 = \tfrac{1}{4}[(2x-y)^2-eqy^2]$.

Then $f(x, y) \equiv 0$, or a quadratic residue mod q.

$\mathfrak{p}$ or π denotes a prime factor of p in the field $k(\omega, \theta)$.

r is the substitution $(\theta : \theta_1)$.

s is the substitution $(\omega : -\omega)$.

ζ is a primitive 8-th root of 1, and ρ a primitive q-th root of 1.

29. In a similar way to that used by Hilbert for the field $k(\iota, \theta)$,† we find that the rules of factorisation in $k(\omega, \theta)$ are as follows.

If p is an odd prime other than q,

if $p \equiv 1$ or 3 (mod 8), and $(p/q) = 1$; then the weight‡ of $\mathfrak{p}$ is 1, that is, p has four conjugate prime factors;

* Hilbert, *Bericht*, p. 267.

† *Math. Annalen*, Bd. 45.

‡ German, *Grad*.

if $p \equiv 1$ or 3 (mod 8), and $(p/q) = -1$, the factorising group is $\{r\}$;

if $p \equiv 5$ or 7 (mod 8), and $(p/q) = 1$, the factorising group is $\{s\}$:

if $p \equiv 5$ or 7 (mod 8), and $(p/q) = -1$, the factorising group is $\{rs\}$;

in the last three cases, the weight of $\mathfrak{p}$ is 2.

When $q \equiv \pm 1$ (mod 8), a prime factor of 2 is (ω, θ), of weight 1.

When $q \equiv \pm 3$ (mod 8), a prime factor of 2 is ω, of weight 2.

When $q \equiv 1$ or 3 (mod 8), a prime factor of q is $(\kappa, \sqrt{(eq)})$, of weight 1, κ being a factor of q in the field $k(\omega)$.

When $q \equiv 5$ or 7 (mod 8), a prime factor of q is $\sqrt{(eq)}$, of weight 2.

30. The next problem is to find the class-number of the field $k(\omega, \theta)$ for the values of q with which we are concerned. For this purpose I use a theorem of Minkowski,* from which is derived this consequence:—

In any algebraic field of order n greater than 2, v being the number of pairs of conjugate imaginary fields, and d being the discriminant of the field, an ideal $\mathfrak{v}$ exists in each ideal class of the field such that

$$N(\mathfrak{v}) < \left(\frac{4}{\pi}\right)^{v} \frac{(n-1)!}{n^{n-1}} \mid d \mid^{\frac{1}{2}}.$$

In the field $k(\omega, \theta)$, $n = 4$, $v = 2$, and so

$$N(\mathfrak{v}) < 3(2\pi^2)^{-1} \mid d \mid^{\frac{1}{2}}$$

$$< q \times 1.22.$$

So when $q = 3, 5, 7, 11, 13,$

$N(\mathfrak{v}) \leqslant 3, 6, 8, 13, 15,$

and $[N(\mathfrak{v})]^{\frac{1}{2}} \leqslant 1, 2, 2, 3, 3.$

We now factorise all rational primes whose factors are of weight 1, not exceeding the limit of $N(\mathfrak{v})$; and if p has as factor a prime ideal $\mathfrak{p}$ of weight 2, then the norm of $\mathfrak{p}$ is p^2, and so in this case, only those primes p need to be factorised which do not exceed $[N(\mathfrak{v})]^{\frac{1}{2}}$.

The prime factors of all rational primes within these limits are given in the table at the end of this part. This table shews that when

$$q = 3, 5, 7, \text{ or } 11,$$

---

* *Geometrie der Zahlen*, pp. 122 and 134.

all these prime factors are principal ideals,* that is, actual numbers, and therefore the class-number is 1.

In the case $q = 13$, the prime factor $\mathfrak{p}$ of 3 is not a principal ideal, for, if it were, $\mathfrak{p}.r\mathfrak{p}$ would be a number of the form $x+y\sqrt{(-26)}$, but 3 clearly cannot have such a factor. Also $\mathfrak{p}.r\mathfrak{p} = (1+\omega)$, and $\mathfrak{p}.s\mathfrak{p} = (\theta)$, and so $r\mathfrak{p}$ and $s\mathfrak{p}$ belong to the same class, and $\mathfrak{p}$ and $rs\mathfrak{p}$ belong to the same class. Again $\mathfrak{p}$ and $s\mathfrak{p}$ belong to different classes, for, if not, $\mathfrak{p}^2$ would be a principal ideal, and then would $x^2+26y^2 = 9$ be soluble. Therefore there are three classes, whose representative ideals are 1, $\mathfrak{p} = (1-\omega, \theta)$, and $s\mathfrak{p} = (1+\omega, \theta)$.

31. In the field $k(\omega, \theta)$, Dirichlet's theorem† shews that there is a single fundamental unit. For each value of q, which is $\equiv -1 \pmod 4$, I have calculated a unit ϵ of $k(\omega, \theta)$ by multiplying the cyclotomic unit $1-\zeta\rho$ by some of its conjugates.

In each case in the table, $\epsilon.rs\epsilon$ is found to be the fundamental unit of $k[\sqrt{(-2eq)}]$, and therefore ϵ is the fundamental unit of $k(\omega, \theta)$.

When $q \equiv 1 \pmod 4$, it is readily proved that the cyclotomic unit $E = \Pi(1-\zeta\rho)$ is a cyclotomic unit of $k(\theta)$. And in the cases $q = 5$ and 13, it may be proved that no unit ϵ exists such that $\epsilon.s\epsilon = \pm E$; therefore in these cases E is the fundamental unit of $k(\omega, \theta)$.

32. We now consider the factors of p in the fields $k(\omega)$ and $k(\theta)$, formed from

$$\pi = d_0+d_1\omega+d_2\theta+d_3\omega\theta.$$

These are
$$c'+d'\omega = \pi.r\pi,$$

and
$$A_0+A_1\theta = \pi.s\pi,$$

where
$$c = f(d_0, d_2)-2f(d_1, d_3),$$

$$d' = 2d_0d_1-d_0d_3-d_1d_2+2kd_2d_3,$$

and
$$A_0 = d_0^2+2d_1^2-k(d_2^2+2d_3^2),$$

$$A_1 = 2d_0d_2+4d_1d_3-d_2^2-2d_3^2.$$

Now
$$A_0+A_1\theta = x+y\sqrt{(eq)},$$

---

* German, *Hauptideal*.

† Hilbert, *Bericht*, p. 214, Satz 47.

where $$x = A_0 - \tfrac{1}{2}A_1,$$

$$y = \tfrac{1}{2}A_1,$$

and $$x^2 - eqy^2 = p.$$

In Cunningham's notation, when $e = 1$, $x = \pm t'$, $y = \pm u'$, and when $e = -1$, $x = \pm t$, $y = \pm u$, except that when $q = 11$,

$$x = \pm \tfrac{1}{2}t, \quad y = \pm \tfrac{1}{2}u.$$

It will be observed that c' and d' may differ in sign from c and d as defined in Part I.

Then $$2x = 2f(d_0, d_2) + eqd_2^2 + 4f(d_1, d_3) + 2eqd_3^2,$$

and so $$x \equiv f(d_0, d_2) + 2f(d_1, d_3).$$

When $q \equiv 1 \pmod 4$, x is essentially positive.

When x is an integer, since $x^2 - eqy^2 = p$ and $eq \equiv 1 \pmod 4$, it follows that x is odd, and $y \equiv 0 \pmod 4$.

Then $$x^2 = (A_0 - y)^2 \equiv A_0^2 + 2y \pmod{16}.$$

And so $$1 + 8m = p \equiv x^2 \equiv A_0^2 + 2y \pmod{16}.$$

For brevity, I write $f = f(d_0, d_2)$ and $f' = f(d_1, d_3)$.

For the remainder of the work, each value of q must be treated separately; the cases $q = 3$ and 5 are dealt with below; and the processes for $q = 7$ and 11 are so similar that they are omitted. In each case, I find Cunningham's corresponding criterion to be correct.

33. *The case* $q = 3$.

Here we have $$c' \equiv f + f',$$

$$x \equiv f - f',$$

and f and f' are $\equiv 0$ or 1.

Since c' and x are both prime to 3, it follows that $c' \equiv 1$.

But $c \equiv (-1)^\gamma$, as in § 7, *supra*. So

$$c' = (-1)^\gamma c \equiv (-1)^\gamma \equiv 1 + 2\gamma \pmod 4.$$

Since $$\pi \equiv d_0 + d_2\theta \pmod \omega,$$

and θ is in this case a unit, by multiplying π by a suitable power of θ we get π in a form such that

$$d_0 \equiv 1, \quad d_2 \equiv 0 \pmod 2.$$

Since $d' \equiv 0 \pmod 2$,

we must then have $d_3 \equiv 0 \pmod 2$.

If $d_1 \equiv 1 \pmod 2$,

then $\pi \equiv 1+\omega \pmod 2$.

But the unit $\epsilon \equiv 1+\omega \pmod 2$,

and so $\epsilon\pi \equiv 1 \pmod 2$.

We may therefore take π in a form such that

$$d_0 \equiv 1, \quad d_1 \equiv d_2 \equiv d_3 \equiv 0 \pmod 2.$$

Then $c' \equiv 1+d_2 \pmod 4$,

and so $d_2 \equiv 2\gamma \pmod 4$.

Again, $A_0 \equiv 1+d_2^2 \pmod 8$,

$\equiv 1+2d_2 \pmod 8$,

$\equiv 1+4\gamma \pmod 8$.

So $A_0^2 \equiv 1+8\gamma \pmod{16}$.

Then, since $y \equiv 4\nu \pmod 8$,

$1+8m \equiv A_0^2+2y \pmod{16}$

$\equiv 1+8\gamma+8\nu \pmod{16}$,

that is, $m+\gamma+\nu \equiv 0 \pmod 2$.

And so $q^{\frac{1}{8}(p-1)} \equiv (-1)^{\alpha+\gamma+m} \equiv (-1)^{\alpha+\nu} \pmod p$,

which is Cunningham's criterion.

34. *The case* $q = 5$.

Here $$\left.\begin{aligned} c' &\equiv f-2f' \\ x &\equiv f+2f', \end{aligned}\right\}$$

and f and f' are $\equiv 0$ or ± 1.

Then we get the four cases—

(i) $f' \equiv 0$, then $c' \equiv x \equiv \pm 1$, $p \equiv 1$, $d' \equiv 0$.

(ii) $f \equiv 0$, then $c' \equiv -x \equiv \pm 2$, $p \equiv -1$, $d' \equiv 0$.

(iii) $f \equiv f'$, then $c' \equiv -2x$, $p \equiv -1$, $d' \not\equiv 0$.

(iv) $f \equiv -f'$, then $c' \equiv 2x$, $p \equiv 1$, $d' \not\equiv 0$

Since in this case x is positive, it follows from Cunningham's definition of τ' and his condition* for $(5/p)_4 = 1$, that

when $p \equiv 1$, $\qquad x \equiv (-1)^{\tau'}$,

and when $p \equiv -1$, $\qquad x \equiv -2(-1)^{\tau'}$.

The only unit in this case being θ, we can get π (by multiplying it by θ or θ^2) in a form such that

$$d_0 \equiv 1, \quad d_1 \equiv 0 \text{ or } 1, \quad d_2 \equiv d_3 \equiv 0 \pmod 2.$$

Then $\qquad c' \equiv 1+2d_1+d_2 \pmod 4$,

so $\qquad c' = (-1)^{d_1+\frac{1}{2}d_2} c$.

The values of c in terms of γ are given in § 8 *supra*.

In case (i) we have $c' \equiv (-1)^{\gamma+d_1+\frac{1}{2}d_2}$, $x \equiv (-1)^{\tau'}$,

so since $\qquad c' \equiv x$,

$$\gamma+\tau' \equiv d_1+\tfrac{1}{2}d_2 \pmod 2.$$

And the same result is found in the other three cases.

Now $\qquad A_0 \equiv 1+2d_1^2+2d_2 \pmod 8$.

So, if $d_1 \equiv 0 \pmod 2$, $\qquad A_0 \equiv 1+2d_2 \pmod 8$,

and $\qquad A_0^2 \equiv 1+4d_2 \pmod{16}$;

and if $d_1 \equiv 1 \pmod 2$, $\qquad A_0 \equiv 3+2d_2 \pmod 8$,

and $\qquad A_0^2 \equiv 9+4d_2 \pmod{16}$.

So in each case $\qquad A_0^2 \equiv 1+8d_1+4d_2 \pmod{16}$,

and then $\qquad m+\nu' \equiv \tfrac{1}{8}(A_0^2-1) \equiv d_1+\tfrac{1}{2}d_2 \pmod 2$.

Therefore, finally, $\qquad m+\gamma+\tau'+\nu' \equiv 0 \pmod 2$,

which proves that $\qquad q^{\frac{1}{2}(p-1)} \equiv (-1)^{m+\alpha+\tau'+\nu'} \pmod p$,

which is Cunningham's criterion.

It will now be shewn that this is true, taking any solution t', u', of

$$x^2-5y^2 = p.$$

Since $\theta^3 = -2+\sqrt{5}$, $\theta^6 = 9-4\sqrt{5}$ gives the fundamental solution of

$$x^2-5y^2 = 1;$$

---

* *Proc. London Math. Soc.*, Ser. 2, Vol. 1, p. 132.

and therefore by multiplying π by a suitable power of θ^3, we can obtain π in that form which corresponds to the fundamental or any other given solution of $x^2-5y^2=p$.

Table of the Fields $k(\omega, \theta)$.

q	p	Weight of $\mathfrak{p}$	$\mathfrak{p}$	Class Number.	Fundamental Unit.
3	3	1	$1-\omega\theta$	1	$1+\omega+2\theta$
5	2	2	ω	1	θ
7	2	1	$\omega+\theta$	1	$1+2\omega+2\theta$
11	2 3 11	2 1 1	ω $1-\omega+\theta$ $3-2\omega+2\theta+\omega\theta$	1	$3+7\omega+6\theta$
13	2 3	2 1	ω $(1-\omega, \theta)$	3	$2+\theta$

PART VI.

The Quartic Field $k(\iota, \theta)$.

35. In this part, θ, r and $f(x, y)$ have the same meanings as in Part V. The field $k(\iota, \theta)$ is a sub-field of the field of $4q$-th roots of 1. A basis of the field is 1, ι, θ, $\iota\theta$, and its discriminant is 2^4q^2.

$$\pi = b_0+b_1\iota+b_2\theta+b_3\iota\theta$$

denotes a prime factor of p in the field.

λ denotes $1+\iota$.

t is the substitution $(\iota, -\iota)$.

As in Part III, an ideal $\mathfrak{d}$ exists in each ideal class such that

$$N(\mathfrak{d}) < q\times\cdot 61.$$

So when $q = 3,\ 5,\ 7,\ 11,\ 13,$

$$N(\mathfrak{d}) \leqslant 1,\ 3,\ 4,\ 6,\ 7.$$

The table at the end of this part shews that for all these values of q the class number of $k(\iota, \theta)$ is 1. The fundamental units have been calculated as in § 31.

36. The factors of p in the three quadratic sub-fields $k(\iota)$, $k(\sqrt{q})$, and $k[\sqrt{(-q)}]$, formed from π are

$$a'+b'\iota = \pi.r\pi,$$

$$A_0+A_1\theta = \pi.t\pi,$$

and $$x'+y'\sqrt{(-eq)} = \pi.rt\pi,$$

where
$$a' = f(b_0, b_2)-f(b_1, b_3),$$

$$b' = 2b_0b_1-b_0b_3-b_1b_2+2kb_2b_3,$$

$$A_0 = b_0^2+b_1^2-k(b_2^2+b_3^2),$$

$$A_1 = 2b_0b_2+2b_1b_3-b_2^2-b_3^2,$$

$$x' = f(b_0, b_2)+f(b_1, b_3),$$

$$y' = b_0b_3-b_1b_2.$$

As in § 32, $$x = A_0-\tfrac{1}{2}A_1, \quad y = \tfrac{1}{2}A_1,$$

when $e = 1$, $x = \pm t'$, $y = \pm u'$, $x' = \pm t$, $y' = \pm u$,

and when $e = -1$, $x = \pm t$, $y = \pm u$, $x' = \pm t'$, $y' = \pm u$

(with the same exception as in § 32 for $q = 11$). And as in § 32,

$$m+\tfrac{1}{4}y \equiv \tfrac{1}{8}(A_0^2-1) \pmod 2,$$

whenever $$y \equiv 0 \pmod 4.$$

It will suffice to give the full proof of Cunningham's criterion for $q = 3$. I have verified his criteria in the cases $q = 5$, 7, and 11.

37. *The case* $q = 3$.

Since $$\pi \equiv b_0+b_1+(b_2+b_3)\theta \pmod \lambda,$$

and 1, θ and θ^2 is a complete set of residues (mod λ), by multiplying π by a suitable power of the unit θ, we get

$$b_0+b_1 \equiv 1, \quad b_2+b_3 \equiv 0 \pmod 2;$$

and then using a suitable power of ι, we get

$$b_0 \equiv 1, \quad b_1 \equiv 0 \pmod 2.$$

If $$b_2 \equiv b_3 \equiv 1 \pmod 2,$$

then $$\pi \equiv 1+\theta(1+\iota) \equiv \epsilon \pmod 2,$$

and then $$\epsilon\pi \equiv \epsilon^2 \equiv 1 \pmod 2.$$

Therefore, in the first place, we take

$$b_0 \equiv 1, \quad b_1 \equiv b_2 \equiv b_3 \equiv 0 \pmod 2.$$

Then $$b' \equiv 0 \pmod 2,$$

and so $$b' = \pm b \equiv 0 \pmod 4,$$

and therefore $$b_3 \equiv 0 \pmod 4,$$

and $$b' \equiv 2b_1+b_3+b_1b_2 \pmod 8.$$

Also $$y' \equiv b_3+b_1b_2 \pmod 8.$$

Therefore $$b'+y' \equiv 2b_1 \pmod 8,$$

that is, $$\beta+\upsilon' \equiv \tfrac{1}{2}b_1 \pmod 2.$$

x' is positive, and so $$t' = x' \equiv 1+b_2 \pmod 4,$$

and $$\tau' \equiv \tfrac{1}{2}(t'-1) \equiv \tfrac{1}{2}b_2 \pmod 2.$$

Therefore $$\beta+\tau'+\upsilon' \equiv \tfrac{1}{2}(b_1+b_2) \pmod 2.$$

Also $y \equiv 0 \pmod 4$, and $A_0 \equiv 1+2(b_1+b_2) \pmod 8$,

and so $$m+\upsilon \equiv \tfrac{1}{2}(b_1+b_2) \pmod 2,$$

and, finally, $$m+\beta+\upsilon+\tau'+\upsilon' \equiv 0 \pmod 2,$$

which proves the criterion for the case of $u' \equiv 0 \pmod 2$.* Since π may be multiplied by any power of ϵ^2 without affecting the argument, the criterion holds for any solution of $t'^2-3u'^2 = p$ in which $u' \equiv 0 \pmod 2$.

For the second case, in which $t' \equiv 0 \pmod 2$, we take $\epsilon\pi$ instead of π, and corresponding to this, we get

$$T'+U'\sqrt{3} = \epsilon.rt\epsilon(t'+u'\sqrt{3}) = (2-\sqrt{3})(t'+u'\sqrt{3}),$$

and so $$T' = 2t'-3u'.$$

Defining τ_0' by $T' = 4\tau_0'+2$,†

$$\tau_0' \equiv \tfrac{1}{2}(t'-1)+\tfrac{1}{4}u' \pmod 2$$
$$\equiv \tau'+\upsilon' \pmod 2.$$

Therefore in this case the desired congruence is

$$m+\beta+\upsilon+\tau_0' \equiv 0 \pmod 2,$$

which proves the criterion for the case of $t' \equiv 0 \pmod 2$.*

---

* *Ante*, p. 10 of this volume, Table II, last column.

† Cunningham writes τ' for τ_0'.

Table of the Fields $k(\iota, \theta)$.

q	p	Weight of $\mathfrak{p}$	$\mathfrak{p}$	Class Number.	Fundamental Unit.
3	—	—	—	1	$1+\theta+\iota\theta$
5	—	—	—	1	θ
7	2	1	$1+\iota+\theta$	1	$1+2\iota-\theta+\iota\theta$
11	2 5	2 1	$1+\iota$ $1+\iota+\theta$	1	$1+2\iota-\theta+\iota\theta$
13	2	2	$1+\iota$	1	$2+\theta$