# RATIONAL CUBIC AND BIQUADRATIC RECIPROCITY

PAUL POLLACK

It is ordinary rational arithmetic which attracts the ordinary man. . .
– G.H. Hardy [48]

## 1. Introduction

### 1.1. Quadratic, Cubic and Biquadratic Reciprocity.

On April 8, 1796, Gauss [40, §125-145] succeeded in proving a remarkable theorem discovered experimentally by Euler fifty years previously. Gauss was so impressed with this result that he referred to it as the Theorema Aureum (Golden Theorem), and to this day it forms the capstone of any course on elementary number theory:

**Law of Quadratic Reciprocity.** *If $p$ and $q$ are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

*Moreover, we have the supplementary laws*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

It seems incredible that $p$ being a square modulo $q$ would have anything to do with $q$ being a square modulo $p$. In his attempts to penetrate this mystery, Gauss by the end of his life produced eight distinct proofs of this law. His first is remarkable not only for the considerable ingenuity it exhibits but also for its somewhat startling technique: induction. Since it is little-known today, we give Dirichlet's version of this argument ([20], [22, §48-51]) in §2.

The existence of the law of quadratic reciprocity raises natural questions: Is there a cubic reciprocity law? a quartic (or biquadratic) law? Euler did not wait for a proof of the quadratic reciprocity law to appear before investigating these questions. In an incomplete draft of a textbook on number theory [27, §§407-411, §458] probably composed between 1748 and 1750, he includes conjectured necessary and sufficient conditions for $2, 3, 5$ and $6$ and to be cubic residues modulo $p$ and for 2 to be a biquadratic residue. (The margins also record similar conditions for 7 and 10 to be cubic residues and for 3 and 5 to be quartic residues.) Remarkably, all these conjectures turned out to be correct! "Divination" was the explanation of R. Fueter, who edited the fifth volume of Euler's collected works [28]. A bit later Fueter added:

> Hence all the Eulerian conjectures have been proved correct, and it borders on the incomprehensible how Euler could have guessed these complicated conditions. There is no more striking example of his brilliant insight into mathematical relationships.

As penetrating as Euler's observations were, the credit for the first rigorous results connected with higher reciprocity must go to Gauss. The earliest developments have been preserved in Gauss's mathematical diary, the February 15, 1807 entry of which reads [45, entry 130]:

> Begun the theory of cubic and biquadratic residues.

On February 22nd, a mere one week later, Gauss records remarkable progress [45, entry 131]:

> The proof of this theory discovered by most elegant methods so that it is totally perfect and nothing further is desired.

Despite Gauss's exuberance, he did not publish on this subject until 1828, and it is unclear exactly how much of the theory of biquadratic residues was in his possession at this time (but see [78, p. 200] for an educated guess). Presumably he did not know the reciprocity laws in their final form, for on October 23, 1813 he would write [45, entry 144]:

> The foundation of the general theory of biquadratic residues which we have sought for with utmost effort for almost seven years but always unsuccessfully at last happily discovered the same day on which our son is born ...

The next entry adds:

> This is the most subtle of all that we have ever accomplished at any time. It is scarcely worthwhile to intermingle it with mention of certain simplifications pertaining to the calculation of parabolic orbits.

The eventual publication of his first memoir [33] on biquadratic residues included a tantalizing pronouncement in its introduction:

> ... a general theory requires that to a certain extent the domain of higher arithmetic needs to be endlessly enlarged.

However, details were deferred to the next memoir. It is clear that Gauss thought he had discovered something significant for the development of arithmetic, but what? In his second, 1832 memoir [34] on biquadratic residues, the secret is finally revealed: here he introduces the so-called Gaussian integers $\mathbf{Z}[i]$ as the natural context for the statement of the fourth power reciprocity law, and births algebraic number theory in the process.

If $\pi$ is a Gaussian prime, one defines in this theory the fourth-power residue symbol $\left[\frac{\alpha}{\pi}\right]_4$ to be that complex fourth of unity satisfying the congruence

$$\left[\frac{\alpha}{\pi}\right]_4 \equiv \alpha^{(N(\pi)-1)/4} \pmod{\pi}.$$

The biquadratic reciprocity law then assumes the form of a relation between $\left[\frac{\pi_1}{\pi_2}\right]_4$ and $\left[\frac{\pi_2}{\pi_1}\right]_4$ when $\pi_1$ and $\pi_2$ are coprime primes of odd norm. A supplementary law governing the biquadratic behavior of $1+i$ brings the theory to the same level of perfection that the theory of quadratic residues had attained through the quadratic reciprocity law.

Gauss recognized that similar considerations apply also to cubic residues; in a footnote to the same 1832 memoir he wrote:

> The theory of cubic residues must similarly be grounded on the consideration of the numbers $a + bh$, where $h$ is an imaginary root of the equation $h^3 - 1$, say $h = -\frac{1}{2} + \sqrt{\frac{3}{4}}i$, and likewise the theory of higher power residues demands the introduction of other imaginary quantities.

A May 30, 1828 letter to Dirichlet [36] reveals that Gauss intended a third memoir in the same series as [33] and [34], where he would finally present a complete proof of the announced quartic reciprocity law. Indeed, we know from the same letter that Gauss claimed to have been in possession of a complete proof for 14 years (consistent with the quoted 1813 diary entry). But for reasons that are unclear, no third memoir appeared, and we owe to Eisenstein the first published proofs of both cubic [24] and biquadratic reciprocity [25]. (One often hears the ring $\mathbf{Z}[\zeta_3]$ referred to as the "Eisenstein integers" in his honor.) It should be noted however that Jacobi had already presented proofs of both laws in his Königsberg lectures of 1837.

1.2. **Rational Reciprocity.** Rational reciprocity, as we use the term in this chapter, aims at answering the following question: Knowing that the cubic and biquadratic reciprocity laws are best formulated in terms of the Eisenstein and Gaussian primes, what interesting statements can be made about reciprocity for rational primes?

If we view Gauss's introduction of $\mathbf{Z}[i]$ into the study of biquadratic residues as the tremendous insight that it so clearly was, then this line of inquiry may seem like a perverse step backwards. There is no point in arguing this – suffice it to say that the reader who bears with us will find the charming theorems to be their own reward.

The first result we take up was published in 1827, shortly before the appearance of Gauss's first memoir [33] on biquadratic residues. That year Jacobi's own investigations on cubic reciprocity were reaching fruition. In a February 1827 letter to Gauss [53], Jacobi gives explicit necessary and sufficient conditions for $q = 2, 3, 5, \ldots, 17$ to be cubic residues of a prime $p$. In [52] he states a weak form of the cubic reciprocity law applicable to pairs of rational primes. Unlike Euler, Jacobi had proofs for his claims; from his letter of Gauss, it appears the rational cubic law was derived from a fledgling application of what are now known as Jacobi sums. One of our goals will be to prove Jacobi's reciprocity theorem in a particularly striking form discovered by Z.-H. Sun [98].

Quadratic reciprocity is neither more nor less than the assertion that for distinct odd primes $p$ and $q$,

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right), \quad \text{where} \quad q^* := (-1)^{(q-1)/2}q.$$

It can therefore be thought of as describing exactly when $q^*$ is a square modulo $p$. In 1828, Dirichlet [18] took up the following question: Suppose we know that $\left(\frac{q^*}{p}\right) = 1$. When is $q^*$ a fourth power modulo $p$?

Dirichlet's answer to this question will provide us with an example of a rational biquadratic reciprocity law. This particular law rediscovered in a slightly modified form more than a century later by E. Lehmer [74] (see Exercise 39). Other laws with a similar flavor, each incorporating their own intriguing twist, have been given

Table 1. Of the first 10000 primes $p \equiv 1 \pmod 3$, the number for which 2 is a cube which lie in various nonzero residue classes modulo 8, 9, 5, 7 and 11.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $p \pmod 8$ | 813 | | 835 | | 833 | | 833 | | | |
| $p \pmod 9$ | 1119 | | | 1108 | | | 1087 | | | |
| $p \pmod 5$ | 814 | 837 | 831 | 832 | | | | | | |
| $p \pmod 7$ | 538 | 557 | 549 | 548 | 565 | 557 | | | | |
| $p \pmod{11}$ | 331 | 325 | 329 | 319 | 320 | 366 | 326 | 344 | 336 | 318 |

by Burde [10] and Scholz [93], and a general rational quartic reciprocity law (which implies all of the others) was proven by Williams, Hardy & Friesen [108]. All of these results will be discussed in this chapter.

1.3. **Conjecturing the Rational Reciprocity Laws: Cubic Reciprocity.** So far we have purposely sidestepped giving a precise statement of any of the rational reciprocity laws alluded to above.

Let us see how far we can get on our own. As a test case, we study experimentally the primes for which 2 and 3 are cubes modulo $p$, restricting always our attention to primes $p \equiv 1 \pmod 3$ (recall that for other primes everything is a cube modulo $p$). A first guess, motivated by quadratic reciprocity, is that the cubic character of 2 and 3 should be governed by congruence considerations.

However, Table 1 suggests that the property of 2 being a cube modulo $p$ is rather indifferent to congruence properties of $p$. (A similar table, omitted here, could be offered for 3.) This imprecise statement can be made rigorous and established in a strong form via Chebotarev's density theorem of algebraic number theory. That theorem implies that if the invertible residue class $a \pmod m$ contains integers congruent to $1 \pmod 3$, then asymptotically $1/3$ of the primes $p \equiv a \pmod m$ have 2 (or 3) as a cube. Hence there can be no characterization of when 2 (or 3) is a cube in terms of congruence conditions on $p$. But why confine ourselves to looking merely at $p$?

Recall the following lemma:

**Lemma 1.1.** *Let $p \equiv 1 \pmod 3$ be prime. Then there are integers $L$ and $M$, uniquely determined up to sign, for which $4p = L^2 + 27M^2$.*

Note that while this lemma only asserts the existence of $L$ and $M$, computing $L$ and $M$ for a given $p$ is not difficult. So there is no cause to grumble if we can find a criterion for 2 or 3 to be a cube in terms of the corresponding numbers $L$ and $M$. But does such a criterion exist?

Table 2 certainly suggests that it does. A bit of staring leads one to the following guess:

**Rational Cubic Character of 2 and 3** (Gauss [38, §4]). *Let $p \equiv 1 \pmod 3$, and write $4p = L^2 + 27M^2$, where $L$ and $M$ are positive. Then*

$$2 \textit{ is a cube mod } p \iff 2 \mid L, 2 \mid M \iff p = L'^2 + 27M'^2 \textit{ for some } L', M',$$

$$3 \textit{ is a cube mod } p \iff 3 \mid M \iff 4p = L'^2 + 243M'^2 \textit{ for some } L', M'.$$

| $p$ | $L$ | $M$ | $2 =$ cube? | $3 =$ cube? | $p$ | $L$ | $M$ | $2 =$ cube? | $3 =$ cube? |
|---|---|---|---|---|---|---|---|---|---|
| 7 | 1 | 1 | N | N | 271 | 29 | 3 | N | Y |
| 13 | 5 | 1 | N | N | 277 | 26 | 4 | Y | N |
| 19 | 7 | 1 | N | N | 283 | 32 | 2 | Y | N |
| 31 | 4 | 2 | Y | N | 307 | 16 | 6 | Y | Y |
| 37 | 11 | 1 | N | N | 313 | 35 | 1 | N | N |
| 43 | 8 | 2 | Y | N | 331 | 1 | 7 | N | N |
| 61 | 1 | 3 | N | Y | 337 | 5 | 7 | N | N |
| 67 | 5 | 3 | N | Y | 349 | 37 | 1 | N | N |
| 73 | 7 | 3 | N | Y | 367 | 35 | 3 | N | Y |
| 79 | 17 | 1 | N | N | 373 | 13 | 7 | N | N |
| 97 | 19 | 1 | N | N | 379 | 29 | 5 | N | N |
| 103 | 13 | 3 | N | Y | 397 | 34 | 4 | Y | N |
| 109 | 2 | 4 | Y | N | 409 | 31 | 5 | N | N |
| 127 | 20 | 2 | Y | N | 421 | 19 | 7 | N | N |
| 139 | 23 | 1 | N | N | 433 | 2 | 8 | Y | N |
| 151 | 19 | 3 | N | Y | 439 | 28 | 6 | Y | Y |
| 157 | 14 | 4 | Y | N | 457 | 10 | 8 | Y | N |
| 163 | 25 | 1 | N | N | 463 | 23 | 7 | N | N |
| 181 | 7 | 5 | N | N | 487 | 25 | 7 | N | N |
| 193 | 23 | 3 | N | Y | 499 | 32 | 6 | Y | Y |
| 199 | 11 | 5 | N | N | 523 | 43 | 3 | N | Y |
| 211 | 13 | 5 | N | N | 541 | 29 | 7 | N | N |
| 223 | 28 | 2 | Y | N | 547 | 1 | 9 | N | Y |
| 229 | 22 | 4 | Y | N | 571 | 31 | 7 | N | N |
| 241 | 17 | 5 | N | N | 577 | 11 | 9 | N | Y |

Table 2. The first fifty primes $p \equiv 1 \pmod 3$ together with positive values of $L$ and $M$ for which $4p = L^2 + 27M^2$ and the cubic residue status of 2 and 3.

We have labeled this in the style of a theorem, and indeed our guess can be proved correct. We will do this in §4.2.

Spurred on by the sweet taste of success, let us attempt to characterize the primes $p$ for which $q = 5$, 7 and 11 are cubic residues. Table 3 shows the results of a computation for primes $p \equiv 1 \pmod 3$ between $10^6$ and $10^6 + 10^3$. This range of primes was motivated by the desire to see reasonably large values of $L$ and $M$. In this table we also include the ratio $\frac{L}{3M} \bmod q$, writing $\frac{L}{3M} \bmod q = \infty$ if $q \mid M$. (Granted, it requires a a bit of prophetic insight to even consider the ratio of $L$ to $M$ mod $q$, and a double portion of such to consider the even more obscure $\frac{L}{3M}$. Patience; all will be clear in time!)

For $q = 3, 5$ and 7, it appears from Table 3 that $q$ is a cube modulo $p$ precisely when $q \mid LM$ (i.e., when $\frac{L}{3M} = 0$ or $\infty$). When $q = 11$, it is also the case that $q$ is a cube modulo $p$ if $\frac{L}{3M} = 0$ or $\infty$, but also when $\frac{L}{3M} = \pm 5$. These limited examples lead us to conjecture that a fixed prime $q$ is a cubic residue of $p$ if and only if $\frac{L}{3M}$ belongs to a certain subset $S$ of $\mathbf{Z}/q\mathbf{Z} \cup \{\infty\}$. This is about as far as experimental mathematics will take us. At this point we can only before the genius of the ages and simply state Jacobi's Rational Cubic Reciprocity Law, which vindicates our conjecture and provides an explicit description of the set $S$:

| $p$ | $L$ | $M$ | 5? | $\frac{L}{3M}$ mod 5 | 7? | $\frac{L}{3M}$ mod 7 | 11? | $\frac{L}{3M}$ mod 11 |
|---|---|---|---|---|---|---|---|---|
| 100003 | 337 | 103 | N | -2 | N | 1 | N | -4 |
| 100057 | 175 | 117 | Y | 0 | Y | 0 | N | 1 |
| 100069 | 458 | 84 | N | -1 | Y | $\infty$ | N | 4 |
| 100129 | 562 | 56 | N | -1 | Y | $\infty$ | N | 4 |
| 100153 | 443 | 87 | N | -2 | N | 1 | N | -1 |
| 100183 | 383 | 97 | N | -2 | N | 3 | N | 4 |
| 100189 | 209 | 115 | Y | $\infty$ | N | 3 | Y | 0 |
| 100207 | 421 | 91 | N | 2 | Y | $\infty$ | N | 4 |
| 100213 | 575 | 51 | Y | 0 | N | -1 | N | -3 |
| 100237 | 194 | 116 | N | -2 | N | 1 | N | 1 |
| 100267 | 224 | 114 | N | 2 | Y | 0 | N | 4 |
| 100279 | 137 | 119 | N | 1 | Y | $\infty$ | N | 1 |
| 100291 | 491 | 77 | N | 1 | Y | $\infty$ | Y | $\infty$ |
| 100297 | 250 | 112 | Y | 0 | Y | $\infty$ | Y | 5 |
| 100333 | 515 | 71 | Y | 0 | N | -1 | Y | 5 |
| 100357 | 631 | 11 | N | 2 | N | 3 | Y | $\infty$ |
| 100363 | 355 | 101 | Y | 0 | N | -1 | Y | -5 |
| 100393 | 593 | 43 | N | 2 | N | -3 | N | 4 |
| 100411 | 179 | 117 | N | -1 | N | -3 | N | -3 |
| 100417 | 139 | 119 | N | 2 | Y | $\infty$ | N | -3 |
| 100447 | 404 | 94 | N | 2 | N | -1 | N | -2 |
| 100459 | 263 | 111 | N | 1 | N | 1 | N | -4 |
| 100483 | 8 | 122 | N | -2 | N | -3 | N | -1 |
| 100501 | 323 | 105 | Y | $\infty$ | Y | $\infty$ | N | -1 |
| 100519 | 523 | 69 | N | -1 | N | 3 | N | -3 |
| 100537 | 305 | 107 | Y | 0 | N | 3 | N | 4 |
| 100549 | 83 | 121 | N | 1 | N | 1 | Y | $\infty$ |
| 100591 | 181 | 117 | N | 1 | N | -1 | Y | -5 |
| 100609 | 622 | 24 | N | 1 | N | 3 | N | 1 |
| 100621 | 574 | 52 | N | -1 | Y | 0 | N | 1 |
| 100669 | 626 | 20 | Y | $\infty$ | N | -1 | N | 2 |
| 100693 | 475 | 81 | Y | 0 | N | -3 | N | 2 |
| 100699 | 143 | 119 | N | -1 | Y | $\infty$ | Y | 0 |
| 100741 | 509 | 73 | N | 1 | N | -1 | N | -3 |
| 100747 | 605 | 37 | Y | 0 | N | -3 | Y | 0 |
| 100801 | 254 | 112 | N | -1 | Y | $\infty$ | N | 2 |
| 100927 | 380 | 98 | Y | 0 | Y | $\infty$ | N | -2 |
| 100957 | 185 | 117 | Y | 0 | N | 3 | N | 2 |
| 100981 | 457 | 85 | Y | $\infty$ | N | 3 | N | 3 |
| 100987 | 595 | 43 | Y | 0 | Y | 0 | N | -4 |
| 100999 | 452 | 86 | N | -1 | N | 3 | N | -2 |

TABLE 3. Primes $p \equiv 1 \pmod 3$ between $10^6$ and $10^6 + 10^3$, together with the cubic residue status of $p$ with respect to $5, 7$ and 11, and the ratios $\frac{L}{3M}$ with respect to the same moduli.

Table 4. Jacobi's criteria for $q = 11, 13, 17, 23, 29, 31$ or $37$ to be cubic residues modulo $p = \frac{1}{4}(L^2 + 27M^2)$. In each case it is necessary and sufficient that either $q \mid L$, $q \mid M$, or that one of the given congruences holds.

| $q$ | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 |
|---|---|---|---|---|---|---|---|---|
| | $L \equiv \pm 4M$ | $L \equiv \pm M$ | $L \equiv \pm 3M$ | $L \equiv \pm 3M$ | $L \equiv \pm 2M$ | $L \equiv \pm 2M$ | $L \equiv \pm 5M$ | $L \equiv \pm 8M$ |
| | | | $L \equiv \pm 9M$ | $L \equiv \pm 9M$ | $L \equiv \pm 8M$ | $L \equiv \pm \ M$ | $L \equiv \pm 7M$ | $L \equiv \pm 3M$ |
| | | | | | $L \equiv \pm 11M$ | $L \equiv \pm 11M$ | $L \equiv \pm 6M$ | $L \equiv \pm 9M$ |
| | | | | | | $L \equiv \pm 13M$ | $L \equiv \pm 11M$ | $L \equiv \pm 7M$ |
| | | | | | | | | $L \equiv \pm 12M$ |

**Jacobi-Sun Rational Cubic Reciprocity Law.** *Let $p$ and $q$ be distinct primes greater than $3$, and suppose that $p \equiv 1 \pmod 3$.* Jacobi:

$$q \textit{ is a cube modulo } p \Leftrightarrow \frac{L + 3M\sqrt{-3}}{L - 3M\sqrt{-3}} \textit{ is a cube in } \mathbf{F}_q(\sqrt{-3}).$$

Z.-H. Sun: *Equivalently, let $G = G(q)$ be the group $\{[a,b] : a, b \in \mathbf{F}_q$ and $a^2 + 3b^2 \neq 0\}$, where $[a,b]$ and $[c,d]$ are identified if one is a nonzero scalar multiple of the other, and where multiplication is defined by*

$$[a,b] \star [c,d] = [ac - 3bd, ad + bc].$$

*Then $G$ is a cyclic group of order $q - \left(\frac{-3}{q}\right)$, and*

$$q \textit{ is a cube modulo } p \Leftrightarrow [L, 3M] \textit{ is a cube in } G.$$

Jacobi also presented ([52], [53]) specific criteria for the primes $q = 11$, $13$, $17$, $23$, $29$, $31$ and $37$ (see Table 4). Note that Jacobi considers the expression $\frac{L}{M} \bmod q$ instead of $\frac{L}{3M}$, but as we shall see in the proof, the latter arises somewhat more naturally. It is worth noting that Jacobi's law appears (without proof) in Gauss's Nachlass [38, §2].

1.4. **Rational Biquadratic Reciprocity.** The two principal theorems of Gauss's first memoir on biquadratic residues concern the biquadratic character of 2. Here he proves:

**Rational Quartic Character of 2.** *Suppose $p \equiv 1 \pmod 8$, so that $2$ is a square modulo $p$. Write $p = a^2 + 4b^2 = c^2 + 2d^2$ for integers $a, b, c$ and $d$. Then the following are equivalent:*

(i) *$2$ is a fourth power residue modulo $p$,*
(ii) *$c \equiv \pm 1 \pmod 8$,*
(iii) *$b \equiv 0 \pmod 4$.*

Though the restriction to $p \equiv 1 \pmod 8$ may seem artificial at first glance, this theorem settles completely the problem of determining the primes for which 2 is a fourth power. For if 2 is a fourth power, then 2 is a square, so that $p \equiv \pm 1 \pmod 8$. If $p \equiv -1 \pmod 8$, then the set of fourth powers modulo $p$ coincides with the set of squares, and there is no further investigation required. And the remaining case when $p \equiv 1 \pmod 8$ is exactly the concern of Gauss's theorem.

We shall prove that (i) is equivalent to (iii) in §5.1 below; the equivalence of (i) and (ii) will be established in Exercise 44. Note the analogy with the results we have seen for cubic residues.

Though Gauss's first memoir concerning biquadratic residues did not appear in print until 1828, its results were announced already [39] in the *Göttingische Gelehrte Anzeigen* of 1825. That year Dirichlet would have been 20 years old – eager, full of enthusiasm, and in awe of the author of the *Disquisitiones.* (According to Kummer, Dirichlet continually culled the Disquisitiones for new insights, resting it always on his worktable and never on his bookshelf.) It appears that Dirichlet obtained the announcement of Gauss's results around 1827 (perhaps from Gauss himself during their first meeting), and immediately set out to obtain a proof.

The story of his ultimate success is told in an October 19, 1827 letter to his mother (where the translation is Rowe's; for a transcript of the original see Rowe's paper [91] as well as the follow-up note [95]):

> Regarding the above mentioned investigations I experienced a most peculiar fortune. Already in the course of the summer I had made a number of steps that brought me nearer to the goal I sought. Still, there always loomed one difficulty that needed to be overcome before I had the proof of Gauss's theorems. I concentrated on this matter incessantly, not only during my trip to the mountains but also in Dresden, and yet without gaining any real insight. One evening, as I wandered alone on the Elbe bridge (which, by the way, occurred only seldom, as I enjoyed too much being in the company of such kindly people as the Remer family) I had a few ideas that appeared to put me within grasp of the so long and zealously searched for results. On the gorgeous Brühl terrace I let my thoughts go for several hours (till around ten o'clock), but still I could not see my way to the end of the matter (probably because nonmathematical ideas kept mixing together with the mathematical ones). With very weak hopes I went to bed and was extremely restless until around one o'clock when I finally fell asleep. But then I woke up again around four o'clock, and even awoke the health official, who slept in the same room, by hollering: "I've found it" ["Ich habe es gefunden"]. It took but a moment for me to get up, turn on the light, and pen in hand, convince myself of its correctness. After this my investigations expanded every day, and fourteen days later I was in a position to send Herr Encke the six-page sketch ...

The completed manuscript was described by Jacobi as "the first time general theorems on biquadratic residues were presented." For there Dirichlet not only presents his own proofs for Gauss's criteria concerning the biquadratic character of 2, but using similar methods completely characterizes the primes for which an arbitrary odd prime $q$ is a fourth power.

Table 5. Determination of $\left(\frac{q^*}{p}\right)$ for $q = 3, 5, 7, 11, 13, 17, 19$. Here $p \equiv 1 \pmod 4$ and $p = a^2 + b^2$ (where $a, b > 0$ and $b$ is even).

| $-3$ | | $+5$ | | $-7$ | | $-11$ | |
|---|---|---|---|---|---|---|---|
| $+1$ | $b \equiv 0$ | $+1$ | $b \equiv 0$ | $+1$ | $b \equiv 0,\ a \equiv 0$ | $+1$ | $b \equiv 0,\ a \equiv \pm 2b$ |
| $-1$ | $a \equiv 0$ | $-1$ | $a \equiv 0$ | $-1$ | $a \equiv b,\ a \equiv -b$ | $-1$ | $a \equiv 0,\ a \equiv \pm 5b$ |

| $+13$ | | $+17$ | | $-19$ | |
|---|---|---|---|---|---|
| $+1$ | $b \equiv 0, \pm 3a$ | $+1$ | $b \equiv 0, a \equiv 0, \pm b$ | $+1$ | $b \equiv 0, a \equiv \pm 4b, \pm 9b$ |
| $-1$ | $a \equiv 0, \pm b$ | $-1$ | $a \equiv \pm 5b, \pm 7b$ | $-1$ | $a \equiv 0, \pm 2b, \pm 5b$ |

Before stating his results it is helpful to introduce the *rational fourth power residue symbol* $\left(\frac{a}{p}\right)_4$ defined for $a$ a nonzero square mod $p$:

$$\left(\frac{a}{p}\right)_4 := \begin{cases} 1 & \text{if } a \text{ is a nonzero fourth power modulo } p, \\ -1 & \text{if } a \text{ is a nonzero square but not a fourth power modulo } p. \end{cases}$$

If $p \equiv 3 \pmod 4$, then this symbol is trivial on its domain of definition. But if $p \equiv 1 \pmod 4$, then $\left(\frac{a}{p}\right)_4$ induces the unique nontrivial character of $(\mathbf{F}_p^*)^2/(\mathbf{F}_p^*)^4$. For these primes we therefore have a reasonable quartic analog of the Legendre symbol, except that the "numerator" is now restricted to squares modulo $p$. As can easily be verified, the analog of Euler's criterion also holds for these primes: $\left(\frac{a}{p}\right)_4 \equiv a^{(p-1)/4} \pmod p$ whenever the left hand side is defined.

Here is one way of stating this extension of Dirichlet:

**Dirichlet-Sun Rational Quartic Reciprocity Law.** *Let $p$ and $q$ be distinct odd primes, where $p \equiv 1 \pmod 4$. Let $q^* := (-1)^{(q-1)/2}q$. Then*

$$\left(\frac{q^*}{p}\right)_4 = \left(\frac{a+bi}{a-bi}\right)^{(q-(\frac{-1}{q}))/4} \quad \text{in } \mathbf{F}_q(i)$$

*provided at least one side is defined and has the value* $\pm 1$. Z.-H. Sun [99]*: Equivalently, let $G = G(q)$ be the group $\{[a,b] : a, b \in \mathbf{F}_q$ and $a^2 + b^2 \neq 0\}$, where $[a,b]$ and $[c,d]$ are identified if one is a nonzero scalar multiple of the other, and where multiplication is defined by*

$$[a,b] \star [c,d] = [ac - bd, ad + bc].$$

*Then $G$ is a cyclic group of order $q - \left(\frac{-1}{q}\right)$, and*

*$q^*$ is a fourth power (respectively square) modulo $p \Leftrightarrow$*

*$[a,b]$ is a fourth power (respectively square) in $G$.*

This is analogous to the Jacobi-Sun law: concrete corollaries for the primes $q = 3, 5, 7, 11, 13$, and $17$ are given in Table 5. For example, let $p = 17341 = 21^2 + 130^2$. Is 11 a quartic residue modulo $p$? Since $p \equiv 1 \pmod 4$,

$$\left(\frac{11}{p}\right) = \left(\frac{p}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1,$$

so 11 is a square mod $p$. (Of course if $-1$ had come out of this calculation, we could stop here. This is why we check the quadratic status of 11 first; from a theoretical standpoint we could skip directly to the application of the Dirichlet-Sun law.) To decide whether 11 is a fourth power, we compute $21/130 \equiv -5 \pmod{11}$, and now Table 5 shows us that

$$\left(\frac{-11}{p}\right)_4 = -1, \text{ and hence } \left(\frac{11}{p}\right)_4 = \left(\frac{-1}{p}\right)_4 \left(\frac{-11}{p}\right)_4 = (-1)(-1) = 1.$$

So 11 *is* a fourth power mod $p$ and in fact $1616^4 \equiv 11 \pmod{17341}$.

Here we must confess that we have taken some license with the name "Dirichlet-Sun Theorem." Dirichlet's original result took a rather different form, viz:

**Dirichlet's Reciprocity Law.** *Let $p$ and $q$ be distinct odd primes, where $p \equiv 1 \pmod 4$ and $\left(\frac{q^*}{p}\right) = 1$. Write $p = a^2 + b^2$, with $a, b > 0$ and $b$ even. If $\sqrt{p} \pmod q$ is chosen so that $b + \sqrt{p} \neq 0$ in $\mathbf{F}_q$, then*

$$\left(\frac{q^*}{p}\right)_4 = \left(\frac{\sqrt{p}(b+\sqrt{p})}{q}\right).$$

*Therefore if $q \equiv 1 \pmod 4$ also, we have*

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{b+\sqrt{p}}{q}\right). \tag{1}$$

Note that the product of rational quartic symbols $\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4$ is defined, since the hypotheses of Theorem Dirichlet's Law imply that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. An equivalent form of (1) was discovered independently by E. Lehmer (Exercise (35)).

There are several other expressions for $\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4$ for primes $p \equiv q \equiv 1 \pmod 4$ with $\left(\frac{p}{q}\right) = 1$. Perhaps the prettiest of all was given by Burde:

**Burde's Rational Reciprocity Law.** *Let $p$ and $q$ be distinct primes congruent to $1 \pmod 4$. Write $p = a^2 + b^2$ and $q = c^2 + d^2$, where $a, b, c, d > 0$ and $2 \mid b, 2 \mid d$. Suppose that $\left(\frac{p}{q}\right) = 1$. Then*

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^{(q-1)/4} \left(\frac{ad-bc}{q}\right).$$

More mysterious is the connection between biquadratic reciprocity and fundamental units in quadratic fields. The next theorem was first discovered by Schönemann and independently rediscovered by both A. Scholz and E. Lehmer:

**Schönemann-Scholz-Lehmer Reciprocity Law.** *Let $p$ and $q$ be distinct primes congruent to $1 \pmod 4$. Write $p = a^2 + b^2$ and $q = c^2 + d^2$, where $a, b, c, d > 0$ and $2 \mid b, 2 \mid c$. Suppose that $\left(\frac{p}{q}\right) = 1$. Then*

$$\left(\frac{\epsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{\epsilon_p}{q}\right),$$

*where $\epsilon_p$ and $\epsilon_q$ are the fundamental units of $\mathbf{Q}(\sqrt{p})$ and $\mathbf{Q}(\sqrt{q})$ respectively.*

Note that there are two choices for $\epsilon_p$ as an element of $\mathbf{Z}/q\mathbf{Z}$, depending on the choice of $\sqrt{p}$ (and similarly for $\epsilon_q$ as an element of $\mathbf{Z}/p\mathbf{Z}$). Part of the theorem is that the stated equalities hold regardless of which roots are chosen.

We will prove Dirichlet's Reciprocity Theorem directly by Dirichlet's original method (with some improvements drawn from Venkov [100]). The Dirichlet-Sun law and the Burde law will be derived as corollaries to this, and the Schönemann-Scholz-Lehmer law will be proven directly by another application of Dirichlet's method.

## 2. The First Proof of Quadratic Reciprocity

Dirichlet's rendition of Gauss's first proof rests on the following version of the reciprocity law for Jacobi symbols:

**Lemma 2.1** (Jacobi's Quadratic Reciprocity Law)**.** *Suppose that the quadratic reciprocity law holds for all pairs of primes less than $x$. Then if $P$ and $Q$ are coprime odd numbers, not both negative, and each of which is composed entirely of primes less than $x$, then*

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}. \tag{2}$$

This follows from the usual argument for Jacobi Reciprocity, since only primes $p \mid PQ$ enter in the proof (2). The Gauss-Dirichlet proof also requires the first supplementary law, i..e, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, which is the simplest consequence of Euler's criterion.

If the law of quadratic reciprocity is false, then there is a pair of primes $p < q$ for which it fails. Let $q$ be minimal with this property. There are now two cases to consider:

(i) We have $q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = -1$. Then we must prove that $\left(\frac{q}{p}\right) = -1$.

(ii) In the second case, either $q \equiv 3 \pmod 4$, or both $q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$. It is possible to choose $\epsilon = \pm 1$ so that $r := \epsilon p$ satisfies $\left(\frac{r}{q}\right) = 1$. In this case it suffices to show that

$$\left(\frac{q}{r}\right) = (-1)^{\frac{q-1}{2}\frac{r-1}{2}}. \tag{3}$$

Indeed, once this is shown, we see

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= \left(\frac{\epsilon}{q}\right)\left(\frac{r}{q}\right)\left(\frac{q}{r}\right) = \left(\frac{\epsilon}{q}\right)(-1)^{\frac{q-1}{2}\frac{r-1}{2}} \\ &= (-1)^{\frac{\epsilon-1}{2}\frac{q-1}{2}}(-1)^{\frac{q-1}{2}\frac{r-1}{2}} = (-1)^{\frac{q-1}{2}\left(\frac{\epsilon-1}{2}+\frac{r-1}{2}\right)} = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}.\end{aligned}$$

*Proof of the second case.* Choose an even root $e$ of the congruence $e^2 \equiv r \pmod q$ with $0 < e < q$. (The two roots of the congruence in this range add to $q$, so one of them is even.) Write

$$e^2 - r = qf. \tag{4}$$

The left hand side is odd, hence so is $f$. Also $f$ is positive. If $f$ were negative, then $r$ would be positive, and hence

$$p = r = e^2 + q(-f) > q;$$

but this contradicts the initial choice of $p$ and $q$. Finally, we also have $f < q$, since

$$qf = e^2 - r \leq (q-1)^2 + (q-1) = (q-1)q.$$

There are two (sub)cases to consider now, according as $r$ divides $f$ or $r$ is prime to $f$. In the latter case (4) implies $r$ is a nonzero square modulo $f$, whence $\left(\frac{r}{f}\right) = 1$. The same equation implies that $\left(\frac{qf}{r}\right) = 1$, and therefore

$$\left(\frac{q}{r}\right) = \left(\frac{f}{r}\right) = \left(\frac{f}{r}\right)\left(\frac{r}{f}\right) = (-1)^{\frac{r-1}{2}\frac{f-1}{2}}. \tag{5}$$

Since $e$ is even, (5) implies $-r \equiv qf \pmod 4$, and hence

$$\frac{-r-1}{2} \equiv \frac{qf-1}{2} \equiv \frac{q-1}{2} + \frac{f-1}{2} \pmod 2.$$

This implies

$$\frac{r-1}{2}\frac{f-1}{2} \equiv -\frac{r-1}{2}\frac{q-1}{2} - \frac{r-1}{2}\frac{r+1}{2} \equiv \frac{r-1}{2}\frac{q-1}{2} \pmod 2,$$

which when inserted in (5) gives (3).

Suppose instead that $r$ divides $f$. Then also $r$ divides $e$. Writing $e = re'$ and $f = rf'$, we obtain from (4) the relation

$$re'^2 - 1 = qf'. \tag{6}$$

Since $re^2 - qf' = 1$, it follows that $r$ and $-f'$ have opposite sign. Thus one of them is positive and the Jacobi Reciprocity Law can be applied to the pair $r, -f'$. Since

$$\left(\frac{qf'}{r}\right) = \left(\frac{re'^2-1}{r}\right) = \left(\frac{-1}{r}\right) \quad \text{and} \quad \left(\frac{r}{f'}\right) = \left(\frac{re'^2}{f'}\right) = \left(\frac{1}{f'}\right) = 1,$$

the Jacobi law shows that

$$\left(\frac{q}{r}\right) = \left(\frac{-f'}{r}\right) = \left(\frac{r}{-f'}\right)(-1)^{\frac{r-1}{2}\frac{-f'-1}{2}} = (-1)^{\frac{r-1}{2}\frac{-f'-1}{2}}. \tag{7}$$

Now $e'$ is even, so $qf' \equiv -1 \pmod 4$ by (7), and $f' \equiv q^2 f' \equiv -q \pmod 4$. It follows that

$$\frac{r-1}{2}\frac{-f'-1}{2} \equiv \frac{r-1}{2}\frac{q-1}{2} \pmod 2,$$

and this when substituted in (7) proves QR for the pair $q$ and $r$ as desired. □

The next lemma is key in demonstrating the first case, and its April 8, 1796 discovery was recorded in a handwritten note made in Gauss's own copy of the *Disquisitiones* (§130). It is key to establishing the first case.

**Lemma 2.2.** *Let $q \equiv 1 \pmod 4$. Then there exists a prime $p < q$ for which $\left(\frac{q}{p}\right) = -1$.*

*Proof.* If $q \equiv 5 \pmod 8$ then this is easy: $\frac{1}{2}(q+1) \equiv 3 \pmod 4$, so must possess a prime divisor $p \equiv 3 \pmod 4$. Then $p < q$ and $q \equiv -1 \pmod p$, hence $\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right) = -1$. So we suppose for the remainder of the argument that $q \equiv 1 \pmod 8$. We claim in this case that $q$ is a quadratic nonresidue of some prime $p < 2\sqrt{q}+1$. Since $q \geq 17$ implies $2\sqrt{q}+1 < q$, the result follows.

If the claim is false, then $\left(\frac{q}{p}\right) = 1$ for every prime $p < 2\sqrt{q}+1$. Since $q \equiv 1 \pmod 8$ also, it follows from Hensel's Lemma and the Chinese Remainder Theorem that $q$ is a square modulo $n$ for every integer $n$ composed of primes less than $2\sqrt{q}+1$. Let $m = \lfloor \sqrt{q} \rfloor$ and choose a positive integer solution $k$ satisfying the congruence

$$q \equiv k^2 \pmod{(2m+1)!}$$

Since

$$\binom{k+m}{2m+1} = \frac{(k+m)(k+m-1)\cdots(k+1)k(k-1)\dots(k-m)}{(2m+1)!}$$

is an integer, it follows that

$$\begin{aligned}0 &\equiv (k+m)(k+m-1)\cdots(k+1)k(k-1)\dots(k-m)\\ &\equiv k(k^2-1)(k^2-2^2)(k^2-3^2)\cdots(k^2-m^2)\\ &\equiv k(q-1^2)(q-2^2)(q-3^2)\cdots(q-m^2) \pmod{(2m+1)!},\end{aligned}$$

and since $k$ is prime to $(2m+1)!$, the expression

$$\frac{1}{m+1}\frac{q-1^2}{(m+1)^2-1^2}\frac{q-2^2}{(m+1)^2-2^2}\cdots\frac{q-m^2}{(m+1)^2-m^2}.$$

represents a positive integer.

But this is impossible: every term in this product is strictly between 0 and 1 since the choice of $m$ implies $(m+1)^2 > q$. □

*Proof for the first case.* By Lemma 2.2 we may choose an auxiliary prime $p' < q$ with $\left(\frac{q}{p'}\right) = -1$. Then necessarily $\left(\frac{p'}{q}\right) = -1$: for the case established above shows that $\left(\frac{p'}{q}\right) = 1 \Rightarrow \left(\frac{q}{p'}\right) = 1$, and the latter is contrary to the choice of $p'$. So to prove the desired relation, viz. $\left(\frac{q}{p}\right) = -1$, it suffices to prove $\left(\frac{q}{pp'}\right) = 1$.

Since $\left(\frac{p}{q}\right) = \left(\frac{p'}{q}\right) = -1$, we have $\left(\frac{pp'}{q}\right) = 1$, and we may choose an even number $0 < e < q$ with $e^2 \equiv pp' \pmod q$. Write

$$e^2 - pp' = qf. \tag{8}$$

The left hand side of (8) odd, so $f$ is odd. Moreover, since the absolute value of the left hand side is less than $q^2$, we also have $|f|$ less than $q$. We now take three (sub)cases, depending on whether $f$ is divisible by none, one or both of $p, p'$.

Suppose first that $f$ is coprime to $pp'$. Then the same is true for $e$, and

$$\left(\frac{q}{pp'}\right) = \left(\frac{qf}{pp'}\right)\left(\frac{f}{pp'}\right) = \left(\frac{e^2}{pp'}\right)\left(\frac{f}{pp'}\right) = (-1)^{\frac{f-1}{2}\frac{pp'-1}{2}}\left(\frac{pp'}{f}\right) = (-1)^{\frac{f-1}{2}\frac{pp'-1}{2}}, \tag{9}$$

since (8) shows that $\left(\frac{pp'}{f}\right) = 1$. Since $e$ is even and $q \equiv 1 \pmod 4$, we have $-pp' \equiv f \pmod 4$, whence

$$\frac{f-1}{2}\frac{pp'-1}{2} \equiv \frac{-pp'-1}{2}\frac{pp'-1}{2} \equiv \frac{pp'+1}{2}\frac{pp'-1}{2} \equiv 0 \pmod 2.$$

Inserting this into (9), we find that $\left(\frac{qq'}{p}\right) = 1$, as we sought to show.

Suppose next that $f$ is divisible by exactly one of $p$ and $p'$. We take the case when $f$ is divisible by $p$, the other case being exactly analogous. Then also $e$ is divisible by $p$, and writing $e = pe'$ and $f = pf'$, equation (8) becomes

$$pe'^2 - p' = qf',$$

and from this we see that $(f', pp') = 1$ and that $p'$ is coprime to $e'$. Now

$$\left(\frac{p}{p'}\right) = \left(\frac{pe'^2}{p'}\right) = \left(\frac{qf'}{p'}\right) = \left(\frac{q}{p'}\right)\left(\frac{f'}{p'}\right) \text{ and } \left(\frac{-p'}{p}\right) = \left(\frac{qf'}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{f'}{p}\right).$$

It follows that

$$\begin{aligned}\left(\frac{q}{pp'}\right) = \left(\frac{q}{p}\right)\left(\frac{q}{p'}\right) &= \left(\frac{-p'}{p}\right)\left(\frac{f'}{p}\right)\left(\frac{p}{p'}\right)\left(\frac{f'}{p'}\right)\\ &= \left(\frac{-p'}{p}\right)\left(\frac{p}{-p'}\right)\left(\frac{f'}{pp'}\right) = (-1)^{\frac{p-1}{2}\frac{-p'-1}{2}}(-1)^{\frac{f'-1}{2}\frac{pp'-1}{2}}\left(\frac{pp'}{f'}\right).\end{aligned}$$

Since $f'$ divides $f$, (8) shows that $\left(\frac{pp'}{f}\right) = 1$. Hence

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{p-1}{2}\frac{-p'-1}{2}+\frac{f'-1}{2}\frac{pp'-1}{2}}.$$

Since $e$ is even and $q \equiv 1 \pmod 4$, we have $f' \equiv -p' \pmod 4$. Therefore

$$\frac{f'-1}{2}\frac{pp'-1}{2} \equiv \frac{-p'-1}{2}\left(\frac{p-1}{2}+\frac{p'-1}{2}\right),$$

and so

$$\frac{p-1}{2}\frac{-p'-1}{2}+\frac{f'-1}{2}\frac{pp'-1}{2} \equiv \frac{-p'-1}{2}\frac{p'-1}{2} \equiv \frac{p'+1}{2}\frac{p'-1}{2} \equiv 0 \pmod 2,$$

so that $\left(\frac{pp'}{q}\right) = 1$ in this case also.

Finally we suppose that both $p$ and $p'$ divide $f$. In this case both $p$ and $p'$ divide $e$ also. Write $e = pp'e'$ and $f = pp'f'$. Equation (8) now implies

$$pp'e'^2 - 1 = qf'.$$

We see from this equation that $(pp', f') = 1$, and so

$$\left(\frac{q}{pp'}\right) = \left(\frac{qf'}{pp'}\right)\left(\frac{f'}{pp'}\right) = \left(\frac{-1}{pp'}\right)\left(\frac{f'}{pp'}\right) = (-1)^{\frac{pp'-1}{2}}\left(\frac{f'}{pp'}\right),$$

$$= (-1)^{\frac{pp'-1}{2}}(-1)^{\frac{pp'-1}{2}\frac{f'-1}{2}}\left(\frac{pp'}{f'}\right) = (-1)^{\frac{pp'-1}{2}+\frac{pp'-1}{2}\frac{f'-1}{2}},$$

using the evaluation $\left(\frac{pp'}{f'}\right) = 1$ which follows from (8). Since $e'$ is even and $q \equiv 1 \pmod 4$, we have $f' \equiv -1 \pmod 4$, hence

$$\frac{pp'-1}{2}+\frac{pp'-1}{2}\frac{f'-1}{2} \equiv \frac{pp'-1}{2} - \frac{pp'-1}{2} \equiv 0 \pmod 2,$$

and once again $\left(\frac{pp'}{q}\right) = 1$. □

## 3. Cyclotomy

> The principles upon which the division of the circle depend, and geometrical divisibility of the same into seventeen parts, etc.

So begins Gauss's mathematical diary, commenced on March 30, 1796, when he was 18-years old. This entry carries more significance for mathematics than a straight reading would suggest: it was his discovery of the constructibility of the regular 17-gon that finally swayed Gauss to choose mathematics over philology, his other early love. There is even a popular legend that Gauss's enthusiasm led him to request that a regular 17-gon be inscribed on his tombstone, but it seems this story is largely apocryphal. (However, a monument with a 17-pointed star on the back of its base proudly stands in Gauss's birthplace of Braunschweig.)

Nowadays cyclotomy (literally "circle-splitting") refers generally to the study of the roots of unity, which Gauss assiduously took up in Section VII of his *Disquisitiones*, the section where he presents the proof of constructibility of the 17-gon and generalizations.

The proof of the Jacobi-Sun Reciprocity law that we give here rests on certain of these preliminary investigations of Gauss. Rather than establish the requisite theorems in isolation, we have chosen to present them in their historical context,

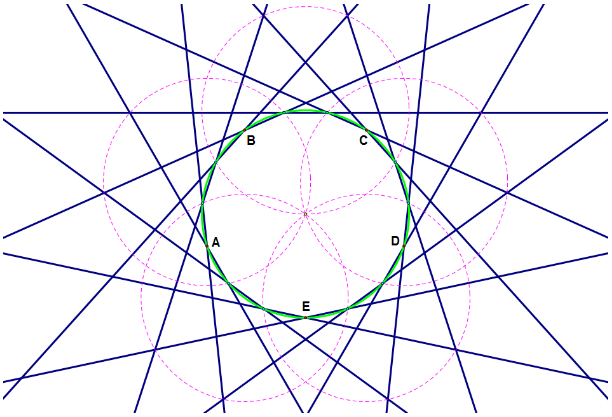


FIGURE 1. A regular 15-gon inscribed in a circle, constructed out of the regular pentagon ABCDE.

and our first goal in this section is to characterize those $n$ for which the regular $n$-gon is constructible.

The rational quartic laws are established by totally different (and more elementary) methods, and readers interested only in those can safely skip to §5.1.

### 3.1. Straightedge & Compass Constructions and the Theorem of Gauss-Wantzel.

To appreciate Gauss's achievement it is necessary to recall the rudiments of straight-edge and compass constructions. (We assume a prior casual acquaintance with these of the type formed in a typical secondary-school geometry course; alternatively, all we need and more can be found in the the book of Courant & Robbins [14, Chapter III, Part I].) We begin with two "constructed points" $O = (0,0)$ and $P = (0,1)$ in the plane $\mathbf{R}^2$. There are now three fundamental constructions we can perform:

(i) Given two constructed points, draw the line between them.
(ii) Given two constructed points, draw the line *segment* between them.
(iii) Given a point and a line segment (both of which assumed to be already constructed), we may draw the circle centered at the given point with radius the length of the given segment.

Each time two distinct lines intersect, or a line and a circle intersect, we add the point(s) of intersection to our set of constructible points. We continue drawing lines and circles and labeling points of intersection as desired.

Euclid's *Elements* [26] contains a thorough investigation into which geometric objects can be constructed in this way (in a finite sequence of steps). Book I, Proposition I is concerned with the construction of "an equilateral triangle on a given finite straight line." Book IV of Euclid's elements contains recipes for the construction of the square, the regular hexagon, the regular pentagon, and the regular 15-gon; moreover, Proposition 30 in Book III can be used to prove that whenever the regular $n$-gon is constructible, so is the regular $2n$-gon. Thus, it has been known since Euclid that the regular $n$-gon is constructible for any

$$n = 2^a 3^b 5^c \quad \text{where} \quad a \geq 0, \quad b = 0 \text{ or } 1, \quad c = 0 \text{ or } 1,$$

where of course the nondegeneracy condition $n \geq 3$ is always understood.

Whether there are other constructible regular polygons remained an open question for 2000 years. The millenia-long silence was broken by the following notice, which appeared in the April 1796 *Allgemeine Literaturzeitung* (see [23, p.28]):

> It is known to every beginner in geometry that various regular polygons, viz., the triangle, tetragon, pentagon, 15-gon and those which arise by the continued doubling of the number of sides of one of them, are geometrically constructible.
>
> One was already that far in the time of Euclid, and, it seems, it has generally been said since then that the field of elementary geometry extends no farther: at least I know of no successful attempt to extend its limits on this side.
>
> So much the more, methinks, does the discovery deserve attention . . . that besides those regular polygons a number of others, e.g., the 17-gon, allow of a geometrical contribution. This discovery is really only a special supplement to a theory of greater inclusiveness, not yet completed, and is to be presented to the public as soon as it has reached its completion.
>
> Carl Friedrich Gauss
> Student of Mathematics at Göttingen

This "theory of greater inclusiveness" appeared five years later in the final section of the *Disquisitiones.* There Gauss claims a complete characterization of the constructible regular polygons:

**Theorem 3.1** (Gauss-Wantzel)**.** *A regular $n$-gon is constructible with straightedge and compass if and only if $n = 2^e p_1 \dots p_k$ for some $e \geq 0$ and distinct Fermat primes $p_1, \dots, p_k$ (where $k \geq 0$).*

Actually the *Disquisitiones* [40, §365] proves only that this condition is sufficient. But there is also an emphatic declaration of necessity:

> Whenever $n-1$ involves prime factors other than 2, we are always led to equations of higher degree . . . We can show with all rigor that these higher-degree equations cannot be avoided in any way nor can they be reduced to lower-degree equations. The limits of the present work exclude this demonstration here . . . (emphasis in original)

Gauss never published his demonstration, and this gap was eventually filled by Wantzel [101].

How can one hope to prove a result like Theorem 3.1? The key is to translate "constructibility" into an algebraic notion. We call the complex number $x + iy$ *constructible* if the point $(x, y) \in \mathbf{R}^2$ is a constructible in finitely many steps. Then one can prove:

**Lemma 3.2.** *The complex number $\alpha$ is constructible if and only if there is a tower of subfields of the complex numbers*

$$\mathbf{Q} := K_0 \subset K_1 \subset \dots K_m$$

*with $\alpha \in K_m$ and $K_i = K_{i-1}(\sqrt{\beta_i})$ for some $\beta_i \in K_{i-1}$ and each $i$. The set of constructible complex numbers form a field under complex addition and multiplication.*

We leave the proof of Lemma 3.2 as Exercise 6. This lemma reduces the proof of the Gauss-Wantzel theorem to an assertion in field theory. To illustrate its power we now show how to quickly dispense with the necessity half of Theorem 3.1. We take for granted the (easy) fact that the constructibility of the $n$-gon is equivalent to the constructibility of an arbitrary primitive $n$th root of unity $\zeta_n$ (Exercise 7) and the fact that the cyclotomic polynomials are always irreducible (see Exercises 13, 14).

**Lemma 3.3.** *If the primitive $n$th root of unity $\zeta_n$ is constructible, then $n$ has the form given in the Gauss-Wantzel Theorem. Also, $\zeta_{2^m}$ is constructible for every $m$ and every choice of a primitive $2^m$th root of unity.*

*Proof.* Suppose $\zeta_n$ is constructible, and let $K_0 \subset \cdots \subset K_m$ be a tower of fields verifying the definition of constructibility for $\zeta_n$. Then the irreducibility of the cyclotomic polynomial $\Phi_n(x)$ implies

$$[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \phi(n) \mid [K_m : \mathbf{Q}] = [K_m : K_{m-1}][K_{m-1} : K_{m-2}] \cdots [K_1 : K_0] = 2^r,$$

say, where $r \geq 0$. Hence $\phi(n)$ is a power of 2, and it is easy to show (Exercise 15) that this forces $n$ to be of the form described in Theorem 3.1.

The final claim of the lemma follows easily by induction: $1 = \zeta_{2^0}$ is constructible. If all the $2^{m-1}$th primitive roots of unity are constructible, then so is an arbitrary $2^m$th root of unity $\zeta_{2^m}$, since $(\zeta_{2^m})^2$ is primitive of order $2^{m-1}$. □

We can reduce the remaining portion of the Gauss-Wantzel result to the following theorem:

**Theorem 3.4** (Gauss). *Let $p$ be a Fermat prime, and let $\zeta_p$ be a primitive $p$th root of unity. Then $\zeta_p$ is constructible.*

For suppose Theorem 3.4 is proven. Let $n := 2^e p_1 \ldots p_k$ be as in the theorem statement. Since the constructible numbers form a field, it follows that $\zeta_{2^e}\zeta_{p_1} \ldots \zeta_{p_r}$ is constructible (for any choices of the primitive roots of unity in question). But $\zeta_{2^e}\zeta_{p_1} \ldots \zeta_{p_r}$ is a primitive $n$th root of unity, and as remarked above, the constructibility of a primitive $n$th root of unity implies the constructibility of the regular $n$-gon.

Below we will give a proof of Theorem 3.4 in the spirit of Gauss. For this it is first necessary to investigate the arithmetic of $\mathbf{Z}[\zeta_p]$.

### 3.2. Much Ado About $\mathbf{Z}[\zeta_p]$.

Let $p$ be any prime, and let $\zeta = \zeta_p$ be a complex primitive $p$th root of unity. The ring $\mathbf{Z}[\zeta]$ is a famous one in algebraic number theory, being the ring of integers of the cyclotomic field $\mathbf{Q}(\zeta_p)$, and the subject of Kummer's deep investigations concerning higher reciprocity laws and Fermat's last theorem.

The properties of $\mathbf{Z}[\zeta]$ which we require lie much closer to the surface, and this permits us develop what we need from scratch without assuming any results from either the theory of algebraic numbers or Galois theory.

**Lemma 3.5** (An Integral Basis). *Every element of $\mathbf{Z}[\zeta]$ (respectively $\mathbf{Q}(\zeta)$) can be expressed uniquely in the form $a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1}$, with integral (respectively rational) $a_i$.*

*Proof.* We prove the claim for $\mathbf{Z}[\zeta]$; the proof for $\mathbf{Q}(\zeta)$ (which $= \mathbf{Q}[\zeta]$) is similar.

*Existence*: Since $\zeta$ is a primitive $p$th root of unity, it is a root of the cyclotomic polynomial

$$\Phi_p(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Substituting $\zeta$ for $x$ yields

$$\zeta^{p-1} = -1 - \zeta - \zeta^2 - \cdots - \zeta^{p-2}, \tag{10}$$

so that every power of $\zeta$ is an integral linear combination of $1, \zeta, \ldots, \zeta^{p-2}$. This implies the same for every element of $\mathbf{Z}[\zeta]$. But (10) allows us to replace 1 by an integral linear combination of $\zeta, \zeta^2, \ldots, \zeta^{p-1}$, and the existence of a representation of the stated form follows.

*Uniqueness* (cf. [40, Art. 341, end of Art. 346]): we deduce this from the irreducibility of $\Phi_p(x)$. This irreducibility follows from the Eisenstein-Schönemann criterion:

$$\Phi_p(x+1) = \frac{1}{x}\left((x+1)^p - 1\right) = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k$$

is a monic polynomial all of whose non-leading coefficients are divisible by $p$, and whose constant coefficient is equal to $p$. Hence $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ are $\mathbf{Q}$-linearly independent, and so are $\zeta \cdot 1, \zeta \cdot \zeta, \ldots, \zeta \cdot \zeta^{p-2}$. □

*Remark.* Gauss's original proof of the irreducibility of $\Phi_p(x)$ [40, Art. 341] is more involved; one version is sketched in Exercise 12. Exercises 13 and 14 describe how to prove the irreducibility of $\Phi_n(x)$ for all $n$.

**Lemma 3.6.** *Suppose $\alpha \in \mathbf{Z}[\zeta] \cap \mathbf{Q}$. Then $\alpha \in \mathbf{Z}$. That is, the only rational elements of $\mathbf{Z}[\zeta]$ are the rational integers.*

*Proof.* Since $\alpha \in \mathbf{Z}[\zeta]$, we can write $\alpha = a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$ uniquely determined integers $a_i$. Since $1, \zeta, \ldots, \zeta^{p-1}$ are a basis field for the field extension $\mathbf{Q}(\zeta)/\mathbf{Q}$, it follows from $\alpha \in \mathbf{Q}$ that $\alpha = a_0 \in \mathbf{Z}$. □

The next two lemmas describe the Galois theory of the extension $\mathbf{Q}(\zeta_p)/\mathbf{Q}$:

**Lemma 3.7** (Description of the automorphisms of $\mathbf{Q}(\zeta)/\mathbf{Q}$)**.** *For each $a \in (\mathbf{Z}/p\mathbf{Z})^*$, there is an automorphism $\sigma_a$ of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$ sending $\zeta \mapsto \zeta^a$. Moreover, every such automorphism is of this form. Consequently,* $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ *can be identified with* $(\mathbf{Z}/p\mathbf{Z})^*$.

*Proof.* The automorphisms of $\mathbf{Q}(\zeta_p)$ are determined by where they send $\zeta_p$. The possible images are the roots of $\Phi_p$, which are precisely $\zeta_p^a$ for $(a,p) = 1$. So for each $(a,p) = 1$, there is an automorphism $\sigma_a$ with $\zeta \mapsto \zeta^a$, and these exhaust the automorphisms.

Note that

$$\sigma_a \circ \sigma_{a'}(\zeta) = \sigma_a(\zeta^{a'}) = \zeta^{aa'} = \sigma_{aa'}(\zeta),$$

and hence the map $a \mapsto \sigma_a$ is an isomorphism between $(\mathbf{Z}/p\mathbf{Z})^*$ and the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. □

**Lemma 3.8** (Description of the fixed fields; cf. [40, Art. 347])**.** *Let $H$ be a subgroup of $(\mathbf{Z}/p\mathbf{Z})^*$; then $H$ is the set of $e$th powers for a uniquely defined $e$ dividing $p-1$. Write $p - 1 = ef$.*

*Let $g$ be a fixed generator of $(\mathbf{Z}/p\mathbf{Z})^*$. Then the set of elements of $\mathbf{Q}(\zeta)$ (respectively $\mathbf{Z}[\zeta]$) fixed by $\sigma_a$ for every $a \in H$ is precisely the set of $\mathbf{Q}$-linear (resp. $\mathbf{Z}$-linear) combinations of $\eta_1, \ldots, \eta_e$, where*

$$\eta_i = \zeta_p^{g^i} + \zeta_p^{g^{e+i}} + \zeta_p^{g^{2e+i}} + \cdots + \zeta_p^{g^{e(f-1)+i}} = \sum_{m=0}^{f-1} \zeta_p^{g^{em+i}}. \tag{11}$$

Following Gauss, we refer to the numbers $\eta_1, \ldots, \eta_e$ as the *$f$-nomial periods* (associated to this prime $p$ and this choice of a generator $g$). Note that the complex numbers $\eta_1, \ldots, \eta_e$ are distinct because of Lemma 3.5. It is convenient to define $\eta_i$ for all $i$ by (11); then the $\eta_i$ are periodic in $i$ with (exact) period $e$.

*Proof.* That $H$ is the set of $e$th powers for some $e \mid p-1$ follows directly from $(\mathbf{Z}/p\mathbf{Z})^*$ being a cyclic group of order $p-1$. Since $g$ is a generator of $(\mathbf{Z}/p\mathbf{Z})^*$, may write $H = \langle g^e \rangle$. Thus an element of $\mathbf{Q}(\zeta)$ is fixed by everything in $H$ once it is fixed by the single automorphism $\sigma_{g^e}$.

Suppose $\alpha$ is fixed by $\sigma_{g^e}$. Write $\alpha = \sum_{i=1}^{p-1} c_i \zeta^{g^i}$, and extend the indices on the $c_i$ cyclically with period $p-1$ (i.e., set $c_i := c_{i \pmod{p-1}}$ for all $i$). Lemma 3.5 implies that $\alpha$ is fixed by $\sigma_{g^e}$ if and only if $c_i = c_{i+e}$ for all $i$. But that implies

$$\alpha = c_1(\zeta^g + \zeta^{g^{2e+1}} + \cdots + \zeta^{g^{(f-1)e+1}}) + c_2(\zeta^{g^2} + \zeta^{g^{e+2}} + \cdots + \zeta^{g^{(f-1)e+2}}) + \\ \cdots + c_e(\zeta^{g^e} + \zeta^{g^{2e}} + \cdots + \zeta^{g^{ef}}) = c_1\eta_1 + c_2\eta_2 + \cdots + c_e\eta_e$$

is a linear combination of the $\eta_i$, as claimed.

The converse is clear, since the individual $\eta_i$ are clearly all fixed by $\sigma_{g^e}$. □

As an easy corollary, we note:

**Corollary 3.9.** *Let $\alpha$ be an element of $\mathbf{Z}[\zeta]$ and suppose that $\sigma_a(\alpha) = \alpha$ for every $a \in \mathbf{Z}/p\mathbf{Z}^*$. Then $\alpha$ is a rational integer.*

*Proof.* We apply the lemma with $H = (\mathbf{Z}/p\mathbf{Z})^*$ (and hence $e = 1$, $f = 16$) to obtain that $\alpha$ is a $\mathbf{Z}$-linear combination of the 16-nomial period

$$\eta_1 = \sum_{m=0}^{p-2} \zeta_p^{g^{m+1}} = \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = -1.$$ □

3.3. **Proof of Theorem 3.4.** Now suppose $p$ is a Fermat prime, so that $p-1 = 2^n$ for some positive integer $n$. Let $g$ be a fixed generator of $(\mathbf{Z}/p\mathbf{Z})^*$, and write down the $2^n$-nomial period

$$\zeta^{g^0} + \zeta^{g^1} + \cdots + \zeta^{g^{p-2}}. \tag{12}$$

We split this into two $2^{n-1}$-nomial periods by taking every other term,

$$\zeta^{g^0} + \zeta^{g^2} + \zeta^{g^4} + \cdots + \zeta^{g^{p-1}}, \quad \zeta^{g^1} + \zeta^{g^3} + \zeta^{g^5} + \cdots + \zeta^{g^{p-2}} \tag{13}$$

Each of these then splits into two $2^{n-1}$-nomial periods in the same manner. Continuing in this way we eventually reach a level with $2^n$ 1-nomial periods (which are simply the individual $2^n$ primitive $p$th roots of unity).

To codify this process, we let $(2^n, g^0)$ denote the $2^n$-nomial period (12), let $(2^{n-1}, g^0)$ and $(2^{n-1}, g^1)$ denote the first and second $2^{n-1}$-nomial periods indicated in (13), and in general let $(f, j)$ denote the $f$-nomial period containing $\zeta^j$ (which in our old notation – where $f$ was suppressed – can be denoted by $\eta_{\mathrm{ind}_g j}$).

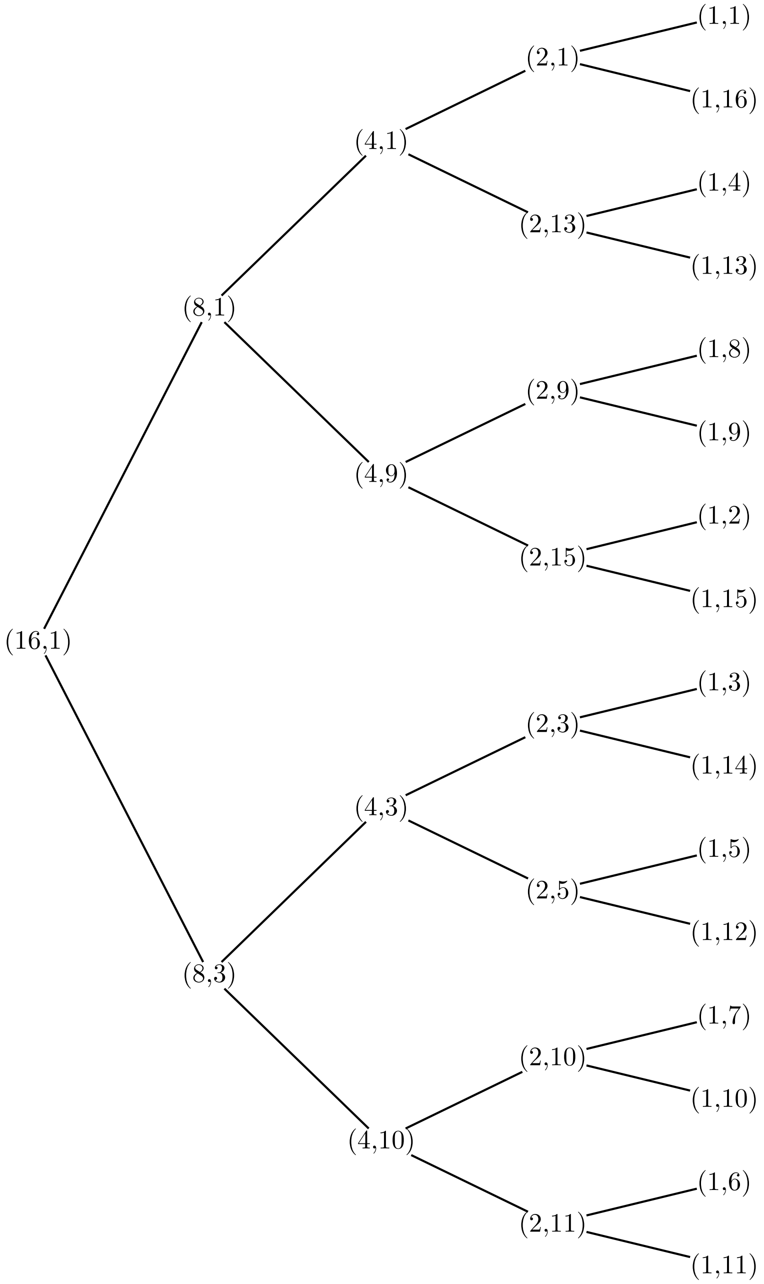
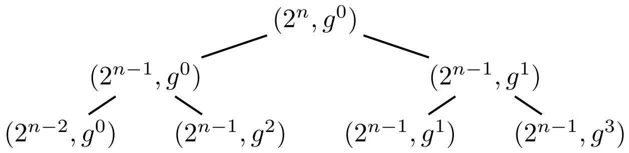


FIGURE 2. Gauss [40, Art. 354]: Binary tree illustrating (for $p = 17$, $g = 3$) the decomposition of the 16-nomial period $\zeta^1 + \zeta^3 + \zeta^9 + \zeta^{10} + \cdots + \zeta^2 + \zeta^6$ into successive half-periods. This can be verified with the following table of powers of 3 (mod 17):

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $3^n$ mod 17 | 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 |

Splitting up the period (12) as above yields a binary tree whose first few rows are shown in the following diagram. Here each period is the sum of the two periods from the nodes immediately below:



In general, $(2^{n-r}, g^k)$ branches off (if $r < n$) to yield the two periods $(2^{n-r-1}, g^k)$ and $(2^{n-r-1}, g^{k+2^r})$. Moreover, the $2^r$ periods of the $r$th row (numbered starting with $r = 0$) are a complete list $2^r$ $2^{n-r}$-nomial periods. To see this, let $f = 2^{n-r}$. Then there are $(p-1)/f = e = 2^r$ distinct periods $\eta_0, \dots, \eta_{e-1}$. But the $r$th row contains $2^r$ distinct $2^{n-r}$-nomial periods by construction (each constructed period is distinct from the others by Lemma 3.5). The claim follows.

We can now prove Gauss's result that $\zeta_p$ is constructible:

*Proof of Theorem 3.4.* Certainly the (unique) $2^n$-nomial period is constructible, being just $\zeta + \cdots + \zeta^{p-2} + \zeta^{p-1} = -1$.

Suppose now that every period in the $r$th row (i.e., every $2^{n-r}$-nomial period) is constructible, for a certain $0 \leq r < n$. Choose a node in the $r$th row, say $(2^{n-r}, g^k)$, and consider the polynomial

$$\phi_r(x) = (x - (2^{n-(r+1)}, g^k))(x - (2^{n-(r+1)}, g^{k+2^r}))$$

whose roots are the periods beneath this node. Since $\sigma_{g^{2^r}}\left((2^{n-(r+1)}, g^k)\right) = (2^{n-(r+1)}, g^{k+2^r})$ and

$$\sigma_{g^{2^r}}((2^{n-(r+1)}, g^{k+2^r})) = (2^{n-(r+1)}, g^{k+2^{r+1}}) = (2^{n-(r+1)}, g^k),$$

the automorphism $\sigma_{g^{2^r}}$ permutes the above factors, so leaves the coefficients of $\phi_r$ fixed. It follows from Lemma 3.8 (with $e = 2^r, f = 2^{n-r}$) that the coefficients of $\phi_r$ are integral-linear combinations of the $2^{n-r}$-nomial periods. In particular, they are constructible by the induction hypothesis.

Therefore the roots of $\phi_r$ can be expessed by the quadratic formula in terms of constructible numbers. Since the constructible numbers form a field closed under the taking of square roots, it follows that $(2^{n-(r+1)}, g^k)$ and $(2^{n-(r+1)}, g^{k+2^r})$ are both constructible. Doing this for each node in the $r$th row, we obtain the constructibility of all the periods in the $(r+1)$th row.

The result now follows by induction, since the individual primitive $p$th roots of unity are the ($2^0$-nomial) periods of the $n$th row. □

A detailed treatment of the case $p = 17$ is the subject of Exercise 8.

3.4. **Period Polynomials and Kummer's Criterion.** The relevance of cyclotomy for our investigations of higher reciprocity laws comes through the remarkable properties of Gauss's period polynomials.

If $p \equiv 1 \pmod{e}$ be a prime, then the *period polynomial* $\phi(x)$ *of degree* $e$ is defined by

$$\phi(x) := (x - \eta_0)(x - \eta_1) \cdots (x - \eta_{e-1}) \in \mathbf{C}[x],$$

and *the reduced period polynomial* $\hat{\phi}(x)$ *of degree* $e$ is defined by

$$\hat{\phi}(x) := (x - (e\eta_0 + 1))(x - (e\eta_1 + 1) \cdots (x - (e\eta_{e-1} + 1)),$$

where the $\eta_i$ are the $f$-nomial periods (and as usual $p = ef + 1$). Note that since the choice of a generator $g$ of $(\mathbf{Z}/p\mathbf{Z})^*$ only impacts the order of the $\eta_i$, both $\phi$ and $\hat{\phi}$ are well-defined independent of any particular such choice.

At this point $\phi$ is as natural to introduce as the Gaussian periods themselves. But what is $\hat{\phi}$? We can describe $\hat{\phi}$ by describing its roots: they are

$$e\eta_0 + 1 = 1 + e\sum_{m=0}^{f-1} \zeta^{g^{em}} = 1 + e \sum_{\substack{\beta \text{ an eth power} \\ \text{in } (\mathbf{Z}/p\mathbf{Z})^*}} \zeta^{\beta} = \sum_{\alpha \in \mathbf{Z}/p\mathbf{Z}} \zeta^{\alpha^e}.$$

and its conjugates (obtained by applying the $\sigma_a$). These roots are examples of "Gauss sums of order $e$," which are interesting in their own right. For us, however, the importance of $\hat{\phi}$ rests in the observation that

$$\begin{aligned}\sum_i (e\eta_i + 1) &= e\sum \eta_i + e \\ &= e(1 + \zeta + \cdots + \zeta^{p-1}) + e = -e + e = 0,\end{aligned}$$

so that the next-to-leading coefficient in $\hat{\phi}$ automatically vanishes. This makes $\hat{\phi}$ a simpler object to work with.

We next prove that $\phi$ and $\hat{\phi}$, which a priori have complex coefficients, in fact have integer coefficients and are irreducible over the rationals:

**Theorem 3.10.** *The period polynomial* $\phi(x)$ *has integer coefficients and is irreducible over the rationals. The same holds for* $\hat{\phi}$.

Of course this agrees with what we already know about the cyclotomic polynomial (which corresponds to $\phi$ upon taking $e = p - 1, f = 1$). We shall compute the period polynomials and reduced period polynomials of degree 2 and 3 below.

*Proof.* It suffices to prove the statements for $\phi$ owing to the relation

$$\hat{\phi} = \prod_{i=0}^{e-1} (x - (e\eta_i + 1)) = e^e \prod_{i=0}^{e-1} \left(\frac{x-1}{e} - \eta_i\right) = e^e \phi((x-1)/e). \tag{14}$$

The coefficients of $\phi(x)$ are clearly elements of $\mathbf{Z}[\zeta]$, so by Corollary 3.9 we need only check that its coefficients are fixed by every $\sigma_a$. Fix a generator $g$ of $(\mathbf{Z}/p\mathbf{Z})^*$. If the index of $a$ with respect to $g$ is congruent to $i \pmod e$, then $\sigma_a(\eta_j) = \eta_{i+j}$. Extend $\sigma_a$ to an automorphism of $\mathbf{Z}[\zeta][x]$ by letting $\sigma_a$ act on coefficients. Then

$$\sigma_a(g(x)) = \sigma_a\left(\prod_{j=0}^{e-1}(x - \eta_j)\right) = \prod_{j=0}^{e-1}(x - \sigma_a(\eta_j)) = \prod_{j=0}^{e-1}(x - \eta_{i+j}) = g(x),$$

since $i + j$ runs through a complete residue system modulo $e$ as $j$ does. This proves that $g$ has integer coefficients.

Irreducibility is easy: if $\pi$ is a polynomial over the rationals which vanishes at $\eta_0$, then repeatedly applying the automorphism $\sigma_g$ we see it also vanishes at $\eta_1, \eta_2, \ldots$, hence (since the $\eta_i$ are distinct) must be divisible by $\phi$. This implies that $\phi$ generates the ideal of polynomials in $\mathbf{Q}[x]$ which vanish at $\eta_0$; this is a prime ideal, hence $\phi$ itself is prime. □

The next theorem, which can itself be viewed as a reciprocity law, provides the link between period polynomials and the study of higher reciprocity. We have attributed it to Kummer, but it seems Gauss from an early version of the *Disquisitiones* that it was also known to Gauss (cf. [35, Art. 367]):

**Theorem 3.11** (Kummer's Criterion). *Let $p = ef + 1$ be prime, and let $\phi$ be the period equation of degree $e$. Let $q$ be a prime distinct from $p$.*

(i) *If $q$ is an $e$th power modulo $p$, then the polynomial $\phi(x)$ has a root mod $q$.*
(ii) *Conversely, if $q$ is a prime not dividing the discriminant of $g$ for which $\phi$ has a root mod $q$, then $q$ is an $e$th power residue mod $p$.*
(iii) *Suppose moreover that $e$ is prime. Then every $q$ dividing the discriminant of $\phi$ is an $e$th power residue of $p$.*

Statements (i)-(iii) yield for prime $e$ the following elegant and uniform corollary:

**Corollary 3.12.** *With notation as in Theorem 3.11, $q$ is an $e$th power residue modulo $p$ if and only if $\phi$ has a root modulo $q$.*

Before proving Theorem 3.11, we establish the following simple auxiliary result:

**Lemma 3.13.** *Suppose that $\eta_i \equiv \eta_j \pmod{q}$, where the congruence is in the ring $\mathbf{Z}[\zeta]$. Then $i \equiv j \pmod{e}$.*

*Proof.* If $\eta_i \equiv \eta_j \pmod{q}$ then $q$ divides $\eta_i - \eta_j$. Lemma 3.5 then implies that $q$ divides every coefficient of $\eta_i - \eta_j$ when both are expressed as integral linear combinations of $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. But referring to the definition of the $\eta_i$ shows that this is only possible when $\eta_i = \eta_j$, i.e., when $i \equiv j \pmod{e}$. □

*Proof of Theorem 3.11 (Kummer* [58]*).* We work modulo $q$ in the ring $\mathbf{Z}[\zeta]$. Write $q \equiv g^r \pmod{p}$, where $g$ is a fixed generator of $(\mathbf{Z}/p\mathbf{Z})^*$, and assume that the periods are numbered so that (11) holds. From the binomial theorem,

$$\eta_k^q = \left(\sum_{m=0}^{f-1} \zeta_p^{g^{em+k}}\right)^q \equiv \sum_{m=0}^{f-1} \zeta_p^{g^{em+k+r}} = \eta_{k+r} \pmod{q}.$$

Since $y^q - y = \prod_{i=0}^{q-1}(y-i)$ is an identity in every ring of characteristic $q$, we have for every integer $n$ the congruence

$$\begin{aligned}(n-\eta_k)(n-\eta_k-1)\cdots(n-\eta_k-(q-1)) &\equiv (n-\eta_k)^q - (n-\eta_k)\\ &\equiv \eta_k^q - \eta_k \equiv \eta_{k+r} - \eta_k \pmod{q}.\end{aligned}$$

Multiplying over $k = 0, 1, \ldots, e-1$, we obtain

$$\phi(n)\phi(n-1)\cdots\phi(n-(q-1)) \equiv \prod_{k=0}^{e-1}(\eta_{k+r} - \eta_k) \pmod{q}. \tag{15}$$

In the case where $q$ is an $e$th power modulo $p$, we have $\eta_{k+r} = \eta_k$ for each $k$, and hence $q$ divides $\phi(n)\ldots\phi(n-(q-1))$ in $\mathbf{Z}[\zeta]$. By Lemma 3.6, this divisibility also holds in the ring of integers. Since $q$ is prime in $\mathbf{Z}$, it follows that $q$ divides (over the integers) some value of $\phi$, which is the assertion of (i).

The congruence (15) also yields a quick proof of (ii): If $q \mid \phi(n)$ and $q$ is not an $e$th power residue mod $p$, then $e \nmid r$. Hence, definining

$$P_j := \prod_{k=0}^{e-1}(\eta_{k+r} - \eta_k), \quad \text{we have} \quad q \mid P_r \mid \prod_{j=1}^{e-1} P_j = \mathrm{Disc}(\phi)$$

in $\mathbf{Z}[\zeta]$. As above, this divisibility holds also in $\mathbf{Z}$, and this proves (b).

We now prove (iii). We suppose $q$ divides the discriminant of $\phi$ and show that in this case $e \mid r$, so that $q \equiv g^r$ must be an $e$th power residue.

Suppose instead that $e \nmid r$. Then $r$ is prime to $e$, since $e$ is a rational prime by hypothesis. Now the $P_j$ are rational integers, since they are fixed by every automorphism $\sigma_a$, and since $\mathrm{Disc}(\phi) = \prod_{1\le j\le e-1} P_j$, we can choose an index $j$, $1 \le j \le e-1$, for which $q \mid P_j$. Since $r$ is prime to $e$ we can also choose $m$ with $j \equiv mr \pmod{e}$. Then

$$\begin{aligned}(\eta_0-\eta_j)^{\frac{q^e-1}{q-1}} = \prod_{i=0}^{e-1}(\eta_0-\eta_{mr})^{q^i} &\equiv \prod_{i=0}^{e-1}(\eta_{ir}-\eta_{j+ir}) \\ &\equiv \prod_{i=0}^{e-1}(\eta_i-\eta_{i+j}) \equiv P_j \pmod{q},\end{aligned}$$

using once more that $r$ is prime to $e$. Since $q \mid P_j$, it follows that

$$q \mid (\eta_0-\eta_k)^{\frac{q^e-1}{q-1}} \mid (\eta_0-\eta_k)^{q^e},$$

and so

$$0 \equiv (\eta_0-\eta_k)^{q^e} \equiv \eta_{0+re}-\eta_{k+re} \equiv \eta_0-\eta_k \pmod{q},$$

so that $\eta_0 \equiv \eta_k \pmod{e}$. But this impossible by Lemma 3.13. □

### 3.5. Quadratic Reciprocity Revisited.

We present another proof of QR in order to illustrate the connection Kummer's criterion establishes between period equations and reciprocity.

Let $p$ be an odd prime. Then $p-1$ is even, hence it makes sense to consider the period polynomial of degree 2. To apply Kummer's criterion we need to determine its coefficients explicitly:

**Theorem 3.14.** *Let $p = 2f+1$ be prime. The corresponding period polynomial of degree 2 is given by*

$$x^2 + x + \frac{1-p^*}{4}.$$

*The reduced period polynomial of degree 2 is given simply by $x^2 - p^*$. (Here, as always, $p^* = (-1)^{(p-1)/2}p$.)*

The computation implicit in this theorem will be facilitated by means of the following lemma, which allows us to simplify any product of two $f$-nomial periods (with $p = ef+1$ as always). Before introducing this, we have to introduce the *cyclotomic numbers.* Fix a generator $g$ of $(\mathbf{Z}/p\mathbf{Z})^*$. Then the cyclotomic numbers are defined for every pair of integers $i$ and $j$ by

$$(16)\quad (i,j) := \\ \#\{\alpha \in \mathbf{F}_p : \alpha \ne 0 \text{ or } -1, \mathrm{ind}_g\alpha \equiv i \mod e \text{ and } \mathrm{ind}_g(\alpha+1) \equiv j \mod e\}.$$

Of course $i$ and $j$ here really only matter modulo $e$. (In our contexts there will be no danger of confusing this symbol with that used to identify the periods of Fermat primes in the preceding section.)

**Lemma 3.15.** *Let $p = ef+1$ be prime, and define the $f$-nomial periods as before. Let $g$ be a generator of $(\mathbf{Z}/p\mathbf{Z})^*$, and assume that both the $f$-nomial periods and* *the cyclotomic numbers are defined with respect to this generator. Then we have for every $i$ and $j$,*

$$\eta_i\eta_{i+j} = \sum_{m=0}^{e-1}(j,m)\eta_{i+m} + \begin{cases} f & \text{if } j \equiv ef/2 \pmod{e}, \\ 0 & \text{otherwise.}\end{cases} \tag{17}$$

*Proof.* We have

$$\begin{aligned}\eta_i\eta_{i+j} &= \sum_{m=0}^{f-1}\zeta^{g^{em+i}}\sum_{n=0}^{f-1}\zeta^{g^{en+i+j}} = \sum_{m=0}^{f-1}\sum_{n=0}^{f-1}\zeta^{g^{em+i}(1+g^{e(n-m)+j})} \\ &= \sum_{m=0}^{f-1}\sum_{n=0}^{f-1}\zeta^{g^{em+i}(1+g^{en+j})} = \sum_{n=0}^{f-1}\sum_{m=0}^{f-1}\zeta^{g^{em+i}(1+g^{en+j})},\end{aligned}$$

where we use in the transition from the first line to the second that $n-m$ runs over a complete residue system modulo $f$ as $n$ does (for fixed $m$).

Suppose $n$ is such that $\mathrm{ind}_g(1+g^{en+j}) \equiv r \pmod{e}$. Then the inner sum over $m$ (for this $n$) is $\eta_{i+r}$. The number of values of $n$ with $0 \le n \le f-1$ for which $\mathrm{ind}_g(1+g^{en+j}) \equiv r \pmod{e}$ is the cyclotomic number $(j,r)$. Adding the contributions from all classes $r = 0, 1, \ldots, e-1$ gives the main term in (17).

The secondary term comes from the (unique if it exists) value $n$, $0 \le n \le f-1$, for which $1+g^{en+j} \equiv 0 \pmod{p}$; this term appears if and only if $(p-1)/2 = ef \equiv j \pmod{e}$. □

*Proof of Theorem 3.14.* We easily have

$$\begin{aligned}\eta_0+\eta_1 &= \left(\zeta^{g^0}+\zeta^{g^2}+\cdots+\zeta^{g^{p-1}}\right)+\left(\zeta^{g^1}+\zeta^{g^3}+\cdots+\zeta^{g^{p-2}}\right) \\ &= \sum_{a\in(\mathbf{Z}/p\mathbf{Z})^*}\zeta^a = -\zeta^0 = -1,\end{aligned}$$

so our task is reduced to computing $\eta_0\eta_1$.

By Lemma 3.15 with $e = 2$ and $f = (p-1)/2$,

$$\eta_0\eta_1 = (1,0)\eta_0 + (1,1)\eta_1 + \begin{cases} f & \text{if } f \text{ is odd,} \\ 0 & \text{if } f \text{ is even.}\end{cases}$$

The automorphism $\sigma_g$ interchanges $\eta_0$ and $\eta_1$ and hence leaves $\eta_0\eta_1$ fixed; from the expression just obtained for $\eta_0\eta_1$ and the observation that $\eta_0$ and $\eta_1$ are linearly independent (which is immediate from Lemma 3.5), we deduce that $(1,0) = (1,1)$. Hence

$$\begin{aligned}2(1,1) = (1,1)+(1,0) &= \#\{\alpha : \alpha \ne 0, -1 \text{ and } \mathrm{ind}_g(\alpha) \equiv 1 \pmod{2}\} \\ &= \#\{\alpha : \alpha \ne 0, -1 : \left(\frac{\alpha}{p}\right) = -1\} = \frac{p-1}{2} - \frac{1-\left(\frac{-1}{p}\right)}{2},\end{aligned}$$

Now if $p \equiv 1 \pmod{4}$ then $f$ is even and hence

$$\begin{aligned}\eta_0\eta_1 &= (1,0)\eta_0 + (1,1)\eta_1 = (\eta_0+\eta_1)(1,1) = -(1,1) \\ &= -\frac{1}{2}\left(\frac{p-1}{2}\right) = \frac{1-p}{4} = \frac{1-p^*}{4},\end{aligned}$$

while if $p \equiv 3 \pmod 4$ we have $f$ odd and

$$\begin{aligned}\eta_0\eta_1 = (1,0)\eta_0 + (1,1)\eta_1 + \frac{p-1}{2} &= -(1,1) - \frac{p-1}{2}\\ &= -\frac{1}{2}\left(\frac{p-3}{2}\right) - \frac{p-1}{2} = \frac{1+p}{4} = \frac{1-p^*}{4}.\end{aligned}$$

This proves the claim about the form of the period polynomial. From this we calculate (from (14)) that the reduced period polynomial is $4\phi(x/2-1/2) = x^2-p^*$, and the theorem is completely proved. □

*Proof of Quadratic Reciprocity.* Let $p$ and $q$ be distinct odd primes. Then $q$ does not divide the discriminant $p^*$ of the period polynomial $x^2+x+\frac{1}{4}(1-p^*)$. By Kummer's criterion (part (i) and (ii)),

$$\begin{aligned}\left(\frac{q}{p}\right) = 1 &\iff x^2+x+\frac{1-p^*}{4} \text{ has a root modulo } q\\ &\iff \mathrm{Disc}\big(x^2+x+\frac{1-p^*}{4}\big) \text{ is a square mod } q \iff \left(\frac{p^*}{q}\right) = 1. \qquad \Box\end{aligned}$$

In the form we have presented it, this proof of quadratic reciprocity most closely resembles the demonstration offered V.A. Lebesgue [66]. However the same ideas can be already found in Gauss's seventh proof [35, Art. 365-366], which was originally intended for publication in the *Disquisitiones*.

Using the same method we can classify the primes for which 2 is a square:

*Proof of the Second Supplementary Law.* Let $p$ be an odd prime. Since $2 \nmid p^*$,

$$\begin{aligned}\left(\frac{2}{p}\right) = 1 &\iff x^2+x+\frac{1-p^*}{4} \text{ has a root mod } 2\\ &\iff \frac{1-p^*}{4} \equiv 0 \pmod 2 \iff p \equiv \pm 1 \pmod 8. \qquad \Box\end{aligned}$$

## 4. The Jacobi-Sun Reciprocity Law

The proof of the Jacobi-Sun law is entirely analogous to the proof of the quadratic reciprocity law offered in §3.5. But each of the corresponding steps is much more difficult: in particular, determining the coefficients of the cubic period polynomial corresponding to a prime $p \equiv 1 \pmod 3$ requires a considerable amount of ingenuity. Here we follow largely Gauss's treatment in [40, Art. 358] (with minor changes in notation). Along the way we will compute the cyclotomic numbers $(i,j)$ of order 3, which will be used to obtain proofs of the rational supplementary laws yielding the cubic residue status of 2 and 3.

But even once one has the cubic period polynomial, it is not obvious how to determine whether it has a root mod $q$; we will tackle this problem by writing down the roots explicitly (in a finite extension of $\mathbf{F}_q$) using Cardano's formulas and then using properties of the $q$th power map to detect when some root lies in $\mathbf{F}_q$.

### 4.1. **Article 358: The Cubic Period Polynomial.**

**Theorem 4.1** (Determination of the Cubic Period Polynomial)**.** *Let $p \equiv 1 \pmod 3$ be prime, say $p = 3f+1$. Write $4p = L^2+27M^2$ with integers $L$ and $M$ and $L \equiv 1$*

(mod 3), *say* $L = 3k - 2$. *Then the cubic period polynomial corresponding to* $p$ *is*

$$x^3 + x^2 - fx - \frac{f + kp}{9}.$$

**Theorem 4.2** (Determination of the Cyclotomic Numbers of Order 3)**.** *The matrix of cyclotomic numbers*

$$\begin{pmatrix} (0,0) & (0,1) & (0,2) \\ (1,0) & (1,1) & (1,2) \\ (2,0) & (2,1) & (2,2) \end{pmatrix} \quad \textit{has the shape} \quad \begin{pmatrix} a & b & c \\ b & c & d \\ c & d & b \end{pmatrix}. \tag{18}$$

*Here* $a, b, c$ *and* $d$ *can be described explicitly as follows: we have*

$$a = \frac{f+k}{3} - 1 \quad \textit{and} \quad d = \frac{f+k}{3}.$$

*We can choose our generator* $g$ *of* $(\mathbf{Z}/p\mathbf{Z})^*$ *so that either of* $b - c = M$ *or* $b - c = -M$ *holds. If* $g$ *is chosen so that* $b - c = M$, *then*

$$b = \frac{M}{2} + \frac{2f - k}{6} \quad \textit{and} \quad c = -\frac{M}{2} + \frac{2f - k}{6}; \tag{19}$$

*otherwise* $b$ *and* $c$ *are interchanged.*

It appears from Gauss's mathematical diary that he discovered these results on October 1, 1796 [45, Entry 39].

We will prove Theorems 4.1 and 4.2 simultaneously. We first recall the following lemma, familiar from the elementary theory of quadratic fields:

**Lemma 4.3.** *Let* $p \equiv 1 \pmod 3$ *be prime. Then there are integers* $L$ *and* $M$, *uniquely determined up to sign, for which* $4p = L^2 + 27M^2$.

We will also require some easy properties of the cubic cyclotomic numbers:

**Lemma 4.4** (Preliminary Observations about the Cubic Cyclotomic Numbers)**.** *Let* $p \equiv 1 \pmod 3$ *and write* $p - 1 = 3f$. *Then the cyclotomic numbers* $(i, j)$ *defined in* (16) *have the following properties:*

(i) *For every pair* $i, j$, *we have* $(i, j) = (j, i)$.
(ii) *We have*
  (a) $(0,0) + (0,1) + (0,2) = f - 1$,
  (b) $(1,0) + (1,1) + (1,2) = f$,
  (c) $(2,0) + (2,1) + (2,2) = f$.

*Proof.* Since $-1$ is a cube in $(\mathbf{Z}/p\mathbf{Z})^*$, the map $\alpha \mapsto -1 - \alpha$ is a bijection between the set counted by $(i, j)$ and that counted by $(j, i)$. This proves (i). To prove (ii), note that

$$(i,0) + (i,1) + (i,2) = \\ \#\{\alpha : \mathrm{ind}_g(\alpha) \equiv i \pmod 3 \text{ and } \mathrm{ind}_g(\alpha + 1) \equiv 0, 1, \text{ or } 2 \pmod 3\}.$$

That is, $(i,0) + (i,1) + (i,2)$ is the number of $\alpha$ with $\mathrm{ind}_g(\alpha) \equiv i \pmod 3$ and $\alpha + 1$ is nonzero. There are $(p-1)/3 = f$ elements $\alpha$ with $\mathrm{ind}_g(\alpha) \equiv i \pmod 3$. If $i \not\equiv 0 \pmod 3$ then for none of these is $\alpha + 1 = 0$. However, if $i \equiv 0 \pmod 3$, then $\alpha = -1$ has index congruent to $i$ mod 3 and $\alpha + 1 = 0$; this explains the anomalous count for $(0,0) + (0,1) + (0,2)$. □

Now onto the proofs. Write the period polynomial $\phi$ in the form

$$x^3 - Ax^2 + Bx - C, \tag{20}$$

where $A = \eta_0 + \eta_1 + \eta_2, B = \eta_0\eta_1 + \eta_1\eta_2 + \eta_0\eta_2$ and $C = \eta_0\eta_1\eta_2$

are the symmetric functions of $\eta_0, \eta_1$ and $\eta_2$. We have

$$A = \eta_0 + \eta_1 + \eta_2 = \sum_{a \in (\mathbf{Z}/p\mathbf{Z})^*} \zeta^a = -\zeta^0 = -1.$$

By Lemma 3.15,

$$\eta_0\eta_1 = (1,0)\eta_0 + (1,1)\eta_1 + (1,2)\eta_2. \tag{21}$$

Applying the automorphism $\sigma_g$ we obtain the two further relations

$$\eta_1\eta_2 = (1,0)\eta_1 + (1,1)\eta_2 + (1,2)\eta_0, \text{ and} \tag{22}$$

$$\eta_2\eta_0 = (1,0)\eta_2 + (1,1)\eta_0 + (1,2)\eta_1. \tag{23}$$

Adding these three equations, we find

$$B = \eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_3 = ((1,0) + (1,1) + (1,2))(\eta_0 + \eta_1 + \eta_2) = -f.$$

Lemma 3.15 also yields

$$\eta_0\eta_2 = (2,0)\eta_0 + (2,1)\eta_1 + (2,2)\eta_2;$$

comparing with (23) shows proves that $(2,0) = (1,1)$ and $(2,2) = (1,0)$. This proves that the matrix of cyclotomic numbers has the form stated in (18). Henceforth we refer to the cyclotomic numbers using by their letter designation.

Since (Lemma 4.4)

$$a + b + c = (00) + (01) + (02) = f - 1 \quad \text{and} \quad b + c + d = f,$$

we obtain the additional relation

$$a = d - 1.$$

From Lemma 3.15 and equations (21), (22), (23), we have

$$\begin{aligned} \eta_0\eta_0 &= f + (d-1)\eta_0 + b\eta_1 + c\eta_2 \\ \eta_0\eta_1 &= b\eta_0 + c\eta_1 + d\eta_2 \\ \eta_0\eta_2 &= c\eta_0 + d\eta_1 + b\eta_2 \\ \eta_1\eta_2 &= d\eta_0 + b\eta_1 + c\eta_2. \end{aligned}$$

Hence

$$\begin{aligned} C = \eta_0 \cdot \eta_1\eta_2 &= d\eta_0^2 + b\eta_0\eta_1 + c\eta_0\eta_2 \\ &= df + (b^2 + c^2 + d^2 - d)\eta_0 + (bd + bc + cd)\eta_1 + (bd + bc + cd)\eta_2. \end{aligned}$$

Now $C$, being a rational integer, is fixed by the automorphism $\sigma_g$. This automorphism takes $\eta_i$ to $\eta_{i+1}$, and so the linear independence of the $\eta_i$ (implied by Lemma 3.5) implies the above coefficients of $\eta_0, \eta_1$ and $\eta_2$ must coincide. That is, we have the important relation

$$b^2 + c^2 + d^2 - d = bd + bc + cd, \tag{24}$$

and hence

$$\begin{aligned} C &= df + (bd + bc + cd)(\eta_0 + \eta_1 + \eta_2) \\ &= d(b + c + d) - (bd + bc + cd) = d^2 - bc. \end{aligned}$$

Now relation (24) can also be written as

$$\begin{aligned} &12d + 12b + 12c + 4 = \\ &\qquad 36d^2 + 36b^2 + 36c^2 - 36bd - 36cd - 36bc - 24d + 12b + 12c + 4, \end{aligned}$$

or, observing that $12(b + c + d) + 4 = 12f + 4 = 4p$, in the very concise form

$$4p = (6d - 3b - 3c - 2)^3 + 27(b - c)^2.$$

But we began by assuming a representation $4p = L^2 + 27M^2$. Since $L$ and $6d - 3b - 3c - 2$ are both 1 (mod 3), it follows from the uniqueness portion of Lemma 4.3 that

$$L = 3k - 2 = 6d - 3b - 3c - 2 \quad \text{and} \quad b - c = \pm M,$$

hence

$$k = 2d - b - c = 3d - f.$$

Hence

$$d = \frac{f + k}{3} \quad \text{and} \quad b + c = m - d = \frac{2f - k}{3}. \tag{25}$$

Consequently,

$$\begin{aligned} C = d^2 - bc &= d^2 - \frac{(b + c)^2}{4} + \frac{(b - c)^2}{4} \\ &= \frac{(f + k)^2}{9} - \frac{(2f - k)^2}{36} + \frac{M^2}{4}. \end{aligned}$$

If we replace $M^2$ by $\frac{1}{27}((12f + 4) - (3k - 2)^2)$, this simplifies to

$$\frac{k(3f + 1) + f}{9} = \frac{f + kp}{9},$$

and this proves Theorem 4.1.

It is now easy to complete the determination of the cyclotomic numbers. First, if we replace the generator $g$ with $g^{-1}$, then $b$ and $c$ interchange roles, so $b - c = \pm M$ can be made to hold for either choice of sign, as was claimed in Theorem 4.2. Next, if $g$ is chosen so that $b - c = M$, then from (25)

$$b + c = \frac{2f - k}{3} \quad \text{while} \quad b - c = M,$$

and solving this system yields (19). Similar considerations apply if $g$ is chosen so that $b - c = -M$. This completes the proof of Theorem 4.2.

We close this section by computing the reduced cubic period polynomial:

**Theorem 4.5.** *Let* $p \equiv 1 \pmod 3$. *Then* $x^3 - 3px - pL$ *is the reduced cubic period polynomial corresponding to* $p$.

*Proof.* By (14) and Theorem 4.1,

$$\hat{\phi}(x) = 3^3\phi(x/3 - 1/3) = x^3 - 3(3f + 1)x + 6f - 3kp + 2.$$

The result now follows since

$$3f + 1 = p \quad \text{and} \quad 6f - 3kp + 2 = -3kp + 2p = p(2 - 3k) = -pL. \qquad \square$$

### 4.2. The Cubic Character of 2 and 3.

**Theorem 4.6** (Cubic Character of 2)**.** *Let $p \equiv 1 \pmod 3$, and write $4p = L^2 + 27M^2$, where $L \equiv 1 \pmod 3$. Suppose $g$ is a primitive root chosen so that $b - c = M$, where $b = (2,2)$ and $c = (1,1)$ are the cyclotomic numbers of the previous section. Then*

$$2 \textit{ is a cube} \iff 2 \mid L \textit{ and } 2 \mid M,$$
$$\operatorname{ind}_g(2) \equiv 1 \pmod 3 \iff 4 \mid L - M,$$
$$\operatorname{ind}_g(2) \equiv 2 \pmod 3 \iff 4 \mid L + M.$$

*In particular, 2 is a cubic residue modulo a prime $p \equiv 1 \pmod 6$ if and only if $p$ can be written in the form $L'^2 + 27M'^2$ for some integers $L'$ and $M'$.*

*Proof.* Let $i$ be an integer and let

$$S := \{\alpha \in \mathbf{F}_p : \alpha \neq 0 \text{ or } -1, \operatorname{ind}_g(\alpha) \equiv i \mod 3 \text{ and } \operatorname{ind}_g(\alpha_1) \equiv i+1 \mod 3\}.$$

Let $\psi$ be the permutation of $S$ defined by $\psi(\alpha) = -1 - \alpha$. Since $(i,i) = \#S$ by definition,

$$(i,i) \text{ is odd} \iff \psi \text{ has a fixed point} \iff \operatorname{ind}_g(1/2) \equiv i \pmod 3 \iff \operatorname{ind}_g(2) \equiv -i \pmod 3. \tag{26}$$

Since $f = (p-1)/3$ is even and $L = 3k - 2 \equiv -k - 2 \pmod 4$, Theorem 4.2 implies

$$(0,0) = a = d - 1 = (f+k)/3 - 1 \equiv k - 1 \equiv L - 1 \pmod 2,$$
$$(1,1) = c, \text{ and } 2c = (2f-k)/3 - M \equiv k - 2f - M \equiv -L - M - 2 \pmod 4,$$
$$(2,2) = b, \text{ and } 2b = M + k - 2f \equiv M - L - 2 \pmod 4.$$

The results now follow from (26): 2 is a cube (i.e., $\operatorname{ind}_g(2) \equiv 0 \pmod 3$) if and only if $(0,0) = L - 1$ is odd, that is, precisely when $2 \mid L$. (Note that in this case $2 \mid M$ also, since $4p = L^2 + 27M^2$ is even.) The other results are proved similarly:

$$\operatorname{ind}_g 2 \equiv 1 \mod 3 \Leftrightarrow (2,2) \text{ is odd} \Leftrightarrow 2(2,2) \equiv 2 \mod 4 \Leftrightarrow M - L \equiv 0 \mod 4,$$
$$\operatorname{ind}_g 2 \equiv 2 \mod 3 \Leftrightarrow (1,1) \text{ is odd} \Leftrightarrow 2(1,1) \equiv 2 \mod 4 \Leftrightarrow M + L \equiv 0 \mod 4. \square$$

**Theorem 4.7** (Cubic Character of 3)**.** *Under the same assumptions of the previous theorem,*

$$3 \textit{ is a cube modulo } p \iff 3 \mid M,$$
$$\operatorname{ind}_g(3) \equiv 1 \pmod 3 \iff M \equiv -1 \pmod 3,$$
$$\operatorname{ind}_g(2) \equiv 2 \pmod 3 \iff M \equiv +1 \pmod 3.$$

*Proof.* We have a bijection between $\mathbf{Z}/p\mathbf{Z}^* \setminus \{-1\}$ and $(\mathbf{Z}/p\mathbf{Z})^* \setminus \{1\}$ given by $\alpha \mapsto (\alpha+1)/\alpha$, with inverse mapping $\beta \mapsto 1/(\beta - 1)$. Then with $g$ our chosen generator and $\omega = g^{(p-1)/3}$, we have

$$1 = -\prod_{\substack{\alpha \in (\mathbf{Z}/p\mathbf{Z})^* \\ \alpha \neq -1}} \frac{\alpha+1}{\alpha} = -\prod_{\substack{\beta \in (\mathbf{Z}/p\mathbf{Z})^* \\ \beta \neq 1}} \beta = \prod_{\substack{\alpha \in (\mathbf{Z}/p\mathbf{Z})^* \\ \alpha \neq -1}} \alpha = \prod_{\substack{\beta \in (\mathbf{Z}/p\mathbf{Z})^* \\ \beta \neq 1}} \frac{1}{\beta - 1}.$$

We decompose the right hand side with respect to the cosets of the subgroup of cubes:

$$\begin{aligned}\prod_{\substack{\beta\in(\mathbf{Z}/p\mathbf{Z})^*\\ \beta\neq 1}} \frac{1}{\beta-1} &= \frac{1}{\omega-1}\frac{1}{\omega^2-1}\prod_{1\neq\gamma\in H}\frac{1}{\gamma-1}\frac{1}{\gamma\omega-1}\frac{1}{\gamma\omega^2-1}\\ &= \frac{1}{1-\omega}\frac{1}{1-\omega^2}\prod_{1\neq\gamma\in H}\frac{1}{\gamma-1}\frac{1}{\gamma-\omega}\frac{1}{\gamma-\omega^2} = \frac{1}{3}\prod_{1\neq\gamma\in H}\frac{1}{\gamma^3-1}.\end{aligned}$$

The elements $\gamma^3-1$ run through all predecessors of cubes except 1. It follows that

$$0 = \mathrm{ind}_g(1) \equiv -\mathrm{ind}_g(3) - \sum_{1\neq\gamma\in H}\mathrm{ind}_g(\gamma^3-1) \pmod{p-1};$$

modulo 3 this gives

$$-\mathrm{ind}_g(3) - 0(0,0) - 1(0,1) - 2(0,2) \equiv 0 \pmod 3,$$

i.e.,

$$\mathrm{ind}_g(3) \equiv -(0,1) - 2(0,2) = -b-2c \equiv c-b = -M \pmod 3,$$

as we sought to show. □

*Remark.* Gauss's first proof of Theorem 4.7 (preserved in [38, pp. 10-11]) is a good deal more intricate; he writes

$$\eta_0^3 = A + B\eta_0 + C\eta_1 + D\eta_2$$

for explicit integers $A, B, C$ and $D$, which are expressed in terms of the quantities appearing §4.1 (and in article 358 of his *Disquisitiones*). Modulo 3, Gauss finds that $A, B, C$ and $D$ are polynomials in $b-c$ (where $b, c$ are the cyclotomic numbers of the previous section) and accordingly he computes the following table:

| $b-c \pmod 3$ | $B \pmod 3$ | $C \pmod 3$ | $D \pmod 3$ |
|---|---|---|---|
| 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 |
| 2 | 0 | 1 | 0 |

So modulo 3, we see that $\eta_0^3 \equiv \eta_0, \eta_2,$ or $\eta_1$ according as $b-c \equiv 0, 1,$ or $2 \pmod 3$. Since $\eta_0^3 \equiv \eta_{\mathrm{ind}_g(3)} \pmod 3$, and since $b-c=M$, Theorem 4.7 follows. The elegant proof presented here seems to have been discovered by Gauss in 1809; on January 6th of that year Gauss made the following entry in his mathematical diary:

> The theorem for the cubic residue 3 is proved with an elegant special method by considering the values of $\frac{x+1}{x}$ where three each always have the values $a, a\epsilon, a\epsilon^2$, with the exception of two which give $\epsilon, \epsilon^2$, but these are
>
> $$\frac{1}{\epsilon-1} = \frac{\epsilon^2-1}{3}, \quad \frac{1}{\epsilon^2-1} = \frac{\epsilon-1}{3}$$
>
> with product $\equiv \frac{1}{3}$.

For many years this comment remained obscure. The reconstruction of Gauss's argument which we have presented here is due to Gröger [46].

### 4.3. Jacobi's Rational Cubic Reciprocity Law.

**Theorem 4.8.** *Let $p$ and $q$ be distinct primes with $p, q > 3$ and $p \equiv 1 \pmod 3$. Write $4p = L^2 + 27M^2$ with $L \equiv 1 \pmod 3$. Then*

$$q \textit{ is a cube in } \mathbf{F}_p \iff \frac{L + 3M\sqrt{-3}}{L - 3M\sqrt{-3}} \textit{ is a cube in } \mathbf{F}_q(\sqrt{-3}).$$

Let $\phi$ (respectively $\hat{\phi}$) be the cubic period polynomial (respectively reduced period polynomial) whose coefficients were determined in §. For the discriminant of $\hat{\phi}$ we have

$$\mathrm{Disc}(\hat{\phi}) = 4(3p)^3 - 27(pL)^2 = 27p^2(4p - L^2) = 3^6 p^2 M^2.$$

But $\mathrm{Disc}(\hat{\phi}) = 3^6 \mathrm{Disc}(\phi)$, so

$$\mathrm{Disc}(\phi) = p^2 M^2.$$

Since $e = 3$ is prime, part (iii) of Kummer's Criterion (Theorem 3.11) yields the following special case of Jacobi's reciprocity law:

**Lemma 4.9.** *Let $p$ and $q$ be distinct primes with $p, q > 3$ and $p \equiv 1 \pmod 3$. Write $4p = L^2 + 27M^2$ with $L \equiv 1 \pmod 3$. If $q$ divides $M$ then $q$ is a cube in $\mathbf{F}_p$.*

For the primes $q > 3$ with $q \nmid pM$, we use Corollary 3.12:

$$q \text{ is a cube modulo } p \iff \phi \text{ has a root mod } q \iff \hat{\phi} \text{ has a root mod } q,$$

the last implication following from (14). To analyze when $\hat{\phi}$ has a root in $\mathbf{F}_q$, we employ the classical solution of the cubic equation. For an alternative derivation of rational cubic reciprocity, see Exercise 33.

**Cardano's Solution of the Cubic.** *Let $f(x) = x^3 + ax - b$ be a cubic polynomial with coefficients in a field $F$ of characteristic $\neq 2, 3$. Suppose also that $a \neq 0$. Then the roots of $f$ in an algebraic closure of $F$ are given by*

$$w + \frac{-a/3}{w}, \quad \textit{where} \quad w^3 = \frac{b}{2} \pm \sqrt{\frac{b^2}{4} + \frac{a^3}{27}},$$

*where $w$ ranges over all six cube roots corresponding to the two choices of sign.*

Applied to our situation we find:

**Corollary 4.10.** *Let $p \equiv 1 \pmod 3$ and let $q > 3$ be a prime not dividing $mP$. Then the roots of the reduced cubic period polynomial $x^3 - 3px - pL$ in an algebraic closure of $\mathbf{F}_q$ can be described by*

$$w + \frac{p}{w}, \quad \textit{where} \quad w^3 = p\frac{L \pm 3M\sqrt{-3}}{2}.$$

Let $w$ be a cube root as above, corresponding to some choice of sign; for the corresponding root we have

$$\begin{aligned} w + p/w \in \mathbf{F}_q &\iff (w + p/w)^q = (w + p/w) \\ &\iff w^q + p/w^q = w + p/w \iff w^q = w \text{ or } w^q = p/w. \end{aligned}$$

The first possibility can only occur if $q \equiv 1 \pmod 3$, and the latter can only occur if $q \equiv 2 \pmod 3$.

**Lemma 4.11.** *Let $p$ and $q$ be distinct primes with $p, q > 3$ and $p \equiv 1 \pmod 3$. Suppose $q \nmid pM$. Suppose the element $w$ in a fixed algebraic closure of $\mathbf{F}_q$ satisfies*

$$w^3 = p\frac{L \pm 3M\sqrt{-3}}{2} \in \mathbf{F}_q(\sqrt{-3}) \tag{27}$$

*for some choice of sign. Then*

$$w^{3q} = w^3 \text{ if and only if } q \equiv 1 \pmod 3,$$

$$\text{while} \quad w^{3q} = p^3/w^3 \text{ if and only if } q \equiv 2 \pmod 3.$$

*Consequently, $w^q = w$ implies $q \equiv 1 \pmod 3$ and $w^q = p/w$ implies $q \equiv 2 \pmod 3$.*

*Proof.* We have

$$w^{3q} = (w^3)^q = p^q\left(\frac{L \pm 3M\sqrt{-3}}{2}\right)^q = p\frac{L \pm 3M\left(\frac{-3}{q}\right)\sqrt{-3}}{2}. \tag{28}$$

As $m \neq 0$ in $\mathbf{F}_q$ by hypothesis, the right hand side agrees with $w^3$ exactly when $\left(\frac{-3}{q}\right) = 1$, i.e., when $q \equiv 1 \pmod 3$. Since

$$p^3/w^3 = \frac{p^3}{p(L \pm 3M\sqrt{-3})/2} = p\frac{p}{(L \pm 3M\sqrt{-3})/2} = p\frac{L \mp 3M\sqrt{-3}}{2},$$

the right hand side of (28) agrees with $p^3/w^3$ if and only if $\left(\frac{-3}{q}\right) = -1$, i.e., when $q \equiv 2 \pmod 3$. □

We now prove Jacobi's law by analyzing for which primes $p \equiv 1 \pmod 3$ we have $w^q = w$ and for which primes $p \equiv 2 \pmod 3$ we have $w^q = p/w$. By Lemma 4.9, we can assume in these proofs that $q \nmid m$.

In what follows we let $\sqrt{3}$ denote a fixed square root of 3 in an algebraic closure of $\mathbf{F}_q$, and let $w$ be an element of this algebraic closure satisfying (27). For notational convenience we also set

$$\pi = \frac{L \pm 3M\sqrt{-3}}{2} \text{ and } \pi' = \frac{L \mp 3M\sqrt{-3}}{2},$$

so that $\pi\pi' = p$ and $w^3 = p\pi$.

*Proof of the Jacobi Law for $q \equiv 1 \pmod 3$.* In this case

$$w + p/w \in \mathbf{F}_q \Leftrightarrow w^q = w \Leftrightarrow w^{q-1} = 1 \Leftrightarrow (p\pi)^{(q-1)/3} = 1 \Leftrightarrow (\pi^2\pi')^{(q-1)/3} = 1$$

Since $q \equiv 1 \pmod 3$, we have $\mathbf{F}_q(\sqrt{-3}) = \mathbf{F}_q$. Hence $\pi$ and $\pi'$ are elements of $\mathbf{F}_q$ (and are nonzero since they multiply to the nonzero element $p$). So by Euler's criterion, the last of the above statements holds if and only if

$$\pi^2\pi' \text{ is a cube in } \mathbf{F}_q \Leftrightarrow \pi'/\pi = \frac{\pi^2\pi'}{\pi'^3} \text{ is a cube in } \mathbf{F}_q.$$

If the minus sign holds in the definition of $\pi$, then this is exactly the criterion of Jacobi's law. If the plus sign holds, then we have only to note that $\pi/\pi'$ is a cube if and only if $\pi'/\pi$ is a cube, and we again recover Jacobi's criterion.

Note that we have proven more than required: we have actually shown that the reduced period equation has *all its roots* (not just one) defined modulo $q$ if and only if $\pi'/\pi$ is a cube in $\mathbf{F}_q(\sqrt{-3})$. □

*Proof of the Jacobi Law for $q \equiv 2 \pmod 3$.* In this case

$$w + p/w \in \mathbf{F}_q \Leftrightarrow w^q = p/w \Leftrightarrow w^{q+1} = p.$$

By Lemma 4.11, we have $w^{3(q+1)} = p^3$; since the cube roots of unity lie outside $\mathbf{F}_q$,

$$w^{q+1} = p \Leftrightarrow w^{q+1} \in \mathbf{F}_q \Leftrightarrow w^{(q+1)(q-1)} = 1 \Leftrightarrow p^{(q^2-1)/3}\pi^{(q^2-1)/3} = 1.$$

By Euler's criterion, $\alpha^{(q^2-1)/3} = 1$ if and only if the nonzero element $\alpha \in \mathbf{F}_q(\sqrt{-3})$ is a cube. Note that since $q \equiv 2 \pmod 3$, every element of $\mathbf{F}_q$ is a cube. In particular, we find

$$\begin{aligned} p^{(q^2-1)/3}\pi^{(q^2-1)/3} = 1 &\Leftrightarrow \pi^{(q^2-1)/3} = 1 \\ &\Leftrightarrow \pi \text{ is a cube in } \mathbf{F}_q(\sqrt{-3}) \\ &\Leftrightarrow \pi^2 \text{ is a cube in } \mathbf{F}_q(\sqrt{-3}) \\ &\Leftrightarrow \pi/\pi' = \pi^2/p \text{ is a cube in } \mathbf{F}_q(\sqrt{-3}). \end{aligned}$$

The proof is now completed as in the case $q \equiv 1 \pmod 3$. (Note that once again we have proved more than we needed.) □

Part of the Jacobi-Sun law is that whether $q$ is a residue or nonresidue of $p$ depends only on the ratio $L/M \pmod q$. The next two theorems describe the ratios $L/M$ corresponding to those $p$ for which $q$ is a cube. We leave their proofs as Exercises 27 and 28.

**Theorem 4.12** (Cunningham & Gosset [16])**.** *Let $p \equiv 1 \pmod 6$ be prime and write $4p = L^2 + 27M^2$ with $L \equiv 1 \pmod 3$. Let $q > 3$ be prime, and let $n = \frac{1}{3}(q - (\frac{-3}{q}))$. Then $q$ is a cube mod $p$ if and only if*

$$\sum_{\substack{0 \le j \le n \\ j \equiv 1 \pmod 2}} 3^j(-3)^{(j-1)/2}\binom{n}{j}L^{n-j}M^j \equiv 0 \pmod q.$$

*The left hand side, if considered as a homogeneous polynomial in $L$ and $M$, breaks up into $\frac{1}{3}(q - (\frac{-3}{q}))$ nonassociated homogeneous linear factors over $\mathbf{F}_q$. It factors as*

$$M \prod_{[a,1] \in G^3} (L - 3aM).$$

The description of these ratios provided by the next theorem is more explicit:

**Theorem 4.13** (E. Lehmer)**.** *Let $p \equiv 1 \pmod 6$ be a prime and write $4p = L^2 + 27M^2$ with $L \equiv 1 \pmod 3$. Then $q$ is a cube mod $p$ if and only if either $q \mid LM$ or $L \equiv \mu M \pmod q$ for some $\mu$ satisfying*

$$\mu^2 \equiv r\left(\frac{9}{2u+1}\right)^2 \pmod q, \quad \text{with } u \not\equiv 0, 1, -\frac{1}{2}, -\frac{1}{3} \pmod q, \tag{29}$$

*and*

$$r \equiv \frac{3u-1}{3u+3} \pmod q \quad \text{with} \quad \left(\frac{r}{q}\right) = 1. \tag{30}$$

4.4. **Sun's Form of Jacobi's Law.** We now prove Sun's pretty equivalent form of Jacobi's law, already enunciated in the introduction. Recall that for $q > 3$ we defined the group $G = G(q)$ by

$$G = \{[a, b] : a, b \in \mathbf{F}_q \oplus \mathbf{F}_q, a^2 + 3b^2 \neq 0\},$$

where we identify $[a, b]$ and $[c, d]$ if $a = \lambda c, b = \lambda d$ for some nonzero $\lambda \in \mathbf{F}_q$, and we multiply according to the rule

$$[a, b] \star [c, d] = [ac - 3bd, ad + bc].$$

All the group axioms are quickly verified (with $[1, 0]$ as the identity element) with the possible exception of associativity. We leave this to the reader to check directly (alternatively, it will follow from the isomorphism proof we offer below).

**Lemma 4.14.** *We have* $\#G = q - \left(\frac{-3}{q}\right)$.

*Proof.* Every element besides $[1, 0]$ can be written uniquely in the form $[a, 1]$ with $a \in \mathbf{F}_q$. We have $[a, 1] \in G$ if and only if $a^2 \neq 3$. Hence

$$\begin{aligned}\#G &= 1 + \#F_q - \#\{a \in \mathbf{F}_q : a^2 = -3\}\\ &= 1 + q - \left(1 + \left(\frac{-3}{q}\right)\right) = q - \left(\frac{-3}{q}\right).\end{aligned}$$ □

**Lemma 4.15.** *Let $\psi$ be the map from $G$ to $\mathbf{F}_q(\sqrt{-3})^*$ defined by*

$$\psi([a, b]) := \frac{a + b\sqrt{-3}}{a - b\sqrt{-3}}.$$

*Then $\psi$ is an injective homomorphism. Hence $G$ is cyclic.*

*Proof.* We need to check first that $\psi$ is well-defined: this follows from $a^2 + 3b^2 \neq 0$, and because we are taking a ratio on the right hand side (so that the ambiguity in $[a, b]$ up to scaling disappears). To see that $\psi$ is a homomorphism, we compute:

$$\begin{aligned}\psi([a, b] \star [c, d]) &= \psi([ac - 3bd, ad + bc])\\ &= \frac{ac - 3bd + (ad + bc)\sqrt{-3}}{ac - 3bd - (ad + bc)\sqrt{-3}}\\ &= \frac{a + b\sqrt{-3}}{a - b\sqrt{-3}} \cdot \frac{c + d\sqrt{-3}}{c - d\sqrt{-3}} = \psi([a, b])\psi([c, d]).\end{aligned}$$

To see that $\psi$ is injective, it suffices to prove the kernel is trivial: But

$$\psi([a, b]) = 1 \Longrightarrow \frac{a + b\sqrt{-3}}{a - b\sqrt{-3}} = 1,$$

and this implies that $b = 0$. Hence $[a, b] = [1, 0]$ is the identity of $G$. This proves $\psi$ is an isomorphism as claimed.

The cyclicity of $G$ is an easy corollary: every finite subgroup of the multiplicative group of a field is cyclic. □

We can now prove Sun's form of Jacobi's law:

**Theorem 4.16.** *Let $p$ and $q$ be distinct primes, with $p, q > 3$ and $p \equiv 1 \pmod 3$. Write $4p = L^2 + 27M^2$ with $L \equiv 1 \pmod 3$, and let $G = G(q)$ be the group defined above. Then*

$$q \text{ is a cube modulo } p \Longleftrightarrow [L, 3M] \text{ is a cube in } G.$$

*Proof.* Let $H$ be the image of $\psi$, where $\psi$ is the isomorphism described above (hence $\#H = \#G$). By the Jacobi law, we know

$$\begin{aligned} q \text{ is a cube modulo } p &\iff \psi([L,3M]) \text{ is a cube in } \mathbf{F}_q(\sqrt{-3}) \\ &\iff \psi([L,3M])^{\#\mathbf{F}_q(\sqrt{-3})^*/3} = 1 \\ &\iff \psi([L,3M])^{\gcd(\#H,\#\mathbf{F}_q(\sqrt{-3})^*/3)} = 1 \\ &\iff \psi([L,3M])^{\#H/3} = 1 \\ &\iff \psi(([L,3M])^{\#H/3}) = 1 \\ &\iff [L,3M]^{\#G/3} = [1,0] \\ &\iff [L,3M] \text{ is a cube in } G. \end{aligned}$$

□

4.5. **Jacobi's Determination of $L$ in $L^2+27M^2 = 4p$.** We cannot resist pointing out a not-entirely-related consequence of our investigations into cyclotomy. The same temptation overcame Jacobi, who mentioned this result both in an addendum to paper [52] and in his letter to Gauss [53], who had proved an analogous theorem concerning the representation of a prime $p \equiv 1 \pmod 4$ in the form $a^2 + b^2$. For an extensive discussion of results of this kind, see [5, Chapter 9].

**Theorem 4.17** (Jacobi). *Let $p \equiv 1 \pmod 6$ be prime, and let $4p = L^2 + 27M^2$, where $L \equiv 1 \pmod 3$. Then $L$ is the least absolute residue of $-\binom{2f}{f} \pmod p$, where $f = (p-1)/3$.*

*Example.* We have

$$4 \cdot 7 = 1^2 + 27 \cdot 1^2, \quad \text{agreeing with } -\binom{4}{2} = -6 \equiv 1 \pmod 7.$$

A somewhat larger example is

$$4 \cdot 73 = (7)^2 + 27 \cdot 3^2, \text{ and } -\binom{48}{24} = -32247603683100 \equiv 7 \pmod{73}.$$

*Proof.* We adopt the notation of §4.1 for the cyclotomic numbers. Choose $g$ so that $b - c = M$ and set $\omega := g^{(p-1)/3}$.

We compute the value of the sum $S = \sum_{z\in(\mathbf{Z}/p\mathbf{Z})^*} (z^3+1)^{2(p-1)/3} \bmod p$ in two ways different. First, the binomial theorem gives

$$\sum_{z\in\mathbf{F}_p^*} (z^3+1)^{2(p-1)/3} = \sum_{z\in\mathbf{F}_p^*} \sum_{m=0}^{2(p-1)/3} \binom{2(p-1)/3}{m} z^{3m};$$

upon reversing the order of summation and observing that

$$\sum_{z\in(\mathbf{Z}/p\mathbf{Z})^*} z^k = \begin{cases} p-1 & \text{if } p-1 \mid k, \\ 0 & \text{otherwise,} \end{cases}$$

we find

$$S \equiv -2 + -\binom{2m}{m} \pmod p. \tag{31}$$

But we can also determine $S$ mod $p$ in terms of the cyclotomic numbers:

$$\begin{aligned} S &\equiv 3(00) + 3(01)\omega^2 + 3(02)\omega \\ &= f + k - 3 + \left(\frac{2f-k}{2} + \frac{3M}{2}\right)\omega^2 + \left(\frac{2f-k}{2} - \frac{3M}{2}\right)\omega \\ &= \frac{2f-k}{2}(1+\omega+\omega^2) + \frac{3M}{2}(\omega^2-\omega) + \frac{3k-2}{2} - 2 \pmod{p}. \end{aligned}$$

Now $1 + \omega + \omega^2 \equiv 0 \pmod{p}$, so the first summand above vanishes. Moreover,

$$(\omega^2 - \omega)^2 = (-2\omega - 1)^2 = 4(\omega^2 + \omega + 1) - 3 = -3.$$

Observing that $L = 3k - 2$ and writing $\sqrt{-3}$ for the element $\omega^2 - \omega$, we have shown

$$S \equiv \frac{L}{2} + \frac{3M}{2}\sqrt{-3} - 2 \pmod{p},$$

which combined with (31) proves

$$\frac{L}{2} + \frac{3M}{2}\sqrt{-3} \equiv \binom{2f}{f} \pmod{p}. \tag{32}$$

Since $\binom{2f}{f} \not\equiv 0 \pmod{p}$ and $p = (\frac{1}{2}(L + 3M\sqrt{-3}))(\frac{1}{2}(L - 3M\sqrt{-3}))$, we must have

$$\frac{L}{2} - \frac{3M}{2}\sqrt{-3} \equiv 0 \pmod{p}. \tag{33}$$

Adding (32) and (33) yields us the asserted congruence on $L$.

It remains to show that $L$ is the *least* absolute residue of $-\binom{2f}{f}$. For this it certainly suffices to prove that $|L| < p/2$. If this is false, then from $L^2 + 27M^2 = 4p$ we deduce that $p^2/4 \leq 4p$, and hence $p \leq 16$. Thus only $p = 7$ and $p = 13$ are possible exceptions, and the fact that the theorem holds for these primes can be checked by hand. □

## 5. Dirichlet's Rational Quartic Reciprocity Law

5.1. **Quartic Character of 2.** In the introduction we stated two criteria of Gauss concerning the biquadratic character of 2: It suffices to treat the case $p \equiv 1 \pmod{8}$. Write

$$p = a^2 + 4b^2 = c^2 + 2d^2$$

for certain integers $a, b, c$ and $d$. Then the statement that 2 is a fourth power modulo $p$ is equivalent to (i) $\left(\frac{2}{c}\right) = 1$, as well as to (ii) $4 \mid b$.

The demonstration that (i) is necessary and sufficient is quite simple, and a proof in the same spirit as Gauss's is offered in Exercise 44(iii). However, as Gauss remarks in his 1825 announcement, the second criterion is "intimately bound with other subtle preliminary investigations." (These complicated preliminaries turn out, in the 1828 memoir, to be the determination of the cyclotomic numbers of order 4; the proof for (ii) then runs along the same lines as the proof we offered for Theorem 4.6 concerning the cubic character of 2.) Having seen only this announcement, Dirichlet rediscovered [18, §2] Gauss's proof of (i), at the same time offering a slick argument demonstrating the equivalence (for all $p \equiv 1 \pmod{8}$) of (i) and (ii) (see Exercise 46).

When Dirichlet wrote to Gauss with these discoveries, attaching a copy of his paper [18], Gauss responded that he was "very well-pleased" at the proof of the equivalence of (i) and (ii). But he insisted that Dirichlet's shrewdness did render his more complicated derivation obsolete [36, p.376] (following Rowe's translation [91, p.21]):

> I could have chosen a number of different forms of proof for the theorem there arising [criterion (ii)]; it will not have escaped you, however, why I have preferred the one carried out here, namely primarily because the classification of 2 with respect to those modules for which it is a quadratic nonresidue (under $B$ or $D$) must be regarded as an essentially integral part of the theorem for which most of the other forms of proof appear to be inapplicable.[1]

This is an admission that while cyclotomy is not necessary to obtain (i) and (ii) as they stand, it yields natural proofs of results seemingly inaccessible to most of the more elementary methods. In particular, when $p \equiv 5 \pmod 8$ (so that 2 is not a square, let alone a fourth power), one can still ask which of the two cosets of $(\mathbf{F}_p^*)^4$ consisting of quadratic nonresidues contains 2. The answer to this question, from the perspective of cyclotomy, is no more difficult then the proof of criterion (ii) (see [33, §21]), but the problem seems unattackable by the methods of [18]. (We can excuse Dirichlet for this "oversight," as Gauss's results for $p \equiv 5 \pmod 8$ were not mentioned in the 1825 announcement.)

However, in a letter to Stern (the relevant portion of which was posthumously published in Crelle's Journal [21]), Dirichlet derives Gauss's most general results from [33] concerning the biquadratic character of 2 in an entirely elementary (cyclotomy-free) way:

**Theorem 5.1** (Quartic Character of 2)**.** *Let $p \equiv 1 \pmod 4$ be prime, and write $p = a^2 + 4b^2$ (so that $a$ is odd). Let $f = -\frac{a}{2b}$ in $\mathbf{F}_p$. Then $f$ is a primitive fourth root of unity and we have*

$$2^{(p-1)/4} = f^{ab} \qquad \textit{in } \mathbf{F}_p.$$

*Proof.* Over $\mathbf{F}_p$, we have

$$f^2 + 1 = \frac{a^2 + 4b^2}{4b^2} = \frac{p}{4b^2} = 0,$$

hence $f^2 = -1$ and $f$ is a primitive fourth root of unity as claimed.

Now $(a + 2b)^2 = a^2 + 4b^2 + 4ab \equiv 4ab \pmod p$, so that (working in $\mathbf{F}_p$)

$$2^{(p-1)/4}(2ab)^{(p-1)/4} = (a + 2b)^{(p-1)/2} = \left(\frac{a + 2b}{p}\right),$$

and therefore (since $2b = -a/f = af$)

$$\begin{aligned} 2^{(p-1)/4} &= \left(\frac{a + 2b}{p}\right)(2ab)^{-(p-1)/4} = \left(\frac{a + 2b}{p}\right)(a^2 f)^{-(p-1)/4} \\ &= \left(\frac{a + 2b}{p}\right)a^{-(p-1)/2} f^{-(p-1)/4} = \left(\frac{a + 2b}{p}\right)\left(\frac{a}{p}\right) f^{-(p-1)/4}. \end{aligned} \tag{34}$$

[1] Let $p \equiv 1 \pmod 4$ and $f$ a fixed primitive fourth root of unity in $\mathbf{F}_p^*$. The classes $A, B, C$ and $D$ are consist of the elements $a$ for which $a^{(p-1)/4} = f^i$ for $i = 0, 1, 2$ and 3 respectively. Note that $A$ and $C$ are independent of the choice of $f$, while replacing $f$ by $f^{-1}$ has the effect of interchanging $B$ and $D$.

Since $p = a^2 + 4b^2$, it follows that

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2+4b^2}{a}\right) = \left(\frac{4b^2}{a}\right) = 1. \tag{35}$$

Moreover, since $2p = (a+2b)^2 + (a-2b)^2$, we have

$$\begin{aligned}\left(\frac{a+2b}{p}\right) = \left(\frac{p}{a+2b}\right) &= \left(\frac{4p}{a+2b}\right) = \left(\frac{2}{a+2b}\right)\left(\frac{2p}{a+2b}\right)\\ &= \left(\frac{2}{a+2b}\right)\left(\frac{(a-2b)^2}{a+2b}\right) = \left(\frac{2}{a+2b}\right). \end{aligned}\tag{36}$$

Putting (34), (35) and (36) together gives

$$\begin{aligned}2^{(p-1)/4} &= (-1)^{\frac{(a+2b)^2-1}{8}} f^{-(p-1)/4}\\ &= f^{\frac{(a+2b)^2-1}{4}} f^{-(p-1)/4} = f^{(p+4ab-1)/4} f^{-(p-1)/4} = f^{ab},\end{aligned}$$

as claimed. □

This immediately implies Gauss's results, which we state as

**Corollary 5.2** (Gauss [33, §21], cf. [34, §24]). *Let $p \equiv 1 \pmod 4$ and let $f$ be a primitive fourth root of unity in $\mathbf{F}_p^*$. Write $p = a^2 + 4b^2$ with the signs chosen so that $a \equiv 1 \pmod 4$ and $2b \equiv af \pmod p$. Then*

$$2^{(p-1)/4} = f^i \iff b \equiv i \pmod 4.$$

*In particular, 2 is a fourth power modulo $p$ if and only if $4 \mid b$, that is, if and only if $p$ can be written in the form $a'^2 + 64b'^2$.*

5.2. **Dirichlet's Law.** We now prove the following theorem announced in the introduction:

**Theorem 5.3** (Dirichlet's Rational Quartic Reciprocity Law). *Let $p$ and $q$ be distinct odd primes with $p \equiv 1 \pmod 4$. Write $p = a^2 + b^2$, where $b$ is even. Suppose $\left(\frac{q^*}{p}\right) = 1$ (so that also $\left(\frac{p}{q}\right) = 1$). Then*

$$\left(\frac{q^*}{p}\right)_4 = \left(\frac{\sqrt{p}(b+\sqrt{p})}{q}\right)$$

*for any choice of $\sqrt{p}$ in $\mathbf{F}_q$ for which $b + \sqrt{p}$ is nonvanishing.*

The only ingredient necessary for the proof, apart from the law of quadratic reciprocity, is the theorem of Legendre on zeros of integral ternary forms:

**Legendre's Theorem.** *Let $a, b$ and $c$ be pairwise coprime integers, not all of the same sign. If the congruences*

$$x^2 \equiv -bc \pmod a, \quad x^2 \equiv -ab \pmod c, \quad x^2 \equiv -ac \pmod b$$

*are all solvable, then the equation $ax^2 + by^2 + cz^2 = 0$ has a solution in integers $x, y$ and $z$ not all vanishing.*

However the proof is by no means simple; indeed, Jacobi referred to it in his Königsberg lectures as [78, pp. 170-171] "quite complex but at the same time a shrewd masterpiece."

Let us begin. We start with a technical lemma, and the only application of Legendre's theorem necessary (one can also substitute Lemma 7.5; see Venkov [100, Chapter 3]):

**Lemma 5.4.** *Let $p, q$ be distinct odd primes as in Theorem 5.3; i.e., $p \equiv 1 \pmod 4$ and $\left(\frac{q^*}{p}\right) = 1$. Then one can find positive integers $s, t$ and $u$ satisfying*

$$ps^2 = t^2 - q^* u^2 \tag{37}$$

*as well as the following additional properties:*

(i) *$s, t$ and $u$ are pairwise coprime,*
(ii) *$p$ is coprime to $tu$ and $q$ is coprime to $st$,*
(iii) *$t$ is odd,*
(iv) *$s$ and $u$ have opposite parity.*

*Proof.* We first show there are integers $s, t$ and $u$ satisfying (37). This is equivalent to showing that the ternary form

$$px^2 - y^2 + q^* z^2$$

in $x, y$ and $z$ has a nontrivial integral zero. The coefficients are not all of the same sign, so we only have to check that $q^*$ is a square modulo $p$ and $p$ is a square modulo $q^*$. The former holds by assumption, and the latter follows by reciprocity.

Consider a solution where not all of $s, t$ and $u$ vanish. Then none of $s$, $t$ and $u$ vanish, and we may assume they are all positive. Dividing through by their greatest common factor we can assume that $\gcd(s, t, u) = 1$.

We now verify that $s, t$ and $u$ have all the required properties. To verify (i) we show that any prime $l$ dividing two of $s, t$ and $u$ must also divide the third: Suppose $l$ divides $s$ and $t$; then $l^2$ divides $q^* u^2$, which implies $l$ divides $u^2$, which implies $l$ divides $u$. Similarly, if $l$ divides $t$ and $u$ then $l^2$ divides $ps^2$, which implies $l$ divides $s$. Finally, if $l$ divides $s$ and $u$ then $l^2$ divides $t^2$, so $l$ divides $t$. In all of these cases we have a nontrivial common divisor of $s, t$ and $u$, contradicting that $\gcd(s, t, u) = 1$.

We use (i) in the proof of (ii): if $p$ divides $t$ then $p \mid ps^2 - t^2 = -q^* u^2$ and since $p$ and $q$ are distinct primes this shows that $p$ divides $u$. But then $u$ and $t$ are not coprime, contradicting (i). Similarly if $p$ divides $u$ then $p$ divides $t^2$, so that $p$ divides $t$. This contradicts pairwise coprimality and proves the half of (ii) concerning $p$. The cases concerning $q$ are similar: if $q$ divides $t$ then $q$ divides $ps^2$, so that $q$ divides $s$, and if $q$ divides $s$ then $q$ divides $t^2$ so that $q$ divides $t$. In both cases we have a contradiction as before.

We prove (iii) and (iv) simultaneously. We have

$$s^2 \equiv ps^2 \equiv t^2 - q^* u^2 \equiv t^2 - u^2 \pmod 4. \tag{38}$$

Suppose first that $s$ is odd. Then $s^2 \equiv 1 \pmod 4$, so that $t$ and $u$ have opposite parity. If $t$ is even and $u$ is odd, then $s^2 \equiv t^2 - u^2 \equiv -1 \pmod 4$, an absurdity. So $t$ must be even and $u$ odd. On the other hand, if $s$ is even, then (38) implies $t$ and $u$ must have the same parity; since they are coprime they must both be odd. □

The following lemma evaluates $\left(\frac{q^*}{p}\right)$ in terms of the auxiliary numbers $t$ and $u$:

**Lemma 5.5.** *Let $p$ and $q$ satisy the conditions of Theorem 5.3. Write*

$$ps^2 = t^2 - q^* u^2, \quad \text{where } s, t, u \text{ are as in Lemma 5.4.} \tag{39}$$

*Then*

$$\left(\frac{q^*}{p}\right)_4 = (-1)^{(t-1)/2} \left(\frac{2}{p}\right)^e \left(\frac{t}{q}\right),$$

*where the integer $e$ is defined by the relation $2^e \| u$.*

*Proof.* Looking at (39) mod $p$ we see that $t^2 \equiv q^* u^2 \pmod{p}$, so that we have the $\mathbf{F}_p$-equation

$$\left(\frac{t}{p}\right)\left(\frac{u}{p}\right) = \left(\frac{t}{p}\right)\left(\frac{u^{-1}}{p}\right) = (t^2u^{-2})^{(p-1)/4} = (q^*)^{(p-1)/4}.$$

We now find alternate expressions for the two Legendre symbols on the left.

Multiplying (39) by $q^*$ we see that

$$-q^*ps^2 = -q^*t^2 + (q^*)^2u^2,$$

so that

$$1 = \left(\frac{-q^*ps^2}{t}\right) = \left(\frac{-q^*p}{t}\right) = \left(\frac{-q^*}{t}\right)\left(\frac{p}{t}\right), \quad \text{whence } \left(\frac{t}{p}\right) = \left(\frac{-q^*}{t}\right) = \left(\frac{-1}{t}\right)\left(\frac{t}{q}\right),$$

where we have used Jacobi reciprocity.

To find an alternative form for $\left(\frac{u}{p}\right)$, we write $u = 2^e v$, where $v$ is odd. Then

$$\left(\frac{u}{p}\right) = \left(\frac{2^e}{p}\right)\left(\frac{v}{p}\right) = \left(\frac{2}{p}\right)^e\left(\frac{p}{v}\right) = \left(\frac{2}{p}\right)^e\left(\frac{t^2-q^*u^2}{v}\right) = \left(\frac{2}{p}\right)^e\left(\frac{t^2}{v}\right) = \left(\frac{2}{p}\right)^e.$$

Combining the results of the previous two paragraphs we obtain

$$(q^*)^{(p-1)/4} = \left(\frac{t}{p}\right)\left(\frac{u}{p}\right) = \left(\frac{-1}{t}\right)\left(\frac{t}{q}\right)\left(\frac{2}{p}\right)^e = (-1)^{(t-1)/2}\left(\frac{t}{q}\right)\left(\frac{2}{p}\right)^e.$$

Since also $(q^*)^{(p-1)/4} \equiv \left(\frac{q^*}{p}\right)_4 \pmod{p}$, the result follows. □

**Lemma 5.6.** *Let $p$ and $q$ be as in Theorem 5.3, and let $a, b$ and $s, t, u$ be as above. If $q$ does not divide $t \pm sb$ for the sign being considered, we have*

$$\left(\frac{t \pm sb}{q}\right) = (-1)^{(t-1)/2}\left(\frac{2}{p}\right)^e,$$

*where $e$ has the same meaning as before: $2^e \| u$.*

*Proof.* We begin with the algebraic difference-of-squares identity identity

$$(t+sb)(t-sb) = (sa)^2 + q^*u^2. \tag{40}$$

The right hand side is clearly positive, and depending on the sign of $b$, one of the terms on the left is also clearly positive. So all three terms here must be positive; we will use this when applying the quadratic reciprocity law below.

Let $g$ be the greatest common divisor of $a$ and $u$. Write

$$sa = g\xi, \quad u = g\eta.$$

Then $\xi$ and $\eta$ are coprime (using that $s$ and $u$ are coprime) and we have

$$(t+sb)(t-sb) = g^2(\xi^2 + q^*\eta^2). \tag{41}$$

Moreover,

$$\gcd(t+sb, t-sb, g) = 1 : \tag{42}$$

any common divisor of the odd integers $t + sb$ and $t - sb$ divides $2t$, hence divides $t$. But then if it divides $g = \gcd(a, u)$ as well, it must divide $\gcd(t, u) = 1$.

It follows from (41), (42) and uniqueness of factorization that there are positive integers $g_1$ and $g_2$ with

$$g_1^2 \mid (t+sb), \quad g_2^2 \mid (t-sb), \quad \text{and } g_1g_2 = g.$$

Suppose now that $q \nmid t+sb$, the case when $q \nmid t-sb$ being entirely similar. Then

$$\left(\frac{t+sb}{q}\right) = \left(\frac{g_1^2}{q}\right)\left(\frac{(t+sb)/g_1^2}{q}\right).$$

Of course $\left(\frac{g_1^2}{q}\right) = 1$ (note that $g_1$ is prime to $q$ since it divides a number we are assuming is prime to $q$). Also

$$\frac{t+sb}{g_1^2} \mid \frac{t+sb}{g_1^2}\cdot\frac{t-sb}{g_2^2} = \xi^2 + q^*\eta^2,$$

and as $\xi$ and $\eta$ are relatively prime we deduce that

$$\begin{aligned}1 = \left(\frac{-q^*}{(t+sb)/g_1^2}\right) &= \left(\frac{-1}{(t+sb)/g_1^2}\right)\left(\frac{q^*}{(t+sb)/g_1^2}\right)\\ &= \left(\frac{-1}{t+sb}\right)\left(\frac{q^*}{(t+sb)/g_1^2}\right) = (-1)^{(t-1)/2+sb/2}\left(\frac{(t+sb)/g_1^2}{q}\right),\end{aligned}$$

using Jacobi reciprocity. Hence

$$\begin{aligned}\left(\frac{t+sb}{q}\right) &= \left(\frac{g_1^2}{q}\right)\left(\frac{(t+sb)/g_1^2}{q}\right)\\ &= 1\cdot(-1)^{(t-1)/2+sb/2} = (-1)^{(t-1)/2}(-1)^{sb/2}.\end{aligned}$$

The proof will therefore be complete once we show that

$$(-1)^{sb/2} = \left(\frac{2}{p}\right)^e.$$

To this end, we first observe that $b/2$ is even if and only if $p = a^2+b^2 \equiv 1 \pmod 8$, which occurs (for $p \equiv 1 \pmod 4$) if and only if 2 is a square (mod $p$). Hence

$$(-1)^{sb/2} = \left((-1)^{b/2}\right)^s = \left(\frac{2}{p}\right)^s.$$

If $p \equiv 1 \pmod 8$, then $\left(\frac{2}{p}\right) = 1$ so that certainly $\left(\frac{2}{p}\right)^s = \left(\frac{2}{p}\right)^e$. So we may suppose that $p \equiv 5 \pmod 8$. In this case we can show that $s$ and $e$ have the same parity, which again gives the result: For if $s$ is even then $u$ is odd (Lemma 5.4), so that $e = 0$. On the other hand, if $s$ is odd then the congruence

$$5 \equiv ps^2 \equiv t^2 - q^*u^2 \equiv 1 - q^*u^2 \pmod 8$$

implies $2^1 \| u$, so that $e = 1$. □

We can now prove the Dirichlet Reciprocity Law. The case when $q \mid a$, which must be handled separately, is contained in the following lemma:

**Lemma 5.7.** *Let $p$ and $q$ be distinct odd primes and suppose $p \equiv 1 \pmod 4$. Write $p = a^2+b^2$ with $b$ even. If $q \mid a$ then $\left(\frac{q^*}{p}\right) = \left(\frac{2}{q}\right)$.*

*Remark.* In the case $q \mid a$, we have $p \equiv b^2 \pmod q$, so that the choices for $\sqrt{p}$ in $\mathbf{F}_q$ are $\pm b$. The expression $b+\sqrt{p}$ is nonvanishing only if we take $\sqrt{p} = b$, and then Dirichlet's law claims

$$\left(\frac{q^*}{p}\right) = \left(\frac{\sqrt{p}(b+\sqrt{p})}{q}\right) = \left(\frac{2b^2}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{b^2}{q}\right) = \left(\frac{2}{q}\right),$$

which is what the lemma asserts. (To obtain the last equality we use that $q$ cannot divide both $a$ and $b$ since it does not divide $p$.)

*Proof.* Note that $q \mid a$ implies $p \equiv b^2 \pmod{q}$, so that $\left(\frac{p}{q}\right) = 1$ and hence $\left(\frac{q^*}{p}\right) = 1$. So $p$ and $q$ satisfy all the hypothesis of Theorem 5.3.

In the case when $q$ divides $a$, we obtain from (40) that $q$ divides $t + sb$ or $t - sb$. If it divides both, then it divides $2sb$; as $q$ is prime to $s$ (by Lemma 5.4), it then divides $b$. But then $q \mid a^2 + b^2 = p$, a contradiction.

So $q$ divides exactly one of $t + sb$ and $t - sb$; suppose it is the second. Then $t \equiv sb \pmod{q}$ and Lemma 5.6 shows that

$$(-1)^{(t-1)/2}\left(\frac{2}{p}\right)^e = \left(\frac{t+sb}{q}\right) = \left(\frac{2t}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{t}{q}\right),$$

hence

$$\left(\frac{2}{q}\right) = (-1)^{(t-1)/2}\left(\frac{2}{p}\right)^e\left(\frac{t}{q}\right) = (q^*)^{(p-1)/4}$$

by Lemma 5.5; the result follows.

The case when $q$ divides the first factor and not the second is nearly identical. □

*Proof of Theorem 5.3.* The case when $q$ divides $a$ is handled by Lemma 5.7, so we assume in what follows that $q$ and $a$ are coprime. By Lemma 5.5,

$$\left(\frac{q^*}{p}\right)_4 = (-1)^{(t-1)/2}\left(\frac{2}{p}\right)^e\left(\frac{t}{q}\right).$$

We now seek to reexpress the right hand side. Since $ps^2 = t^2 - q^*u^2$, we have the $\mathbf{F}_q$-equation

$$t = \epsilon s\sqrt{p} \tag{43}$$

for an appropriate choice of $\epsilon = \pm 1$, hence

$$\left(\frac{t}{q}\right) = \left(\frac{\epsilon s\sqrt{p}}{q}\right).$$

Since $q$ does not divide $a$, the identity (40) shows that $q$ divides neither $t + sb$ nor $t - sb$. Therefore regardless of the value of $\epsilon$ we have by Lemma 5.6 that (keeping (43) in mind)

$$\begin{aligned}(-1)^{(t-1)/2}\left(\frac{2}{p}\right)^e\left(\frac{t}{q}\right) &= \left(\frac{t+\epsilon sb}{q}\right)\left(\frac{t}{q}\right) = \left(\frac{\epsilon s\sqrt{p}+\epsilon sb}{q}\right)\left(\frac{\epsilon s\sqrt{p}}{q}\right)\\ &= \left(\frac{\epsilon s}{q}\right)\left(\frac{\sqrt{p}+b}{q}\right)\left(\frac{\epsilon s}{q}\right)\left(\frac{\sqrt{p}}{q}\right) = \left(\frac{\sqrt{p}(\sqrt{p}+b)}{q}\right),\end{aligned}$$

and the theorem follows. □

As an immediate consequence, we derive:

**Corollary 5.8.** *Suppose $p, q$ are distinct odd primes, where $p \equiv 1 \pmod{4}$. Write $p = a^2 + b^2$ with $b$ even. If $q$ divides $b$ then $q^*$ is a quartic residue modulo $p$.*

*Proof.* We first show that the Dirichlet law is applicable to this situation. We have

$$\left(\frac{p}{q}\right) = \left(\frac{a^2}{q}\right) = 1, \quad \text{and so by reciprocity} \quad \left(\frac{q^*}{p}\right) = 1.$$

Also, if we choose an arbitrary value of $\sqrt{p} \in \mathbf{F}_q$, then $b + \sqrt{p} = \sqrt{p} \neq 0$. Thus the Dirichlet law applies and we find

$$\left(\frac{q^*}{p}\right)_4 = \left(\frac{\sqrt{p}(b+\sqrt{p})}{q}\right) = \left(\frac{\sqrt{p}\sqrt{p}}{q}\right) = \left(\frac{p}{q}\right) = 1.$$ □

5.3. **The Dirichlet-Sun Law.** Let $G$ be defined by

$$G = \{[a, b] : a, b \in \mathbf{F}_q, a^2 + b^2 \neq 0\},$$

where we identify $[a, b]$ and $[c, d]$ if $a = \lambda c, b = \lambda d$ for some nonzero $\lambda \in \mathbf{F}_q$, and where we multiplying according to the rule

$$[a, b] \star [c, d] := [ac - bd, ad + bc].$$

Then $G$ is a cyclic group of order $q - \left(\frac{-1}{q}\right)$ which injects into $\mathbf{F}_q(i)^*$ by means of the map $\psi$, where

$$\psi([a, b]) = \frac{a + bi}{a - bi}.$$

This follows mutatis mutandis from the proofs of 4.4 (replacing $\sqrt{-3}$ by $\sqrt{-1}$ everywhere).

**Theorem 5.9** (Dirichlet-Sun Law)**.** *Let $p$ and $q$ be distinct odd primes, with $p \equiv 1 \pmod 4$. Write $p = a^2 + b^2$ with $b$ even. Then with $q^* = (-1)^{(q-1)/2}q$,*

$$q^* \text{ is a fourth power (respectively a square) mod } p \Leftrightarrow$$
$$[a, b] \text{ is a fourth power (respectively a square) in } G.$$

Note that the introduction states an equivalent form of this law in terms of a certain power of $\frac{a+bi}{a-bi}$ in $\mathbf{F}_q(i)$; we defer the proof of that form of the law to the end of the section.

Unfortunately, the deduction of the Dirichlet-Sun Law from Dirichlet's Reciprocity Law is not nearly so neat as the deduction of the Jacobi-Sun Law from Jacobi's Reciprocity Law. We begin by proving those equivalences of Theorem 5.9 involving squares: these follow in a straightforward manner from quadratic reciprocity and our injection of $G$ into $\mathbf{F}_q(i)^*$.

*Proof of Sun's Law for Squares.* Let $H$ be the image of $\psi$, where $\psi$ is the injection of $G$ into $\mathbf{F}_q(i)^*$ given above. Then

$$\begin{aligned}
[a, b] \text{ is a square in } G &\Longleftrightarrow \psi([a, b])^{\#H/2} = 1 \\
&\Longleftrightarrow \left(\frac{a + bi}{a - bi}\right)^{(q - \left(\frac{-1}{q}\right))/2} = 1 \\
&\Longleftrightarrow p^{(q - \left(\frac{-1}{q}\right))/2}(a - bi)^{(-q - \left(\frac{-1}{q}\right))} = 1;
\end{aligned}$$

We now consider separately the cases $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. In the former $i^q = 1$, in the latter $i^q = -1$. In both cases that the last statement in our chain of equivalences reduces down to $p^{(q-1)/2} = 1$. This is of course equivalent to $\left(\frac{p}{q}\right) = 1$, which by the law of quadratic reciprocity is the same as $\left(\frac{q}{p}\right) = 1$. □

We now prove the fourth power law. It is necessary to separate out the case when $q$ divides $b$.

*Proof of the Dirichlet-Sun law in the case $q \mid b$.* Since in this $[a, b] = [1, 0]$ is the identity of $G$, which is certainly a fourth power, the Dirichlet-Sun law asserts that $q^*$ is a fourth power mod $p$. But this is exactly what we proved in Corollary (5.8). □

The general case of the Dirichlet-Sun law requires a few preliminary technical lemmas.

**Lemma 5.10.** *Let $p$ and $q$ be distinct odd primes with $p \equiv 1 \pmod 4$, and suppose that $\left(\frac{q^*}{p}\right) = 1$. Write $p = a^2 + b^2$ with $b$ even, and assume that $q \nmid b$. Moreover, suppose $\sqrt{p} \in \mathbf{F}_q$ is chosen so that $b + \sqrt{p} \neq 0$. Then there exists an element $\kappa \in \mathbf{F}_q$ for which $[\kappa, 1] \in G$ and $[\kappa, 1] \star [\kappa, 1] = [a, b]$. If $\kappa$ denotes any such element, then*

$$\left(\frac{\sqrt{p}(\sqrt{p}+b)}{q}\right) = \left(\frac{\kappa^2+1}{q}\right). \tag{44}$$

*Proof.* We begin by rewriting the conditions on $\kappa$. First, $[\kappa, 1] \in G$ asserts that

$$\kappa^2 + 1 \neq 0. \tag{45}$$

Second,

$$[\kappa, 1] \star [\kappa, 1] = [a, b] \Longleftrightarrow \frac{1}{2}\left(\kappa - \frac{1}{\kappa}\right) = \frac{a}{b}. \tag{46}$$

Note that if there is one value of $\kappa$ meeting these conditions, then there are two: the other is $-1/\kappa$, which is distinct from $\kappa$ by condition (45). (We leave it to the reader to check there can be no others.) Since $\kappa$ is necessarily nonzero by (46), we have

$$\left(\frac{\kappa^2+1}{q}\right) = \left(\frac{(\kappa)^{-2}(\kappa^2+1)}{q}\right) = \left(\frac{(-\kappa^{-1})^2+1}{q}\right),$$

so that if (44) holds for either value of $\kappa$, it holds for both of them.

We now construct a value of $\kappa$ for which (44) is true. Since $b \neq 0$ in $\mathbf{F}_q$, we can write $\sqrt{p} = \lambda b$ and $a = \tau b$ for some $\lambda, \tau \in \mathbf{F}_q$. Then

$$(\sqrt{p} - b)(\sqrt{p} - b) = a^2 \Longrightarrow b^2(\lambda^2 - 1) = b^2\tau^2 \Longrightarrow (\lambda - \tau)(\lambda + \tau) = 1.$$

Set $\kappa := \lambda + \tau$. Then $1/\kappa = \lambda - \tau$, hence

$$2\tau = \kappa - 1/\kappa \quad \text{and} \quad 2\lambda = \kappa + 1/\kappa.$$

The first of these equalities yields (46). From the second we deduce

$$\begin{aligned}\left(\frac{(\sqrt{p}+b)\sqrt{p}}{q}\right) &= \left(\frac{\sqrt{p}(\sqrt{p}+\sqrt{p}/\lambda)}{q}\right) = \left(\frac{p}{q}\right)\left(\frac{(\lambda+1)/\lambda}{q}\right) \\ &= \left(\frac{(\lambda+1)/\lambda}{q}\right) = \left(\frac{(\kappa+1)^2/(\kappa^2+1)}{q}\right) = \left(\frac{\kappa^2+1}{q}\right).\end{aligned}$$

(Note that $\kappa^2 + 1 \neq 0$ since $\sqrt{p}$ was chosen so that $b + \sqrt{p}$ is nonvanishing.) This proves (44), which implies (45). □

The next lemma analyzes when $\left(\frac{\kappa^2+1}{q}\right) = 1$ in terms of the group $G$:

**Lemma 5.11.** *Let $\kappa$ be an element of $\mathbf{F}_q$. Then*

$$\left(\frac{\kappa^2+1}{q}\right) = 1 \Leftrightarrow [\kappa, 1] \in G \text{ and } [\kappa, 1] = [\beta, 1] \star [\beta, 1] \text{ for some } [\beta, 1] \in G \text{ with } \beta \neq 0.$$

*Proof.* The theorem asserts that

$$\kappa^2 + 1 \text{ is a nonzero square in } \mathbf{F}_q \Longleftrightarrow \kappa = \frac{1}{2}(\beta - 1/\beta)$$

for some nonzero $\beta \in \mathbf{F}_q$ for which $\beta^2 + 1 \neq 0$. If $\kappa$ is of this form, then

$$\kappa^2 + 1 = \left(\frac{1}{2}(\beta + 1/\beta)\right)^2,$$

which is a nonzero square by the conditions on $\beta$. We leave it to the reader to check that if we begin by assuming $\kappa^2+1$ is a nonzero square, then solving the equation $\beta - 1/\beta = 2\kappa$ by the quadratic formula yields a value of $\beta$ with the stated properties. □

*Proof of Sun's Law for Fourth Powers.* We may assume $q$ and $b$ are coprime.

Suppose $\left(\frac{q^*}{p}\right)_4 = 1$. By Dirichlet's Law and Lemma 5.10, it follows that $\left(\frac{\kappa^2+1}{q}\right) = 1$, where $\kappa$ is such that $[\kappa, 1] \star [\kappa, 1] = [a, b]$. By Lemma 5.11, we have $[\kappa, 1] = [\beta, 1] \star [\beta, 1]$ for some $[\beta, 1] \in G$. Hence $[a, b] = [\beta, 1]^4$ is a fourth power in $G$.

Conversely, suppose $[a, b]$ is a fourth power in $G$. Then $[a, b]$ is certainly a square in $G$, so that by Sun's law for squares $q^*$ is a square modulo $p$. Since $[a, b] \neq [1, 0]$ (by our assumption that $q \nmid b$), we must have $[a, b] = [\beta, 1]^4$ for some $\beta$. Moreover, $\beta \neq 0$, since $[0, 1]^4 = [1, 0]^2 = [1, 0]$. Let $\kappa$ be defined by

$$[\kappa, 1] = [\beta, 1]^2 \quad \text{so that } \kappa = \frac{\beta^2 - 1}{2\beta}.$$

Then $\kappa \star \kappa = [a, b]$. By Dirichlet's law, Lemma 5.10 and Lemma 5.11,

$$\left(\frac{q}{p}\right)_4 = \left(\frac{\sqrt{p}(\sqrt{p}+b)}{q}\right) = \left(\frac{\kappa^2+1}{q}\right) = 1;$$

this completes the proof of Theorem 5.9. □

**Corollary 5.12.** *Let $p$ and $q$ be distinct odd primes with $p \equiv 1 \pmod 4$, and write $p = a^2 + b^2$ with $b$ even. Then in $\mathbf{F}_q(i)$*

$$\left(\frac{q^*}{p}\right)_4 = \left(\frac{a+bi}{a-bi}\right)^{(q-(\frac{-1}{q}))/4}, \tag{47}$$

*provided at least one side is defined and equal to $\pm 1$.*

*Proof.* We claim that we can assume $\left(\frac{q^*}{p}\right) = 1$, i.e., that the the left hand side is defined. In the case when the right hand side is equal to $\pm 1$, let $\psi$ be the injection into $\mathbf{F}_q(i)^*$ mentioned above. Then

$$\psi([a, b])^{(q-(\frac{-1}{q}))/2} = (\pm 1)^2 = 1.$$

It follows that $\psi([a, b])$ a square in $\psi(G)$, so that $[a, b]$ is a square in $G$. But by that portion of Theorem 5.9 concerned with squares,

$$[a, b] \text{ is a square in } G \Longleftrightarrow \left(\frac{q^*}{p}\right) = 1. \tag{48}$$

This proves the claim.

Since $[a, b]$ is a square in $G$ (by another reference to (48)), we have

$$\psi([a, b])^{\#G/2} = 1,$$

hence

$$\left(\frac{a+bi}{a-bi}\right)^{(q-(\frac{-1}{q}))/2} = 1, \quad \text{and} \quad \left(\frac{a+bi}{a-bi}\right)^{(q-(\frac{-1}{q}))/4} = \pm 1.$$

But using that portion of Theorem 5.9 concerned with fourth powers,

$$\left(\frac{q^*}{p}\right)_4 = 1 \iff [a,b] \text{ is a fourth power in } G$$

$$\iff \psi([a,b]) \text{ is a fourth power in } \psi(G) \iff \left(\frac{a+bi}{a-bi}\right)^{(q-\left(\frac{-1}{q}\right))/4} = 1,$$

and so the result follows. □

We leave as Exercise 34 the converse task of deducing Theorem 5.9 from Corollary 5.12.

## 6. Burde's Rational Quartic Reciprocity Law

**Theorem 6.1** (K. Burde)**.** *Let $p$ and $q$ be distinct primes with $p \equiv q \equiv 1 \pmod 4$, and write $p = a^2 + b^2$ and $q = c^2 + d^2$ where $2 \mid b$ and $2 \mid d$. Suppose that $\left(\frac{p}{q}\right) = 1$. Then*

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{ac-bd}{q}\right), \text{ or equivalently}$$
$$= (-1)^{(q-1)/4}\left(\frac{ad-bc}{q}\right).$$

The following proof of Theorem 6.1 was communicated to the author by Zhi-Hong Sun:

**Lemma 6.2** (Z.-H. Sun [97, Theorem 1(1)])**.** *Let $q$ be an odd prime and $b$ and $c$ elements of $\mathbf{F}_q$ with $c(b+c) \neq 0$ and $\left(\frac{b^2-c^2}{q}\right) = 1$. Then*

$$\left(\frac{b+c}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{b+\sqrt{b^2-c^2}}{q}\right)$$

*for either choice of the square root.*

*Proof.* Since $c(b+c) \neq 0$, we have both

$$b + c \neq 0 \quad \text{and} \quad b + \sqrt{b^2-c^2} \neq 0.$$

Hence the algebraic identity

$$(b+c)\left(\frac{b+\sqrt{b^2-c^2}}{2}\right) = \left(\frac{b+c+\sqrt{b^2-c^2}}{2}\right)^2,$$

implies that

$$\left(\frac{b+c}{q}\right)\left(\frac{2}{q}\right)\left(\frac{b+\sqrt{b^2-c^2}}{q}\right) = 1,$$

and multiplying both sides of this identity by $\left(\frac{b+c}{q}\right)$ finishes the proof. □

*Proof of Theorem 6.1.* Choose $\sqrt{p}$ in $\mathbf{F}_q$ so that $b + \sqrt{p}$ is nonvanishing. Then by Dirichlet's law (Theorem 5.3),

(49)
$$\left(\frac{q}{p}\right)_4 = \left(\frac{\sqrt{p}(b+\sqrt{p})}{q}\right) = \left(\frac{p}{q}\right)_4\left(\frac{b+\sqrt{p}}{q}\right), \quad \text{and so} \quad \left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = \left(\frac{b+\sqrt{p}}{q}\right).$$

Write $d = 2^e d_0$, where $d_0$ is odd. Since $q = c^2 + d^2$, we have $q \equiv 5 \pmod 8$ if and only if $e = 1$, and $q \equiv 1 \pmod 8$ otherwise. It follows that $\left(\frac{2}{q}\right)^e = \left(\frac{2}{q}\right)$, and so

$$\left(\frac{d}{q}\right) = \left(\frac{2}{q}\right)^e \left(\frac{d_0}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{q_0}{d}\right) = \left(\frac{2}{q}\right).$$

Now applying Lemma 6.2 with the given value of $b$ and with $c = \sqrt{p}$ we find

$$\begin{aligned}\left(\frac{b+\sqrt{p}}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{b+\sqrt{-a^2}}{q}\right) &= \left(\frac{2}{q}\right)\left(\frac{b+a(-c/d)}{q}\right)\\ &= \left(\frac{2}{q}\right)\left(\frac{d}{q}\right)\left(\frac{ac-bd}{q}\right) = \left(\frac{ac-bd}{q}\right).\end{aligned}$$

Similarly, using instead $-d/c$ to replace $\sqrt{-1} \pmod q$, we find

$$\begin{aligned}\left(\frac{b+\sqrt{p}}{q}\right) &= \left(\frac{2}{q}\right)\left(\frac{b+\sqrt{-a^2}}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{b+a(-d/c)}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{c}{q}\right)\left(\frac{bc-ad}{q}\right)\\ &= ((-1)^{(q+1)/2})^{(q-1)/4}\left(\frac{q}{c}\right)\left(\frac{ad-bc}{q}\right) = (-1)^{(q-1)/4}\left(\frac{ad-bc}{q}\right).\end{aligned}$$

Comparing with (49) yields the theorem. □

## 7. The Schönemann-Scholz-Lehmer Law

**Theorem 7.1.** *Let $p$ and $q$ be distinct primes, both congruent to* $1 \mod 4$, *and suppose that $\left(\frac{p}{q}\right) = 1$. Let $\epsilon_p$ and $\epsilon_q$ be the fundamental units of $\mathbf{Q}(\sqrt{p})$ and $\mathbf{Q}(\sqrt{q})$, respectively. Then*

$$\left(\frac{\epsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = \left(\frac{\epsilon_p}{q}\right). \tag{50}$$

*These assertions hold regardless of the choices of $\sqrt{p} \in \mathbf{F}_q$ and $\sqrt{q} \in \mathbf{F}_p$.*

For the fundamental unit $\epsilon_2 = 1 + \sqrt{2}$ of $\mathbf{Q}(\sqrt{2})$ we have:

**Theorem 7.2** (Schönemann-Scholz-Lehmer Supplementary Law)**.** *For every prime* $p \equiv 1 \pmod 8$ *we have*

$$\left(\frac{2}{p}\right)_4\left(\frac{p}{2}\right)_4 = \left(\frac{\epsilon_2}{p}\right), \quad \textit{where } \left(\frac{p}{2}\right)_4 := (-1)^{(p-1)/8}.$$

This law has a curious history. It was conjectured by Emma Lehmer ca. 1970; after devising her own proof (which appears in [73]), she discovered Scholz's Law as the fourth of five-part theorem in a difficult 1934 paper of Scholz [93]. Recently Lemmermeyer unearthed the law in an 1839 paper of Schönemnan [94]. The proof we present is due to Williams [107], and incorporates a patch of Lemmermeyer [78, Exercise 5.10].

We need a few lemmas from the theory of quadratic fields; references are to H. Cohn's book [12].

**Lemma 7.3.** *Let* $q \equiv 1 \pmod 4$ *be prime, and let $R$ be the ring of integers of $\mathbf{Q}(\sqrt{q})$. If $\alpha$ is an element of $R$ of odd norm, then $\alpha^3 \in \mathbf{Z}[\sqrt{q}]$.*

*Proof.* If 2 is inert then $R/2R \cong \mathbf{F}_4$, while if 2 splits then $R/2R \cong \mathbf{F}_2 \oplus \mathbf{F}_2$; in both cases the size of the unit group $(R/2R)^*$ divides 3. The assumption that $\alpha$ has odd norm implies that $\alpha$ is a unit in $R/2R$, hence $\alpha^3 \equiv 1 \pmod 2$. Consequently,

$$\alpha^3 \in 1 + 2R = 1 + 2\left(\mathbf{Z} \oplus \mathbf{Z}\frac{1+\sqrt{q}}{2}\right) \subset \mathbf{Z} \oplus \mathbf{Z}\sqrt{q}. \qquad \square$$

**Lemma 7.4.** *Let $q \equiv 1 \pmod 4$ be prime. Then the fundamental unit $\epsilon_q$ of $\mathbf{Q}(\sqrt{q})$ has norm $-1$. Also*

$$\epsilon_q^3 = T + U\sqrt{q} \quad \textit{for positive integers} \quad T, U,$$

*where $T$ is even and every positive divisor of $U$ (including $U$ itself) is congruent to* $1 \pmod 4$.

*Proof (sketch).* That $\epsilon_q$ has norm $-1$ follows from [12, Theorem 3 (p. 185)]. Write

$$\epsilon_q^3 = T + U\sqrt{q}, \qquad \text{so that } T \text{ and } U \text{ are positive.}$$

By Lemma 7.3, $T$ and $U$ are integers. Looking at the relation $T^2 - qU^2 = -1$ modulo 4 we find that $T$ must be even and $U$ odd. The same equation also implies that $-1$ is a square modulo $U$, and this yields the final claim. □

**Lemma 7.5.** *Let $p$ and $q$ be as in Theorem 7.1. Then for a certain odd positive integer $\lambda$ we can write*

$$p^\lambda = u^2 - 4qv^2 \quad \textit{with positive coprime integers } u, v.$$

*Proof (sketch).* Since $\left(\frac{q}{p}\right) = 1$, the prime $p$ splits as a product of two prime ideals in $R$, say $(p) = \mathfrak{p}\mathfrak{p}'$. Let $h$ be the class number of $R$. Then $h$ is odd [12, Theorem 6, p.187]. The ideal $\mathfrak{p}^h$ is principal. By Lemma 7.4, we can choose a generator, say $\pi$, with norm $p^h$. Since $\pi^3 \in \mathbf{Z}[\sqrt{q}]$ by Lemma 7.3 we can write $\pi^3 = x + y\sqrt{q}$ for certain integers $x$ and $y$.

We now have

$$x^2 - qy^2 = N(\pi^3) = N(\pi)^3 = p^{3h}. \tag{51}$$

Examining (51) modulo 4, we find that $x$ must be odd and $y$ even. We take $u = x$ and $v = y/2$, and check that $u$ and $v$ so defined are coprime; the lemma then follows with this choice of $u$ and $v$ and with $\lambda := 3h$.

To prove $u$ and $v$ coprime it suffices to prove that $x$ and $y$ are coprime. Suppose the prime $r$ divides both $x$ and $y$; by (51) we must have $r = p$. But then

$$\mathfrak{p}' \mid (r) \mid (x + y\sqrt{q}) = (\pi^3) = \mathfrak{p}^{3h},$$

contradicting uniqueness of factorization into prime ideals. □

*Proof of Theorem 7.1.* We begin with some preliminary observations: By symmetry it suffices to prove the first equality in (50), i.e.,

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{\epsilon_q}{p}\right).$$

Moreover, we can easily establish the final clause about the independence of the choice of $\sqrt{q} \pmod p$: if we define $\epsilon_q$ modulo $p$ by using a particular value of $\sqrt{q}$ $(\text{mod } p)$ and define $\epsilon_q'$ by using the opposite value, then

$$\left(\frac{\epsilon_q}{p}\right)\left(\frac{\epsilon_q'}{p}\right) = \left(\frac{-1}{p}\right) = 1, \quad \text{whence } \left(\frac{\epsilon_q}{p}\right) = \left(\frac{\epsilon_q'}{p}\right).$$

We get our choice of $\sqrt{q} \in \mathbf{F}_p$ by fixing a representation $p^\lambda = u^2 - 4qv^2$ of the type considered in Lemma 7.5 and setting

$$\sqrt{q} := u/2v \pmod{p}.$$

Now

$$\left(\frac{\epsilon_q}{p}\right) = \left(\frac{\epsilon_q^3}{p}\right) = \left(\frac{T + U\sqrt{q}}{p}\right) = \left(\frac{T + Uu/2v}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{v}{p}\right)\left(\frac{2Tv + Uu}{p}\right).$$

Let $t = \gcd(U, v)$, and define $U'$, $v'$ and $W$ by

$$U = tU', \quad v = tv', \quad \text{and} \quad 2Tv + Uu = tW, \text{ so that } W = 2Tv' + U'u. \tag{52}$$

Then

$$\left(\frac{\epsilon_q}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{v}{p}\right)\left(\frac{t}{p}\right)\left(\frac{W}{p}\right). \tag{53}$$

Now we have

$$\left(\frac{t}{p}\right) = \left(\frac{p}{t}\right) = \left(\frac{p^\lambda}{t}\right) = \left(\frac{u^2 - 4qv^2}{t}\right) = \left(\frac{u^2}{t}\right) = 1. \tag{54}$$

Also

$$\left(\frac{W}{p}\right) = \left(\frac{p}{W}\right) = \left(\frac{p^\lambda}{W}\right) = \left(\frac{u^2 - 4qv^2}{W}\right), \tag{55}$$

and since

$$\gcd(W, U') = \frac{1}{t}\gcd(2Tv + Uu, U) = \frac{1}{t}\gcd(2Tv, U) = 1,$$

we have

$$\begin{aligned} \left(\frac{u^2 - 4qv^2}{W}\right) &= \left(\frac{U'^2u^2 - 4qU'^2v^2}{W}\right) \\ &= \left(\frac{4T^2v'^2 - 4qU'^2v^2}{W}\right) \\ &= \left(\frac{4T^2v'^2 - 4qU^2v'^2}{W}\right) = \left(\frac{4v'^2}{W}\right)\left(\frac{-1}{W}\right) = \left(\frac{-1}{W}\right). \end{aligned} \tag{56}$$

We have used here that $U'^2u^2 \equiv 4T^2v'^2 \pmod{W}$ (which follows from the last equality of (52)). We've also used that $2v'$ is coprime to $W$ – this follows from the coprimeness of $u$ and $v$, the definitions (52) and the observation that $uU'$ is odd.

Since $T$ is even and $U' \equiv 1 \pmod 4$, we have $W = 2Tv' + U'u \equiv u \pmod 4$, hence

$$\left(\frac{-1}{W}\right) = \left(\frac{-1}{u}\right). \tag{57}$$

From equations (53)-(57),

$$\left(\frac{\epsilon_q}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{v}{p}\right)\left(\frac{-1}{u}\right). \tag{58}$$

Since $qp^\lambda = qu^2 - 4q^2v^2$,

$$\left(\frac{-1}{u}\right) = \left(\frac{-4q^2v^2}{u}\right) = \left(\frac{qp^\lambda}{u}\right) = \left(\frac{qp}{u}\right) = \left(\frac{q}{u}\right)\left(\frac{p}{u}\right) = \left(\frac{u}{q}\right)\left(\frac{u}{p}\right),$$

and substituting this into (58) we obtain

$$\left(\frac{\epsilon_q}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{v}{p}\right)\left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = \left(\frac{2}{p}\right)\left(\frac{(vu)^2}{p}\right)_4\left(\frac{u^2}{q}\right)_4.$$

Since

$$u^2 \equiv p^\lambda \pmod{q} \quad \text{and} \quad v^2u^2 \equiv v^2 \cdot 4qv^2 \equiv 4qv^4 \pmod{p},$$

we have

$$\left(\frac{u^2}{q}\right)_4 = \left(\frac{p^\lambda}{q}\right)_4 = \left(\frac{p}{q}\right)_4 \quad \text{and} \quad \left(\frac{(vu)^2}{p}\right)_4 = \left(\frac{4q}{p}\right)_4\left(\frac{v^4}{p}\right)_4 = \left(\frac{4q}{p}\right)_4.$$

Putting everything together gives

$$\left(\frac{\epsilon_q}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{4q}{p}\right)_4\left(\frac{p}{q}\right)_4 = \left(\frac{2}{p}\right)\left(\frac{2}{p}\right)\left(\frac{q}{p}\right)_4\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4\left(\frac{p}{q}\right)_4,$$

as asserted. □

*Proof of the Supplementary Law.* Over the complex numbers we have the identity

$$(1+\zeta_8)^2 = (1+i)(1+\sqrt{2}), \tag{59}$$

which can be verified by means of the relations

$$i = \zeta_8^2, \quad \sqrt{2} = \zeta_8 - \zeta_8^3. \tag{60}$$

Now let $p \equiv 1 \pmod 8$. Fix a primitive eighth root of unity $\zeta_8$ in $(\mathbf{Z}/p\mathbf{Z})^*$. If we define $i$ and $\sqrt{2}$ in $\mathbf{Z}/p\mathbf{Z}$ by (60), then $i^2 = -1$, $(\sqrt{2})^2 = 2$ and (59) remains valid. (We leave the straightforward verification of these identities to the reader; alternatively, one can give a "pure thought" proof – see Exercise 17.) Therefore

$$\left(\frac{1+\sqrt{2}}{p}\right) = \left(\frac{1+i}{p}\right). \tag{61}$$

Since

$$(1+i)^2 = (1+2i+i^2) = 2i \quad \text{and} \quad (1+i)^4 = (2i)^2 = -4,$$

we have

$$\left(\frac{1+i}{p}\right) = \left(\frac{-4}{p}\right)_8. \tag{62}$$

By (61) and (62),

$$\begin{aligned}\left(\frac{1+\sqrt{2}}{p}\right) = \left(\frac{1+i}{p}\right) = \left(\frac{-4}{p}\right)_8 &= \left(\frac{4}{p}\right)_8\left(\frac{-1}{p}\right)_8 \\ &= \left(\frac{2}{p}\right)_4\left(\frac{-1}{p}\right)_8 = \left(\frac{2}{p}\right)_4(-1)^{(p-1)/8} = \left(\frac{2}{p}\right)_4\left(\frac{p}{2}\right)_4,\end{aligned}$$

proving the theorem. □

In Exercise 44 we give a number of evaluations of $\left(\frac{-4}{p}\right)_8$; see also Exercise 5.

## 8. The Universal Rational Quartic Reciprocity Law

We mentioned in the introduction that all the quartic laws we've discussed can be seen as consequences of a general rational quartic law discovered by Friesen, Hardy & Williams [108]. Before stating this law, we introduce some convenient notation. If $m = p_1 \dots p_k$ is a product of (not necessarily distinct) primes for which $a$ is a nonzero square, then we define the rational quartic Jacobi symbol according to the rule

$$\left(\frac{a}{m}\right)_4 := \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)_4.$$

Then we have:

**Theorem 8.1** (Universal Rational Quartic Law). *Let $m = p_1 p_2 \dots p_k$ be a product of distinct primes $p_i \equiv 1 \pmod 4$. Let $A, B$ and $C$ be integers such that*

$$A^2 = m(B^2 + C^2), \quad 2|B,$$
$$(A, B) = (B, C) = (C, A) = 1, \quad A + B \equiv 1 \pmod 4.$$

*If $q$ is an odd prime with $\left(\frac{q}{p_i}\right) = 1$ for every $i$, then*

$$\left(\frac{A + B\sqrt{m}}{q}\right) = \left(\frac{q}{m}\right)_4 \tag{63}$$

*provided $\sqrt{m}$ in $\mathbf{F}_q$ is chosen so that $A + B\sqrt{m}$ is nonvanishing.*

For applications we note that the following easy corollary:

**Corollary 8.2.** *If we replace in Theorem 8.1 the hypothesis that $A+B \equiv 1 \pmod 4$ with the hypothesis that $q \equiv 1 \pmod 4$, then the the conclusion (63) still holds.*

*Proof.* We may suppose that $q \equiv 1 \pmod 4$ and $A + B \equiv -1 \pmod 4$. Then the original hypotheses of the theorem hold with $A$ replaced by $-A$ and the opposite choice of $\sqrt{m}$. Since $q \equiv 1 \pmod 4$, we have $\left(\frac{-A-B\sqrt{m}}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{A+B\sqrt{m}}{q}\right) = \left(\frac{A+B\sqrt{m}}{q}\right)$ and so (63) still holds. □

To illustrate the power of Theorem 8.1, we offer the following quick proof of Dirichlet's Quartic Reciprocity Law:

*Proof of Dirichlet's Quartic Law using Theorem 8.1.* We separate off to the end the case when both $q \equiv 3 \pmod 4$ and $p \equiv 5 \pmod 8$.

If either $q \equiv 1 \pmod 4$ or $p \equiv 1 \pmod 8$, then $\left(\frac{q^*}{p}\right)_4 = \left(\frac{q}{p}\right)_4$, and Dirichlet's law reads

$$\left(\frac{q}{p}\right)_4 = \left(\frac{\sqrt{p}(b + \sqrt{p})}{q}\right), \tag{64}$$

which is ready made for an application of Theorem 8.1. Since $\sqrt{p}(b+\sqrt{p}) = p+b\sqrt{p}$, we take $A = p, B = b, C = a$ and $m = p$. If $q \equiv 1 \pmod 4$, then by Corollary 8.2 we can ignore the congruence condition on $A + B$ when applying Theorem 8.1. If $p \equiv 1 \pmod 8$, then we can check the congruence condition: in this case $4 \mid b$, hence $A + B = p + b \equiv p \equiv 1 \pmod 4$. So in both cases Theorem 8.1 applies, and it immediately yields (64).

Suppose finally that $q \equiv 3 \pmod 4$ and $p \equiv 5 \pmod 8$. Then $q^* = -q$. Since $\left(\frac{-1}{p}\right)_4 = (-1)^{(p-1)/4} = -1$, we seek to prove

$$\left(\frac{q}{p}\right)_4 = -\left(\frac{\sqrt{p}(b+\sqrt{p})}{q}\right). \tag{65}$$

But now Theorem 8.1 is applicable with $A = -p, B = b, C = a, m = p$ and with $-\sqrt{p}$ in place of $\sqrt{p}$. This yields

$$\left(\frac{-b-\sqrt{p}}{q}\right) = \left(\frac{q}{p}\right)_4 \quad \text{hence} \quad \left(\frac{b+\sqrt{p}}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{q}{p}\right)_4 = -\left(\frac{q}{p}\right)_4,$$

as desired. □

In Exercises 47 and 48 we indicate how the universal rational quartic law can be used to prove generalizations of the Burde and Schönemann-Scholz-Lehmer laws.

We will not prove Theorem 8.1 here. But it is worth noting that the original proof of Friesen, Hardy & Williams is entirely elementary, requiring only Legendre's Theorem and crafty machinations with Jacobi symbols; thus it is eminently accessible to anyone who has made it this far. A very different proof, employing the methods of algebraic number theory, is described in Exercises 49-51.

## 9. Quadratic Exercises

**Exercise 1** (Reichardt [88])**.** Prove that the equation $x^4 + 17y^4 = 2z^2$ has no solution in integers $x, y$, and $z$ not all vanishing. (*Hint:* use quadratic reciprocity to show that $z$ is quadratic residue modulo 17. Now obtain a contradiction to 2 being a quartic nonresidue of the same modulus.)

Of course $x^4 + 17y^4 = 2z^2$ has real solutions, and it can be shown that it also has nontrivial solutions modulo every prime power – we thus have a counterexample to the "local-global principle." For an elementary proof of this last fact, see the article of Aitken & Lemmermeyer [1].

**Exercise 2.** Let $q$ be a prime greater than 3, and let $G = G(q)$ be the group considered in the proof of the Jacobi-Sun cubic reciprocity law. Show that the element $[1,1]$ has order 3; hence $3 \mid \#G$. From the formula $\#G = q - \left(\frac{-3}{q}\right)$, deduce that $\left(\frac{-3}{q}\right) = 1$ if and only if $q \equiv 1 \pmod 3$. Using instead the groups considered in the proof of the Dirichlet-Sun law, give an analogous proof of the first supplementary law concerning $\left(\frac{-1}{p}\right)$. These proofs are due to David Harden.

**Exercise 3** (continuation)**.** Let $p$ be an odd prime and let $G = G(p)$ be the group appearing in the proof of the Dirichlet-Sun law. Fill in the following series of implications which together yield an alternate derivation of the quadratic character of 2:

$$\begin{aligned} p \equiv \pm 1 \pmod 8 &\Longleftrightarrow 8 \mid \#G \\ &\Longleftrightarrow G \text{ contains an element of order } 8 \\ &\Longleftrightarrow \text{the element } [1,1] \text{ of order 4 has a square root in } G \\ &\Longleftrightarrow \left(\frac{2}{p}\right) = 1. \end{aligned}$$

**Exercise 4** (Gauss, Dirichlet)**.** Write out the details in the following proof by descent for the second supplementary law: $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

(i) First prove that $\left(\frac{2}{p}\right) = -1$ for $p \equiv 3, 5 \pmod 8$: supposing otherwise, let $p$ be the smallest counterexample, and choose $0 < e < p$ odd with $e^2 \equiv 2 \pmod p$. Then $e^2 - 2 = pf$. Then $0 < f < p$, and 2 is a square modulo every prime $q$ dividing $f$. We can choose such a prime $q \equiv 3, 5 \pmod 8$, and this contradicts the minimality of $p$.

(ii) Give an analogous proof that $\left(\frac{-2}{p}\right) = -1$ for $p \equiv 5, 7 \pmod 8$. Deduce from the first supplementary law that $\left(\frac{2}{p}\right) = -1$ for $p \equiv 3, 5 \pmod 8$ and $\left(\frac{2}{p}\right) = 1$ for $p \equiv 7 \pmod 8$.

(iii) So if $q$ is the smallest exception to the second supplementary law, then $q \equiv 1 \pmod 8$ while $\left(\frac{2}{q}\right) = -1$. Choose $p < q$ with $\left(\frac{p}{q}\right) = -1$; then (we assume QR for this part of the exercise) also $\left(\frac{q}{p}\right) = -1$, and $\left(\frac{2p}{q}\right) = 1$. Choose an odd $e$ with $0 < e < q$ and $e^2 \equiv 2p \pmod q$. Then

$$e^2 - 2p = qf \tag{66}$$

for an odd $f$ with $|f| < q$. We now take two cases, according as $p$ divides $f$ or $p$ is prime to $f$. In the latter case, the hypothesis on $q$ together with (66) implies $\left(\frac{f}{p}\right) = -1$. But by quadratic reciprocity and (66),

$$\left(\frac{f}{p}\right) = (-1)^{\frac{p-1}{2}\frac{f-1}{2}}\left(\frac{p}{f}\right) = (-1)^{\frac{p-1}{2}\frac{f-1}{2}}\left(\frac{-1}{f}\right)\left(\frac{2}{f}\right).$$

Using the evaluations $\left(\frac{-1}{f}\right) = (-1)^{(f-1)/2}$ and $\left(\frac{2}{f}\right) = (-1)^{(f^2-1)/8}$ (the latter of which follows from the minimality of $p$), show the right hand side here has the value $+1$. Obtain a similar contradiction in the remaining case when $p$ divides $f$.

The proofs in parts (1) and (2) are due to Gauss and can be found in his *Disquisitiones* [40, Art. 111-113]. Part (3) is due to Dirichlet [20, §7]. The case $p \equiv 1 \pmod 8$ is also treated by Gauss [40, Art. 114-115], but not by descent: he notes that for such primes there exists a primitive 8th root of unity $\zeta_8 \in \mathbf{F}_p^*$, and $2 = (\zeta_8 + \zeta_8^{-1})^2$.

**Exercise 5** (Quadratic Reciprocity for $\mathbf{Z}[i]$)**.** If $\pi$ is a Gaussian prime and $\alpha$ a Gaussian integer not divisible by $\pi$, we define the Legendre symbol $\left[\frac{\alpha}{\pi}\right]$ in $\mathbf{Z}[i]$ by

$$\left[\frac{\alpha}{\pi}\right] = \begin{cases} 1 & \text{if } \alpha \text{ is a square modulo } \pi, \\ -1 & \text{otherwise.} \end{cases}$$

Here we show that if $\pi = a + bi$ and $\lambda = c + di$ are nonassociated Gaussian primes both congruent to 1 (mod 2), then $\left[\frac{\pi}{\lambda}\right] = \left[\frac{\lambda}{\pi}\right]$. This law was discovered by Gauss and stated in [33]; the simple proof we outline here is due to Dirichlet [19].

(i) Prove the law in the case where both $\pi$ and $\lambda$ are rational primes.

(ii) Prove that if $\pi = p$ is a rational prime while $\lambda$ is a Gaussian prime with prime norm $l$, then $\left[\frac{\lambda}{\pi}\right] = \left(\frac{l}{p}\right)$. Use this to prove the reciprocity law for the pair $\pi$ and $\lambda$.

(iii) Prove that if $\pi$ and $\lambda$ are Gaussian primes with prime norms $p$ and $l$, then

$$\left[\frac{\pi}{\lambda}\right] = \left(\frac{d}{l}\right)\left(\frac{ad - bc}{l}\right). \tag{67}$$

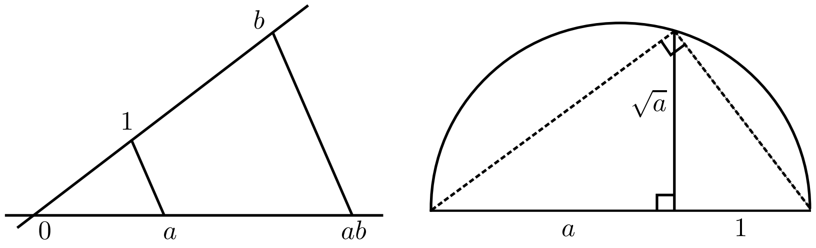


FIGURE 3. Figures accompanying Exercise 6. The left-hand diagram illustrates that if $a$ and $b$ are constructible numbers, then so is $ab$. The right-hand figure indicates the construction of $\sqrt{a}$ for a constructible number $a > 0$.

Using the identiy

$$(ac+bd)^2 + (ad-bc)^2 = pl,$$

prove that

$$\left(\frac{ad-bc}{l}\right) = \left(\frac{ac+bd}{l}\right)\left(\frac{-1}{l}\right)_4 = \left(\frac{ac+bd}{l}\right)(-1)^{(l-1)/4}. \tag{68}$$

Using the usual law of quadratic reciprocity, prove that $\left(\frac{d}{l}\right) = \left(\frac{2}{l}\right) = (-1)^{(l-1)/4}$. From this, equation (68) and (67), conclude that

$$\left[\frac{\pi}{\lambda}\right] = \left(\frac{ac+bd}{l}\right).$$

(iv) Prove the supplementary laws

$$\left[\frac{i}{\pi}\right] = (-1)^{\frac{N(\pi)-1}{4}} \quad \text{and} \quad \left[\frac{1+i}{\pi}\right] = (-1)^{\frac{(a+b)^2-1}{8}}.$$

*Hint for the latter in the case when $N(\pi) = p$ is prime:* First prove that $\left[\frac{1+i}{p}\right] = \left(\frac{b}{p}\right)\left(\frac{b-a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{b-a}{p}\right)$. Now evaluate $\left(\frac{b-a}{p}\right)$ using quadratic reciprocity and the identity $2p = (b-a)^2 + (b+a)^2$.

(v) Formulate and prove an analog of Jacobi's law of quadratic reciprocity. Extend the supplementary laws in a similar way.

For quadratic reciprocity in other quadratic number fields, see [79].

## 10. Cyclotomy Exercises

**Exercise 6** (Proof of Lemma 3.2)**.** Say that a real number $\alpha$ is *real-constructible* if it is possible to construct two points a distance $|\alpha|$ apart.

(i) Prove (or look up) the following (geometric) lemma: If $\alpha$ and $\beta$ are two real-constructible numbers, then so are

$$\alpha \pm \beta, \quad \alpha\beta, \quad 1/\alpha \quad (\text{if } \alpha \neq 0), \quad \sqrt{\alpha} \quad (\text{if } \alpha \geq 0).$$

(Figure 3 may jog your memory.) Show moreover that the point $(x, y)$ is constructible if and only if its components $x$ and $y$ are both real-constructible. Hence the real-constructible numbers form a subfield of $\mathbf{R}$, say $\mathrm{Cons}_{\mathbf{R}}$.

(ii) Suppose we have a tower of subfields of the real numbers

$$\mathbf{Q} := K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m$$

with $\alpha \in K_m$ and each $K_i = K_{i-1}(\sqrt{\beta_i})$ for some nonnegative $\beta_i \in K_{i-1}$. Using part (i), prove that $\alpha$ is real-constructible.

(iii) Let $L$ be the line described by the equation $ax + by = c$, and let $C$ be the circle described by the equation $(x - x_0)^2 + (y - y_0)^2 = r^2$. Let $K = \mathbf{Q}(a, b, c, x_0, y_0, r)$. Prove that each coordinate of a point of intersection of $L$ and $C$ lies either in $K$ or in a quadratic extension of $K$.

(iv) Use (iii) to prove the converse of (ii): if $\alpha$ is real-constructible, then there is such a tower whose last term contains $\alpha$.

(v) Prove that the point $(x, y)$ is constructible if and only if $x + yi \in \mathrm{Cons}_{\mathbf{R}}(i)$. Now prove that the elements of (the field!) $\mathrm{Cons}_{\mathbf{R}}(i)$ are exactly the elements described in Lemma 3.2. For one containment you may find helpful the identity

$$\sqrt{x+iy} = \frac{1}{2}\sqrt{2}\left(\sqrt{\sqrt{x^2+y^2}+x} + i \,\mathrm{sgn}(y)\sqrt{\sqrt{x^2+y^2}-x}\right).$$

Here $\mathrm{sgn}(y) = \pm 1$ is defined as $y/|y|$ for $y \neq 0$ and defined to be 0 at $y = 0$.

**Exercise 7.** Prove that it is possible to construct the vertices of a regular $n$-gon if and only if some primitive $n$th root of unity is constructible, in which case all primitive $n$th roots of unity are constructible.

**Exercise 8** (Gauss [40, Art. 354])**.** In this exercise we make explicit Theorem 3.4 for the case $p = 17$. We use the notation of Figure 2 for the Gaussian periods.

(i) Using Lemma 3.15, prove the polynomial identities
  (a) $(x - (8,1))(x - (8,3)) = x^2 + x - 4$,
  (b) $(x - (4,1))(x - (4,9)) = x^2 - (8,1)x - 1$,
  (c) $(x - (4,3))(x - (4,10)) = x^2 - (8,3)x - 1$,
  (d) $(x - (2,1))(x - (2,3)) = x^2 - (4,1)x + (4,3)$.
  (e) $(x - (1,1))(x - (1,16)) = x^2 - (2,1)x + 1$.

(ii) Show that one can choose the primitive 17th root of unity $\zeta$ so that

$$(8,1) = \frac{-1+\sqrt{17}}{2} \text{ and } (4,1) = \frac{(8,1)+\sqrt{(8,1)^2+4}}{2}.$$

Of course the difficulty is in proving that we can make the plus sign hold in both places.

(iii) These choices of sign force a choice of sign for $(4,3)$ in (c): to see this, prove that

$$((4,1) - (4,9))\,((4,3) - (4,10)) = 2\,((8,1) - (8,3)) > 0,$$

and deduce that $(4,3) = \frac{1}{2}((8,3) + \sqrt{(8,3)^2 + 4})$.

(iv) Prove that we can choose $\zeta$ as above for which

$$(2,1) = \frac{(4,1)+\sqrt{(4,1)^2-4(4,3)}}{2};$$

again, the nontrivial aspect is to prove we can force the plus sign. (Note that $(4,1)^2 - 4(4,3) > 0$, as follows from a rough numerical calculation.)

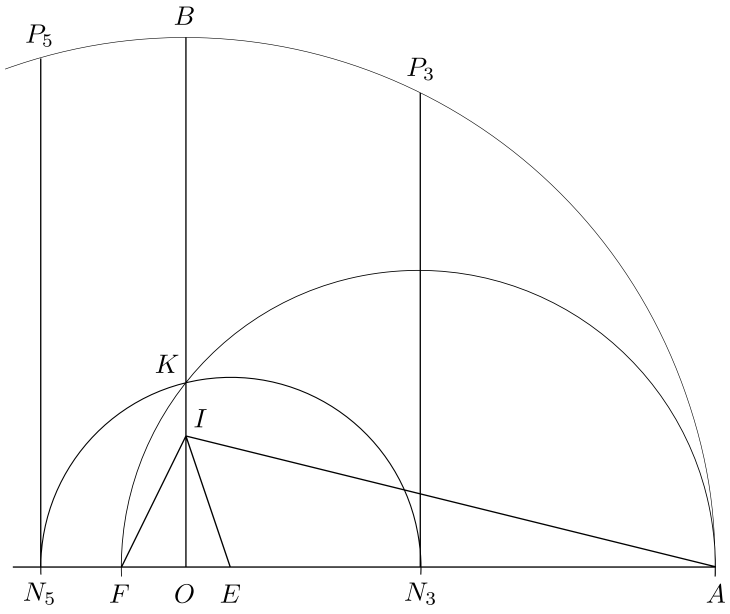


FIGURE 4. Diagram accompanying Richmond's construction of the 17-gon (see Exercise 9).

(v) We have

$$(2,1) = \zeta + \zeta^{g^8} = \zeta + \zeta^{-1} = 2\Re(\zeta).$$

Obtain a rough numerical approximation (on a calculator, say) of $(2,1)$ sufficient to prove to pin down $\zeta$ to one of the two values $e^{\pm 2\pi i/17}$; hence $(2,1) = 2\cos\frac{2\pi}{17}$.

(vi) Prove that $e^{2\pi i/17}$ and $e^{-2\pi i/17}$ are the roots of $x^2 - (2,1)x + 1$.

(vii) Combining (i)-(v), show that

$$(2,1) = 2\cos\frac{2\pi}{17} = \frac{1}{8}\sqrt{34 - 2\sqrt{17}} - \frac{1}{8} + \frac{1}{8}\sqrt{17} +$$
$$\frac{1}{8}\sqrt{68 + 12\sqrt{17} - 2\sqrt{34 - 2\sqrt{17}} + 2\sqrt{34 - 2\sqrt{17}}\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}}}.$$

Now use (vi) to compute an explicit representation of $\zeta_{17}$. (You may wish to use a computer algebra system for this part.)

Lecture 7 of [86] is a self-contained account of the results of this exercise; see also Hardy & Wright [47, §5.8].

**Exercise 9.** The result of the preceding exercise gives us an explicit way of constructing the 17-gon – however, such a direct attack is both inefficient and onerous. In 1893, Richmond proposed the following direct geometric construction ([89], [90]):

> Let $OA, OB$ [Figure 4] be two perpendicular radii of a circle. Make $OI$ one-fourth of $OB$, and the angle $OIE$ one-fourth of $OIA$; also

> find in $OA$ produced a point $F$ such that $EIF$ is 45°. Let the circle on $AF$ as diameter cut $OB$ in $K$, and let the circle whose centre is $E$ and radius $EK$ cut $OA$ in $N_3$ and $N_5$; then if ordinates $N_3P_3$, $N_5P_5$ are drawn to the circle, the arcs $AP_3$, $AP_5$ will be $3/17$ and $5/17$ of the circumference.

Prove Richmond's assertions. If you have trouble with this, Hardy & Wright [47, §5.8] present his construction in detail.

**Exercise 10** (Luca [82])**.** Using the Gauss-Wantzel Theorem, show that if the regular $(n-1)$-gon and $n$-gon are both constructible, then $n$ is a Fermat prime or $n \in \{2 \cdot 3, 2^2, 2^{2^2}, 2^{2^3}, 2^{2^4}, 2^{2^5}\}$. Proceed as follows:

(i) Consider a nonempty product of distinct Fermat numbers

$$F_{n_0} F_{n_1} \cdots F_{n_{k-1}}, \tag{69}$$

where $0 \leq n_0 < n_1 < \cdots < n_{k-1}$.

(a) Prove that this product has precisely $2^k$ nonzero digits in its binary expansion.

(b) Moreover, there are $1 + 2^{n_0} + 2^{n_1} + \cdots + 2^{n_{k-1}}$ total binary digits in this product. Thus, if we start with the number of binary digits in the product, subtract one and compute the binary expansion, we can read off the $n_i$ corresponding to the Fermat number factors.

(ii) Using (a), prove that any odd number $n$ with the property of the problem statement must be a Fermat prime.

(iii) Using (b), prove that if $n$ is even with the stated property, and $n - 1 \equiv 1 \pmod 4$, then $n - 1 = F_1$, hence $n = 6$.

(iv) Finally, suppose $n$ is even with the stated property and $n - 1 \equiv 3 \pmod 4$. Then $n - 1$ can be written in the form (69), where $n_0 = 0$, $n_1 = 1$, $n_2 = 2$, $\ldots$, $n_{k'} = k'$ for a certain $k' \geq 0$ and $n_j \geq k' + 2$ for the remaining indices $k' < j < k$. In this case the binary expansion of $n - 1$ ends with precisely $2^{k'+1}$ trailing 1's, and the binary expansion of $n$ contains precisely $2^k - 2^{k'+1} + 1$ nonzero binary digits.

Now obtain a contradiction to (a) unless $k = k' + 1$, i.e., unless $n - 1 = F_0 F_1 \cdots F_{k'}$. Complete the proof making use of Euler's discovery that $F_5$ is composite.

**Exercise 11.** Let $p$ be a Fermat prime. Show that the $f$-nomial periods with $f > 1$ are all real. Conclude that the "rough numerical calculation" in part (iv) of the preceding exercise was superfluous.

**Exercise 12** (Gauss's Proof of the Irreducibility of $\Phi_p(x)$ [40, Art. 341])**.** Let $\zeta$ be a primitive $p$th root of unity and let $f$ be its minimal polynomial. Then $f(x) \in \mathbf{Z}[x]$. We now sketch Gauss's proof that $f$ has degree $p - 1$; thus $f(x) = \Phi_p(x)$ and so $\Phi_p(x)$ is irreducible.

(i) (A Lemma from [40, Art. 340]) Let $g(x_1, \ldots, x_d) \in \mathbf{Z}[x_1, \ldots, x_d]$ be an integral polynomial in $d \geq 1$ variables. Prove that if $c_1, \ldots, c_d$ are any integers, then

$$\sum_{k \pmod p} g(\zeta^{kc_1}, \ldots, \zeta^{kc_d})$$

is a rational integer divisible by $p$.

(ii) Let $d$ be the degree of $f$. Then we have $f(x) = \prod_{i=1}^{d}(x - \zeta_i^{c_i})$, for distinct integers $c_i$ in the range $1 \leq c_i \leq p-1$. Moreover, if $f^{(k)}(x) := \prod_{i=1}^{d}(x - \zeta_i^{kc_i})$, then the coefficients of $f^{(k)}$ are integral (for $k = 0, 1, 2, \dots$). *Hint:* Use the symmetric function theorem.

(iii) Prove that for each $k = 1, 2, \dots, p-1$, the inequality $f^{(k)}(x) > 0$ holds for every real $x$. *Hint:* Show that we can pair each factor in the product expansion of $f^{(k)}$ with its complex conjugate.

(iv) Prove that

$$\sum_{k=1}^{p-1} f^{(k)}(1) \equiv 0 \pmod p \quad \text{and} \quad \prod_{k=1}^{p-1} f^{(k)}(1) = p^d.$$

Deduce from the latter that for each $k = 1, \dots, p-1$, either $f^{(k)}(1) = 1$ or $p \mid f^{(k)}(1)$. From the above congruence, deduce that $p \mid f^{(k)}(1)$ for all $k = 1, \dots, p-1$. Conclude that $p - 1 \leq d$, so that (since $d \leq p-1$) we must have $d = p-1$.

This sketch owes much to an expository article of Savitt on the mathematics of Gauss [92].

**Exercise 13** (Irreducibility of the General Cyclotomic Polynomial)**.** Let $\zeta$ be a primitive $n$th root of unity, and let $f(x)$ be its minimal polynomial. We have $f(x) \in \mathbf{Z}[x]$, and we have the factorization $\Phi_n(x) = f(x)g(x)$ for some $g(x) \in \mathbf{Z}[x]$. We claim that $f(x) = \Phi_n(x)$.

(i) Show that it suffices to prove that $\zeta^p$ is a root of $f(x)$ for every prime $p$ not dividing $n$.

(ii) Suppose $\zeta^p$ is not a root of $f$ for a certain prime $p$ not dividing $n$. Prove that $f(x)$ divides $g(x)^p$ in $\mathbf{Z}[x]$.

(iii) Deduce that under this hypothesis, the reductions of $f(x)$ and $g(x)$ modulo $p$ have common factors in $\mathbf{F}_p[x]$. Conclude that $\Phi_n(x)$ has a repeated factor in $\mathbf{F}_p[x]$.

(iv) Obtain a contradiction by noting that $\Phi_n(x) \mid x^n - 1$ and proving that $x^n - 1$ has no multiple roots in the algebraic closure of $\mathbf{F}_p$.

**Exercise 14.** Here we give two further proofs for the irreducibility of the cyclotomic polynomials: Let $\zeta$ be a primitive $n$th root of unity with minimal polynomial $f$. Then $f(x)$ divides $\Phi_n(x)$ and to prove that $f = \Phi_n$ it suffices to prove that $\zeta^a$ is a root of $f$ for each $a$ coprime to $n$.

(i) Prove that a nonzero element of the ring $\mathbf{Z}[\zeta]$ is divisible by only finitely many rational primes $p$.

(ii) Prove that $p \mid f(\zeta^p)$ in the ring $\mathbf{Z}[\zeta]$ for every prime $p$ not dividing $n$.

(iii) (Grandjot [44]) We can now give a simple proof by means of Dirichlet's Theorem. Let $a$ be prime to $n$. Letting $p$ run through the primes congruent to $a$ mod $n$, show that the single element $f(\zeta^a)$ has infinitely many rational prime divisors; conclude from part (i) that $f(\zeta^a) = 0$ as desired.

(iv) (Landau [63]) Using (i) show that we can choose a real number $B$ (depending only on $n$) so that if $p > B$ is prime and $a$ is prime to $N$ then either $f(\zeta^a) = 0$ or $p \nmid f(\zeta^a)$.

Fix such a $B$, and fix a particular integer $a$ coprime to $n$. Choose a positive integer $m$ with $m \equiv a \pmod n$ and coprime to $\prod_{p \leq B} p$. Factor

$m = q_1 q_2 \dots q_j$ as a product of primes, and show successively that all of

$$\zeta^{q_1}, \zeta^{q_1 q_2}, \dots, \zeta^{q_1 \cdots q_j} = \zeta^a$$

are roots of $f$.

**Exercise 15.** Prove that if $\phi(n)$ is a power of 2 then $n = 2^e p_1 \dots p_k$ for some integer $e \geq 0$ and some distinct Fermat primes $p_1, p_2, \dots, p_k$.

**Exercise 16** (Kummer [59])**.** Let $e$ be a positive integer and suppose $p \equiv 1 \pmod{e}$ is an odd prime for which $g$ is a primitive root. Show that

$$\mathrm{ind}_g(l) + (1,0) + 2(2,0) + \cdots + (e-1)(e-1,0) \equiv \frac{p-1}{2} \pmod{l};$$

here $(1,0), (2,0), \dots$ represent the cyclotomic numbers introduced in definition 16. *Hint:* Examine the proof of Theorem 4.7. This proof is suggested by Gröger [46].

**Exercise 17** (Reading identities modulo $p$)**.** Let $f(x) \in \mathbf{Z}[x]$ be a polynomial with integer coefficients, irreducible over the integers. Let $\alpha$ be a root of $f$, and suppose that $p(\alpha) = 0$ for a certain $p(x) \in \mathbf{Z}[x]$. If $\overline{\alpha}$ is a root of $f$ in an arbitrary field $F$, then we also have the polynomial identity $p(\overline{\alpha}) = 0$.

As one application of this result, fill in the details of the "pure thought" argument suggested in the proof of Theorem 7.2 by taking $f(x) = \Phi_8(x)$.

*Remark.* For another application see Exercise 20. In both applications we start with a certain identity of complex algebraic numbers and translate it into an identity in a field $F$ of finite characteristic; this explains the title of the exercise.

**Exercise 18.** Let $p \equiv 1 \pmod 3$ be prime and let $\hat{\phi(x)} = x^3 - 3px - pL$ be the reduced cubic period polynomial. Observing that $|L| < 2\sqrt{p}$, prove that

$$\hat{\phi}(-2\sqrt{p}) < 0 < \hat{\phi}(-\sqrt{p}), \quad \hat{\phi}(\sqrt{p}) < 0 < \hat{\phi}(-\sqrt{p}), \quad \hat{\phi}(\sqrt{p}) < 0 < \hat{\phi}(2\sqrt{p}).$$

Deduce that $\hat{\phi}$ has a zero in each of the intervals $I_0 = (-2\sqrt{p}, -\sqrt{p})$, $I_1 = (-\sqrt{p}, \sqrt{p})$ and $I_2 = (\sqrt{p}, 2\sqrt{p})$.

*Remark.* Heath-Brown & Patterson [49] have shown that the relative density of primes $p \equiv 1 \pmod 3$ for which the specific root $\sum_{a \bmod p} e^{2\pi i a^3/p}$ lies in a given $I_k$ is just what one would naively expect: 1/3; this difficult theorem contradicted a century-plus-old conjecture of Kummer [57].

The next two exercises are concerned with Ankeny's Theorem 13.4. They assume familiarity with the basic properties of Gauss sums such as can be found in [51].

**Exercise 19** (Proof of Theorem 13.4)**.** Fix a prime $e$. Let $p$ and $q$ be primes distinct from each other and distinct from $e$ with $p \equiv 1 \pmod{e}$. Let $\zeta_e$ and $\zeta_p$ be fixed primitive $e$th and $p$th roots of unity in a fixed algebraic closure $\overline{\mathbf{F}}_q$ of $\mathbf{F}_q$. Finally, let $\chi\colon \mathbf{F}_p^* \to \overline{\mathbf{F}}_q^*$ be an $\overline{\mathbf{F}}_q$-valued character of order $e$. We define the Gauss sum $\tau_a(\chi)$ by

$$\tau_a(\chi) := \sum_{n=1}^{p-1} \chi(n)\zeta_p^{an}.$$

If $a = 1$ we write $\tau_1(\chi) = \tau(\chi)$.

(i) Prove that $\tau_a(\chi)\tau_{-a}(\chi^{-1}) = p$ for every $a$ not divisible by $p$. In particular, $\tau_a(\chi)$ is nonzero for all such $a$. *Hint:*

$$\tau_a(\chi)\tau_{-a}(\chi^{-1}) = \sum_{n,m\in\mathbf{F}_p^*} \chi(nm^{-1})\zeta_p^{a(n-m)} = \sum_{l\in\mathbf{F}_p^*} \chi(l) \sum_{m\in\mathbf{F}_p^*} \zeta_p^{am(l-1)}.$$

(ii) Let $f$ be the order of $q \pmod e$. Prove that $\tau(\chi)^{q^f} = \chi(q)^{-f}\tau(\chi)$.

(iii) Deduce from (ii) that $\tau(\chi)^e$ is fixed by the $q^f$th power map, and conclude that $\tau(\chi)^e \in \mathbf{F}_q(\zeta_e)$.

(iv) Using (i) and (ii), show that

$$\begin{aligned} q \text{ is an } e\text{th power mod } p &\iff (\tau(\chi)^e)^{\frac{q^f-1}{e}} = 1 \\ &\iff \tau(\chi)^e \text{ is an } e\text{th power in } \mathbf{F}_q(\zeta_e). \end{aligned}$$

(Where in the proof do we use that $e$ is prime?)

**Exercise 20** (continuation)**.** Here we consider the cases $e = 2$ and $e = 3$ which correspond to Gauss's quadratic reciprocity law and Jacobi's cubic reciprocity law.

(i) Let $e = 2$, so that the nontrivial character $\chi(\cdot)$ of order 2 can be identified with the Legendre symbol $\left(\frac{\cdot}{p}\right)$. Prove that $\tau_{-1}(\chi) = \chi(-1)\tau_1(\chi)$. Using part (i) of the preceding exercise, show that $\tau(\chi)^2 = \left(\frac{-1}{p}\right)p$, and deduce from Theorem 13.4 another proof of the law of quadratic reciprocity.

(ii) Now suppose $e = 3$. Using [51, Corollary, p.115] and the result of Exercise 17, prove that $\tau(\chi)^3 = p\pi$, where $\pi = \frac{L+3M\sqrt{-3}}{2}$ for certain integers $L, M$ satisfying $L^2 + 27M^2 = 4p$ and $L \equiv 1 \pmod 3$. Use this to deduce another proof of Jacobi's Cubic Reciprocity Law.

**Exercise 21** (Sign of the Quadratic Gauss Sum)**.** Let $p$ be an odd prime and $\zeta$ be a complex primitive $p$th root of unity. The sum $\tau := \sum_{a \pmod p} \left(\frac{a}{p}\right)\zeta^a$ is called a quadratic Gauss sum. Check that the method of Exercise 20(i) proves that $\tau^2 = \left(\frac{-1}{p}\right)p$. (Previously we worked over $\overline{\mathbf{F}}_q$ instead of $\mathbf{C}$, but all we really required was a field of characteristic not divisible by $p$.) Hence

$$\tau = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ \pm i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{70}$$

Determining which sign to put here is a difficult problem. The solution was obtained by Gauss, who showed that the plus sign holds in both places if $\zeta := e^{2\pi i/p}$. Here we outline an argument due to Schur for determining the sign (with this choice of $\zeta$); our version of the argument is taken from the book of Borevich & Shafarevich [6, Chapter 5, §4.3].

(i) Prove that $\sum_{a \pmod p} \left(\frac{a}{p}\right)\zeta^a = \sum_{b \pmod p} \zeta^{b^2}$. *Hint:* investigate what happens when you add $\sum_{a \pmod p} \zeta_p^a$ to the left hand side.

(ii) Define the matrix

$$A := (\zeta^{ij})_{0\le i,j\le p-1} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta & \zeta^2 & \dots & \zeta^{p-1} \\ 1 & \zeta^2 & \zeta^4 & \dots & \zeta^{2(p-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{p-1} & \zeta^{2(p-1)} & \dots & \zeta^{(p-1)^2} \end{pmatrix}.$$

Then $\tau = \sum_{i=1}^{p} \xi_i$, where the $\xi_i$ are the eigenvalues of $A$ counted with (algebraic) multiplicity.

(iii) Prove that

$$A^2 = (s_{k+l})_{0\le k,l\le p-1} = \begin{pmatrix} p & 0 & \dots & 0 \\ 0 & 0 & \dots & p \\ \vdots & \vdots & \ddots & \vdots \\ 0 & p & \dots & 0 \end{pmatrix}, \quad \text{where } s_j = \begin{cases} 0 & \text{if } p \nmid j, \\ p & \text{otherwise.} \end{cases}.$$

Now show that the characteristic polynomial of $A^2$ is $(t-p)^{(p+1)/2}(t+p)^{(p-1)/2}$. Recalling that the roots of the characteristic polynomial of $A^2$ are the squares of the roots of the characteristic polynomial of $A$, deduce that each $\xi_i$ is one of $\sqrt{p}, -\sqrt{p}, i\sqrt{p}$, and $-i\sqrt{p}$ and that if $a, b, c$ and $d$ are the respective multiplicities, then

$$a+b = \frac{p+1}{2} \quad \text{while} \quad c+d = \frac{p-1}{2}. \tag{71}$$

(iv) Moreover,

$$\tau(\chi) = \sum \xi_i = ((a-b)+(c-d)i)\sqrt{p}.$$

From $\tau^2 = \left(\frac{-1}{p}\right)p$, deduce that $a-b = \pm 1, c = d$ if $p \equiv 1 \pmod 4$, and $a = b, c-d = \pm 1$ if $p \equiv 3 \pmod 4$.

(v) It remains to show that $a-b = 1$ in the former case and that $c-d = 1$ in the latter case. For this we evaluate $\det A$ in two different ways. First, show that $\det(A^2) = (-1)^{p(p-1)/2}p^p$; hence $\det(A) = \pm i^{p(p-1)/2}p^{p/2}$. To determine which choice of sign holds here, use the fact that $A$ is a Vandermonde matrix:

$$\begin{aligned}\det A = \prod_{0\le l<k\le p-1} (\zeta^k - \zeta^l) &= \prod_{0\le l<k\le p-1} e^{\pi i(k+l)/p}\left(e^{\pi i(k-l)/p} - e^{\pi i(l-k)/p}\right) \\ &= e^{\frac{\pi i}{p}\sum_{0\le l<k\le p-1}(k+l)} \prod_{0\le l<k\le p-1}\left(2i\sin\frac{\pi(k-l)}{p}\right).\end{aligned}$$

Verify that $2p \mid \sum_{0\le l<k\le p-1}(k+l)$ and conclude that $\det A$ is a positive real multiple of $i^{p(p-1)/2}$. Hence $\det A = i^{p(p-1)/2}p^{p/2}$.

(vi) On the other hand, we have $\det A = \prod \xi_i = i^{2b+c-d}p^{p/2}$. Conclude that

$$2b+c-d \equiv \frac{p(p-1)}{2} \pmod 4.$$

Using (71), prove that $a-b \equiv 1 \pmod 4$ if $p \equiv 1 \pmod 4$ and that $c-d \equiv 1 \pmod 4$ if $p \equiv 3 \pmod 4$. Hence $a-b = 1$ in the former case and $c-d = 1$ in the latter, completing the proof that the plus sign holds in (70) with the choice $\zeta = e^{2\pi i/p}$.

(vii) Show that if $\tau$ is defined instead with respect to the choice $\zeta = e^{2\pi i a/p}$, then the sign we must take in (70) is $\left(\frac{a}{p}\right)$.

*Remark.* In a May 1801 diary entry [45, Entry 118] Gauss conjectures more generally the precise value of the sums $\sum_{a \pmod n} e^{2\pi i a^2/n}$ for $n$ not necessarily prime. He worked "for 4 years and more with every effort" before proving these conjectures on August 30, 1805 [45, Entry 123]. In a September 3 letter to Olbers from the same year [37], he writes

Table 6. Primes $p = 3\cdot 2^n + 1$ with $n \le 750000$ which divide some Fermat number $F_m$.

| $n$ | Fermat number $F_m$ | Discoverer | Discovered |
|---:|---:|---:|---:|
| 41 | $F_{38}$ | R.M. Robinson | 1956 |
| 209 | $F_{207}$ | R.M. Robinson | 1956 |
| 157169 | $F_{157167}$ | J. Young | 1995 |
| 213321 | $F_{213319}$ | J. Young | 1996 |
| 303093 | $F_{303088}$ | J. Young | 1998 |
| 382449 | $F_{382447}$ | J.B. Cosgrave & Y. Gallot | 1999 |

> Finally a few days ago I succeeded – but not by my own efforts, rather, I may say, entirely by the grace of God. As lightning strikes was the riddle solved . . .

Versions of Gauss's original argument can be found in [5, §1.3] and [86, Lecture 11]. For other proofs (all of which work in the case $n = p$ and most of which work more generally) see [51, §6.4], [5, §1.4] and [64, Kapitel 6].

## 11. Cubic Exercises

**Exercise 22.** Give a necessary and sufficient condition in terms of $L$ and $M$ for 6 to be a cubic residue modulo $p$.

**Exercise 23** (Golomb [41])**.** Suppose $p = 3 \cdot 2^n + 1$ is prime. Then $p$ divides the $j$th Fermat number $F_j = 2^{2^j} + 1$ for some $j$ if and only if the order of 3 $\pmod p$ is not divisible by 3. Moreover, in this case there is exactly one such $j$, and $j < n$.

Now prove that if $p = 3 \cdot 2^{2m} + 1$ is prime, then the order of 2 modulo $p$ is divisible by 3, and hence no such primes can divide Fermat numbers. (*Hint:* relate this criterion to the cubic residuacity of 2, and then apply Theorem.)

Table 11 lists all primes of this form with $n \le 750000$ which divide a Fermat number.

**Exercise 24** (Kraïtchik, Pellet)**.** Prove that if $q = 2n + 1$ and $p = 12n + 7$ are prime, and if $p = L'^2 + 27M'^2$ for integers $L'$ and $M'$, then $q \mid 2^p - 1$.

Similarly, prove that if $q = 12n + 5$ and $p = 72n + 31$ are prime, and $p = L'^2 + 27M'^2$ for integers $L'$ and $M'$, then $q \mid 2^p - 1$.

*Example:* Let $n = 18$; then $q = 37$, $p = 223 = 14^2 + 27 \cdot 1^2$, and $2^{37} - 1 = 223 \cdot 616318177$.

For other results of this kind see the papers of Storchi [96] and Golubev [42].

**Exercise 25.** Prove the following four criteria of R. Fueter [31]:

(i) If $p = 1 + 2^{2n} \cdot 3^{2m+3}$ is prime (with $n > 0$ and $m \ge 0$), then 5 is a primitive root modulo $p$ if and only if $n \equiv m \pmod 2$.

(ii) With the same assumptions as above, 7 is a primitive root modulo $p$ if and only if $2n + m \equiv 1 \pmod 3$.

(iii) Suppose that $q$ and $p = 1 + 3 \cdot 4q$ are prime. Write $p = n^2 + 3m^2$ with integers $n$ and $m$. Then 2 is a primitive root modulo $p$ if and only if 3 does not divide $m$.

TABLE 7. The odd primes $q < 50$ for which $p = 6q + 1$ is also prime together with $L$ and $M$ satisfying $L^2 + 27M^2 = 4p$, along with indications of when 3, 5 and 7 generate $(\mathbf{Z}/p\mathbf{Z})^*$. See Exercise 25(iv).

| $q$ | $p$ | $L$ | $M$ | 3 generates? | 5 generates? | 7 generates? |
|---|---|---|---|---|---|---|
| 3 | 19 | 7 | 1 | ✓ | | |
| 5 | 31 | 4 | 2 | ✓ | | |
| 7 | 43 | 8 | 2 | ✓ | ✓ | |
| 11 | 67 | 5 | 3 | | | ✓ |
| 13 | 79 | 17 | 1 | ✓ | | ✓ |
| 17 | 103 | 13 | 3 | | ✓ | |
| 23 | 139 | 23 | 1 | ✓ | | |
| 37 | 223 | 28 | 2 | ✓ | ✓ | |
| 47 | 283 | 32 | 2 | ✓ | ✓ | |

(iv) Suppose that $q$ and $p = 1 + 2 \cdot 3q$ are both odd primes, and write $4p = L^2 + 27M^2$. Then 3 is a primitive root modulo $p$ if and only if 3 does not divide $m$. Also,

$$5 \text{ is a primitive root mod } p \iff L \equiv \pm M \not\equiv 0 \pmod 5,$$
$$7 \text{ is a primitive root mod } p \neq 43 \iff L \equiv \pm 3M \not\equiv 0 \pmod 7.$$

Some examples are provided in Figure 7.

**Exercise 26.** Use Kummer's Criterion to rederive that 2 is a cube mod $p$ if and only if $2 \mid L$ and $2 \mid M$, and that 3 is a cube mod $p$ if and only if $3 \mid M$. Note that these results are weaker than Theorems 4.6 and 4.7. *Hint:* Before tackling the problem of when 3 is a cube, reexpress the final coefficient of the period equation in a form more amenable to computations modulo 3.

**Exercise 27.** Prove Theorem 4.12. Use the Jacobi's Law in its original form and the binomial theorem.

**Exercise 28.** Prove E. Lehmer's Theorem 4.13. Show first that we can assume that $q$ is greater than 3 and coprime to $LM$. Then proceed as follows:

(i) Suppose $q$ is a cubic residue of $p$ and that $L \equiv \mu M \pmod p$. Then $p \equiv \lambda L^2 \pmod q$, where $\lambda := (\mu^2 + 27)/(4\mu^2)$.

(ii) Prove that if the reduced period equation has a root mod $q$, then the polynomial $y^3 - 3\lambda y - \lambda$ also has a root over $\mathbf{F}_q$. (*Hint:* substitute $x = Ly$ in the reduced period polynomial.) Deduce that $\lambda = u^3/(3u + 1)$ for some $u$ in $\mathbf{F}_q$. Prove that $u \not\equiv 0, 1, -\frac{1}{2}, -\frac{1}{3} \pmod q$.

(iii) Verify the congruence

$$\mu^2 \equiv \frac{27}{4\lambda - 1} \equiv \left(\frac{9}{2u+1}\right)^2 \frac{3u-1}{3u+3} \pmod q,$$

and deduce that $\frac{3u-1}{3u+3}$ is a nonzero square in $\mathbf{F}_q^*$. This proves the necessity portion of Theorem 4.13.

(iv) Reversing the steps, prove that the conditions of Theorem 4.13 are also sufficient.

**Exercise 29** (Lehmer [69])**.** Let $p$ and $q$ be distinct primes both greater than 3 with $p \equiv 1 \pmod 3$. Write $4p = L^2 + 27M^2$. Suppose that $p \equiv \lambda L^2 \pmod q$ for a prime $\lambda$ which can be written in the form $4\lambda = 1 + 27m^2$ with $q$ not dividing $m$. Then $q$ is a cubic residue of $p$ if and only if $q$ is a cubic residue of $\lambda$.

*Example (with $\lambda = 7, m = 1$):* if $p \equiv \lambda 7L^2 \pmod q$ (equivalently, if $L^2 \equiv M^2 \pmod q$), then $q$ is a cubic residue modulo $p$ if and only if $q \equiv \pm 1 \pmod 7$.

**Exercise 30** (Lehmer [70], Williams [103])**.** Let $p \equiv 1 \pmod 3$ be prime, and choose a representation $4p = L^2 + 27M^2$ with $L \equiv 1 \pmod 3$. Show that

$$1, \quad \frac{L+9M}{L-9M}, \quad \text{and} \quad \frac{L-9M}{L+9M}$$

are the three cube roots of unity in $(\mathbf{Z}/p\mathbf{Z})^*$ and deduce from Euler's criterion that if $D$ is a noncube modulo $p$ then $D^{(p-1)/3} \equiv (L \pm 9M)/(L \mp 9M) \pmod p$ for an appropriate choice of sign.

(i) Let $g$ be a generator of $(\mathbf{Z}/p\mathbf{Z})^*$, and let $(i, j)$ denote the cubic cyclotomic numbers defined with respect to $g$. Prove that

$$\begin{aligned}(0,1) - (0,2) = M \iff & \frac{L}{2} - \frac{3M}{2}\sqrt{-3} \equiv 0 \pmod p \\ \iff & g^{(p-1)/3} \equiv \frac{L+9M}{L-9M} \pmod p;\end{aligned}$$

here the square root of $-3$ modulo $p$ is defined by $\sqrt{-3} := g^{2(p-1)/3} - g^{(p-1)/3}$. (*Hint:* examine equation (33).)

(ii) Suppose that 2 is a cubic nonresidue. Using Theorem 4.6, prove that $2^{(p-1)/3} \equiv \frac{L+9M}{L-9M} \pmod p$ if and only if $M \equiv L \pmod 4$.

(iii) Suppose that 3 is a cubic nonresidue. Using Theorem 4.7, prove that $3^{(p-1)/3} \equiv \frac{L+9M}{L-9M} \pmod p$ if and only if $M \equiv -1 \pmod 3$.

Williams's paper [103] describes how to determine the ambiguous sign for every prime $D$ (see also [98, Theorem 2.1]).

**Exercise 31** (Gauss)**.** Let $p \equiv 1 \pmod 3$ be prime. Using Gauss's determination of the cyclotomic numbers, prove that there are exactly $p - 2 + L$ pairs $(x, y) \in \mathbf{F}_p^2$ with $x^3 + y^3 = 1$.

**Exercise 32** (continuation; S. Chowla, M. Cowles and J. Cowles [11])**.** Let $M_c$ denote the number of ordered triples of $x, y$ and $z$ in $\mathbf{F}_p$ for which $x^3 + y^3 + cz^3 = 0$. Clearly $M_c$ (for $c \neq 0$) depends only on the coset of $c$ with respect to the subgroup of cubes.

(i) Deduce from the preceding exercise that $M_1 = p^2 + L(p-1)$.

(ii) Now suppose $c$ is a noncube modulo $p$. Let $g$ be a generator of $(\mathbf{Z}/p\mathbf{Z})^*$ which lies in the same coset of cubes as $c$. Furthermore, let $4p = L^2 + 27M^2$ with $L \equiv 1 \pmod 3$ and the sign of $M$ chosen so that any of the three equivalent conditions of Exercise 30(i) are satisfied; then

$$M_c = p^2 + \frac{1}{2}(p-1)(9M - L).$$

(iii) If 2 is a noncube then the above formula holds for $M_2$ if the sign of $M$ is chosen in such a way that $M \equiv L \pmod 4$, and it holds for $M_4$ if the sign of $M$ is determined so that $M \equiv L + 2 \pmod 4$. Similarly, if 3 is a noncube, then the above formula holds for $M_3$ if $M \equiv 2 \pmod 3$ and for $M_9$ if $M \equiv 1 \pmod 3$.

(iv) Show that if $p > 7$ is prime, then every element of $\mathbf{Z}/p\mathbf{Z}$ is a sum of two cubes.

*Remark* (on part (iv)). In the paper of Leep & Shapiro [67] it is shown that if $G$ is a multiplicative subgroup of index 3 in an arbitrary field $F$, then $G + G = F$ except when $\#F = 4, 7, 13$, or 16; see also [4].

**Exercise 33** (Z.-H. Sun, personal communication)**.** One may prove rational cubic reciprocity (in the form of Theorem 4.16) directly from Kummer's criterion (Theorem 3.11) and the determination of the cubic period polynomial (Theorem 4.5), without recourse to Cardano's formula.

Fill in the details in the following demonstration, due to Z.-H. Sun. All notation is as in the statement of Theorem 4.16.

(i) Using Corollary 3.12, prove that if $q \mid LM$ then $q$ is a cube modulo $p$. Since $[0, 1]$ and $[1, 0]$ are cubes in $G(q)$, Theorem 4.16 holds in this case, and we may assume $q \nmid LM$.

(ii) Under this hypothesis, show that

$$[L, 3M] \text{ is a cube in } G(q) \Longleftrightarrow L(3s^2 - 3) = 3M(s^3 - 9s) \quad \text{for some } s \in \mathbf{F}_q.$$

(iii) Making the substitution $s = \frac{2x}{M} + \frac{L}{3M}$, show that this last possibility holds if and only if $x^3 - 3px - pL$ has a root modulo $q$. Finish the proof by another appeal to Corollary 3.12.

## 12. Quartic Exercises

**Exercise 34.** Deduce Theorem 5.9 from Corollary 5.12.

**Exercise 35** (Lehmer [71])**.** The Fibonacci and Lucas sequences are defined by the initial conditions $F_0 = 0, F_1 = 1$ and $L_0 = 0, L_1 = 2$ and the requirement that each term be the sum of the two preceding:

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Fibonacci | 0 | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | 89 | 144 | 233 | 377 |
| Lucas | 2 | 1 | 3 | 4 | 7 | 11 | 18 | 29 | 47 | 76 | 123 | 199 | 322 | 521 | 84 |

They can also be defined by the explicit formulas

$$F_n = \frac{\phi^n - \phi'^n}{\phi - \phi'} \qquad \text{and} \qquad L_n = \phi^n + \phi'^n,$$

where $\phi := (1 + \sqrt{5})/2$ is the ubiquitous golden ratio and $\phi' := (1 - \sqrt{5})/2$ is its algebraic conjugate. In this exercise and the next we study the prime divisors of the $F_n$ and $L_n$. Let $\sqrt{5}$ denote a fixed square root of 5 inside the algebraic closure of $\mathbf{F}_p$.

(i) Show that

$$5 \mid F_n \Leftrightarrow 5 \mid n \text{ and } \quad 2 \mid F_n \Leftrightarrow 3 \mid n.$$

Prove that if $p$ divides a single $F_n$ then $p$ divides infinitely many $F_n$.

(ii) If $p \neq 2, 5$, show that

$$p \mid F_{p - \left(\frac{5}{p}\right)}, \qquad \text{and that } p \mid F_{\frac{1}{2}(p - \left(\frac{5}{p}\right))} \Longleftrightarrow p \equiv 1 \pmod 4.$$

(iii) We now characterize when $p \mid F_{\frac{1}{4}(p-(\frac{5}{p}))}$. Prove that if this occurs then $p \mid F_{\frac{1}{2}(p-(\frac{5}{p}))}$ and hence $p \equiv 1 \pmod 4$. Thus $\left(\frac{5}{p}\right) = 1$ (since $4 \mid p - \left(\frac{5}{p}\right)$). Hence $p \equiv 1, 9 \pmod{20}$.

(iv) Using the Schönemann-Scholz-Lehmer law together with the observation that $\phi = \epsilon_5$ is the fundamental unit of $\mathbf{Q}(\sqrt{5})$, prove that

$$p \mid F_{\frac{1}{4}(p-(\frac{5}{p}))} \Longleftrightarrow \left(\frac{5}{p}\right)_4 \left(\frac{p}{5}\right)_4 = \left(\frac{2}{p}\right).$$

**Exercise 36.** In contrast to what we just witnessed with the Fibonacci sequence, it is not the case that all primes divide a Lucas number. The following partial characterization is due to Redei [87]:

(i) Prove that no $L_n$ is divisible by 5, and that 2 divides $L_n$ if and only if 3 divides $n$. Moreover, prove that if a prime $p$ divides a single value of $L_n$ then $p$ divides infinitely many $L_n$.

(ii) Prove that $L_n^2 - 5 \cdot F_n^2 = 4(-1)^n$, and deduce that no prime $p \equiv 13, 17 \pmod{20}$ can divide a Lucas number $L_n$.

(iii) Prove the "duplication formula" $L_{2n} = L_n^2 - 2(-1)^n$. Use this to show that if $p \equiv 3 \pmod 4$ then $p \mid L_{(p-(\frac{5}{p}))/2}$.

(iv) It remains to determine the status of the primes $p \equiv 1, 9 \pmod{20}$. (Note that $\left(\frac{5}{p}\right) = 1$ for these $p$.) Write $p = 1 + 2^e r$, where $r$ is odd. Show that $p$ divides some Lucas number if and only if

$$\left(\frac{1+\sqrt{5}}{1-\sqrt{5}}\right)^r \neq 1 \Longleftrightarrow \frac{1+\sqrt{5}}{1-\sqrt{5}} \text{ is not a } 2^e\text{th power residue in } \mathbf{F}_p.$$

Using the Schönemann-Scholz-Lehmer law, prove that a prime $p \equiv 21, 29 \pmod{40}$ divides a Lucas number if and only if $\left(\frac{5}{p}\right)_4 \left(\frac{p}{5}\right)_4 = 1$. Show that if $p \equiv 1, 9 \pmod{40}$, then $\left(\frac{5}{p}\right)_4 \left(\frac{p}{5}\right)_4 = -1$ is sufficient for $p$ to divide a Lucas number, but not necessary.

We note that Lagarias ([61], [62]) has shown the related result that precisely 2/3 of the primes divide some Lucas number.

**Exercise 37** (Lehmer [71])**.** Suppose that for a certain choice of $\sqrt{5} \pmod p$, the number $\phi = (1+\sqrt{5})/2$ is a quadratic, but not a higher power residue of the prime $p \equiv \pm 1 \pmod{10}$. Prove that if we define $r_0 = 0, r_1 = \phi$ and $r_n = r_{n-1} + r_{n-2}$ for $n = 2, 3, \ldots$, then $r_0, r_1, r_2, \ldots, r_{(p-3)/2}$ is a complete list of quadratic residues modulo $p$.

**Exercise 38** (Lehmer [69])**.** Let $p$ and $q$ be distinct primes with $p \equiv 1 \pmod 4$ and $\left(\frac{q}{p}\right) = 1$. Write $p = a^2 + b^2$ with $b$ even. Suppose that $p \equiv ra^2 \pmod q$, where $r \equiv p \pmod 8$ is a prime such that $r = 1 + \beta^2$ for some $\beta$ not divisible by $q$. Then $\left(\frac{q}{p}\right)_4 = \left(\frac{q}{r}\right)_4$.

*Example ($r = 5$):* if $p \equiv 5 \pmod 8$ and $p \equiv 5a^2 \pmod q$, then $q$ is a quartic residue of $p$ if and only if $q \equiv 1 \pmod 5$.

**Exercise 39** (Z.-H. Sun, private communication)**.** Let $p$ and $q$ be distinct primes both $1 \pmod 4$ and with $\left(\frac{p}{q}\right) = 1$. Write $p = a^2 + b^2$ with $b$ even. Using Lemma

6.2 and Dirichlet's Law (Theorem 5.3), prove that

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = \left(\frac{2}{q}\right)\left(\frac{a+\sqrt{p}}{q}\right),$$

provided $\sqrt{p}$ in $\mathbf{F}_q$ is chosen so that $a+\sqrt{p}$ is nonvanishing. This consequence of Dirichlet's reciprocity law owes its rediscovery in recent years (with a different proof) to E. Lehmer (see [69], [75]).

**Exercise 40** (Gosset [43])**.** Let $p \equiv q \equiv 1 \pmod 4$ be distinct primes and suppose that $\left(\frac{p}{q}\right) = 1$. Prove that

$$\left(\frac{q}{p}\right)_4 = \left(\frac{ad-bc}{ad+bc}\right)^{(q-1)/4}.$$

(Here the large parenthesized expression is a fraction, not a power-residue symbol!)

**Exercise 41.** State and prove a quartic analog of Theorem 4.12 based on Sun's form of Dirichlet's law.

**Exercise 42.** Let $p$ and $q$ be distinct primes both congruent to $1 \pmod 4$. Suppose that $ps^2 = t^2 + qu^2$ for an odd $s$ and coprime positive integers $t$ and $u$, so that $\left(\frac{-q}{p}\right) = 1$ (and hence $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = 1$). Using the method of Dirichlet, prove that

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = \begin{cases} \left(\frac{s}{q}\right) & \text{if } q \equiv 1 \pmod 8, \\ (-1)^u\left(\frac{s}{q}\right) & \text{if } q \equiv 5 \pmod 8. \end{cases}$$

Proceed as follows:

(i) Show that $\left(\frac{p}{q}\right)_4 = \left(\frac{s}{q}\right)\left(\frac{t}{q}\right)$, and deduce by the method of Lemma that

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = (-1)^{(p-1)/4}\left(\frac{s}{q}\right)\left(\frac{t}{pq}\right)\left(\frac{u}{p}\right).$$

(ii) Suppose that $t$ is odd (so that $u$ is even). Imitating the proof of Lemma 5.6, show that $\left(\frac{t\pm sb}{q}\right) = 1$ provided that $q$ does not divide $t \pm sb$ for the sign being considered. Choose $\sqrt{p} \in \mathbf{F}_q$ with $b+\sqrt{p} \neq 0$ (why is this possible?). Now $t = \epsilon s\sqrt{p}$ for some $\epsilon = \pm 1$. Show that

$$\left(\frac{t}{p}\right)\left(\frac{t+\epsilon sb}{q}\right) = \left(\frac{\sqrt{p}}{q}\right)\left(\frac{\sqrt{p}+b}{q}\right) = \left(\frac{q}{p}\right)_4; \quad \text{deduce } \left(\frac{t}{p}\right) = \left(\frac{q}{p}\right)_4.$$

(iii) Again supposing $t$ is odd, prove that $\left(\frac{t}{pq}\right) = 1$, so that $\left(\frac{t}{p}\right) = \left(\frac{t}{q}\right)$. Conclude from the previous two steps that $\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = 1$ in this case.

(iv) Now suppose $t$ is even (so $u$ is odd). Show that $\left(\frac{u}{p}\right) = 1$ and (imitating the proof of ) that

$$\left(\frac{t}{pq}\right) = \left(\frac{2}{pq}\right)^e = (-1)^{e\cdot t^2/4},$$

where $2^e \| t$. Deduce that in this case we have

$$\left(\frac{q}{p}\right)_4\left(\frac{p}{q}\right)_4 = (-1)^{(p-1)/4}(-1)^{e(p-q)/4}\left(\frac{s}{q}\right).$$

(v) Complete the proof!

The case $s = 1$ appears Theorem 2 in a paper of E. Brown [7]; the general case was considered independently and essentially simultaneously by E. Lehmer [74, Theorem 1].

**Exercise 43** (continuation)**.** Prove that if $q = 5, 13$ or $37$, then every prime $p \equiv 1 \pmod 4$ for which $\left(\frac{-q}{p}\right) = 1$ can be written in the form $t^2 + qu^2$.

(i) First establish the theorem of Thue: for every integer $a$, one can find $x, y$ not both zero with $|x| < \sqrt{p}, |y| < \sqrt{p}$ and $x \equiv ay \pmod p$. (Apply the Pigeonhole principle to the set $\{x - ay \mod p : 0 \leq x, y \leq \sqrt{p}\}$).

(ii) Applying this with $a = \sqrt{-q} \bmod p$, prove that there are integers $x, y$ for which $x^2 + qy^2 = Mp$ for an integer $M$ satisfying $0 < M \leq q$.

(iii) Using the congruence $Mp \equiv x^2 \pmod q$, prove that $\left(\frac{M}{q}\right) \neq -1$.

(iv) Now fix $q = 5, 13$, or $37$, and let $M$ be satisfy $0 < M \leq q$ and $\left(\frac{M}{q}\right) \neq -1$. For each such $M$, show that either $Mp$ cannot be represented in the form $x^2 + qy^2$, or show how to construct a representation of $p$ in the same form from a representation of $Mp$. *Example for $q = 37$:* if $7p = x^2 + 37y^2$, then $\left(\frac{-37}{7}\right) = -1$ implies $7 \mid x$ and $7 \mid y$, so that $49 \mid 7p$ and $p = 7$, contradicting $\left(\frac{-37}{p}\right) = 1$.

The method of proof given here is Mordell's [83]; our account is based on [5, Proof of Corollary 8.3.3]. That these are the only $q \equiv 1 \pmod 4$ with this property follows from genus theory as developed in [12, Chapter XIII, §3] and the classification of imaginary quadratic fields with class number 2.

**Exercise 44.** In the course of proving the supplement to the Schönemann-Scholz-Lehmer law (Theorem 7.2) we saw that for primes $p \equiv 1 \pmod 8$, $\left(\frac{1+\sqrt{2}}{p}\right) = \left(\frac{-4}{p}\right)_8$. Here we establish a number of necessary and sufficient conditions, due to Barrucand & Cohn [3], for $-4$ to be an eighth power residue modulo such a prime. Our proofs follow Williams [105].

(i) Show that $p$ can be written in each of the forms $a^2 + 16b^2$, $c^2 + 8d^2$, and $e^2 - 32f^2$. (*Hint for the last case:* first show that $p$ can be written in the form $x^2 - 8y^2$; if now $x$ and $y$ are both odd, then use the identity $x^2 - 8y^2 = (3x + 8y)^2 - 8(x + 3y)^2$.)

(ii) Suppose that $a$ above is chosen so that $a \equiv 1 \pmod 4$. Use the relation

$$\left(\frac{-4}{p}\right)_8 = \left(\frac{-1}{p}\right)_8 \left(\frac{2}{p}\right)_4 = (-1)^{(p-1)/8+b} \tag{72}$$

to prove that $-4$ is an 8th power residue $\Leftrightarrow (a - 1)/4 + b \equiv 0 \pmod 2$.

(iii) Let $\sqrt{2}$ denote an arbitrary square root of 2 inside $\mathbf{F}_p$; then $\left(\frac{\sqrt{2}}{p}\right) = \left(\frac{2}{p}\right)_4$. Observe that $(c + 2\sqrt{2}d)^2 = 4cd\sqrt{2}$, and prove that

$$\left(\frac{c}{p}\right) = \left(\frac{p}{|c|}\right) = (-1)^{(c^2-1)/8} = (-1)^{(p-1)/8-d} \quad \text{while} \quad \left(\frac{d}{p}\right) = 1.$$

Deduce that

$$\left(\frac{2}{p}\right)_4 = (-1)^{(c^2-1)/8} = (-1)^{(p-1)/8-d},$$

so that by the first equality in (72), $-4$ is an 8th power residue $\Leftrightarrow (-1)^d = 1$.

(iv) Let $\sqrt{-2}$ denote an arbitrary square root of $-2$ inside $\mathbf{F}_p$; then $\left(\frac{\sqrt{-2}}{p}\right) = \left(\frac{-2}{p}\right)_4$. Observe that $(e+4f\sqrt{-2})^2 = 8ef\sqrt{-2}$ and prove that

$$\left(\frac{e}{p}\right) = \left(\frac{-2}{|e|}\right) = (-1)^{(|e|-1)/2+(|e|^2-1)/8} \quad \text{while} \quad \left(\frac{f}{p}\right) = 1.$$

Deduce that

$$\left(\frac{-2}{p}\right)_4 = \left(\frac{8}{p}\right)\left(\frac{-2}{|e|}\right) = \left(\frac{-2}{|e|}\right) \quad \text{and} \quad \left(\frac{-4}{p}\right)_8 = \left(\frac{-2}{p}\right)_4\left(\frac{-1}{p}\right)_8.$$

Use these equations to prove that $-4$ is an 8th power residue modulo $p$ $\Leftrightarrow (-1)^{(|e|-1)/2} = 1$.

**Exercise 45** (continuation, Kaplansky [55])**.** Combining Theorem 5.1 with part (ii) of the preceding exercise, prove that a prime $p \equiv 9 \pmod{16}$ is represented by exactly one of $x^2+32y^2$ and $x^2+64y^2$. If $p \equiv 1 \pmod{16}$, prove that $p$ is represented either by both of these forms or by neither.

**Exercise 46** (Dirichlet [18, §2])**.** In the notation of Exercise 44, Gauss's two criteria for 2 to be a fourth power modulo a prime $p \equiv 1 \pmod 8$ are (i) $\left(\frac{2}{c}\right) = 1$ and (ii) $2 \mid b$. Fill in the details in the following proof that (i) and (ii) are equivalent:

(i) We have $c^2 - 16b^2 = a^2 - 8d^2$. Setting $D := \gcd(a,d)$, we see $D$ is odd and

$$(c-4b)(c+4b) = D^2(a'^2 - 8d'^2), \qquad \text{where } a = Da', d = Dd'.$$

Hence there exist integers $A, B, C$ and $D$ with

$$c + 4b = AB, \quad c - 4b = CD$$

and satisfying

$$AC = D^2 \quad \text{and} \quad BD = a'^2 - 8d'^2;$$

moreover, we can assume $A, B$ and $C$ are positive.

(ii) We have $\gcd(A,C) = 1$. Thus $A$ and $C$ are individually (odd) perfect squares.

(iii) Since $B$ divides $a'^2 - 8d'^2$ with $(a',d') = 1$, the congruence $B \equiv \pm 1 \pmod 8$ holds. Since $A \equiv 1 \pmod 8$, we have also $c + 4b \equiv \pm 1 \pmod 8$. Thus

$$2 \mid b \Longleftrightarrow c \equiv \pm 1 \pmod 8 \Longleftrightarrow \left(\frac{2}{c}\right) = 1.$$

The next two exercises show how the universal rational quartic reciprocity law (Theorem 8.1) can be used to prove general versions of both Burde's law and the Schönemann-Scholz-Lehmer law:

**Exercise 47** (Lemmermeyer [77], Kaplan [54])**.** Let $m = \prod p_i$ and $n = \prod q_j$ be coprime products of distinct primes, with each $p_i$ and $q_j$ congruent to 1 (mod 4). Assume that $\left(\frac{m}{q_j}\right) = 1$ for all $i, j$.

(i) Write $m = a^2 + b^2$ and $n = c^2 + d^2$ with $b$ and $d$ even. Define

$$A := mn, \quad B := b(c^2 - d^2) + 2acd, \quad C := a(c^2 - d^2) - 2bcd.$$

Check that $B^2 + C^2 = mn^2$, and thus $A^2 = m(B^2 + C^2)$. Use the first of these equations to prove that if $A, B$ and $C$ are not pairwise coprime, then $q \mid BC$ for some $q \mid n$.

(ii) Prove that for each $q \mid n$, we have

$$B \equiv 2d(ac-bd) \pmod{q}, \quad C \equiv -2d(ad+bc) \pmod{q}$$

and use this to prove that $BC$ is coprime to $n$. Hence $A, B$ and $C$ are coprime in pairs.

(iii) Now apply the general rational quartic reciprocity law to deduce that

$$\left(\frac{B\sqrt{m}}{q}\right) = \left(\frac{A+B\sqrt{m}}{q}\right) = \left(\frac{q}{m}\right)_4, \quad \text{hence } \left(\frac{q}{m}\right)_4 \left(\frac{m}{q}\right)_4 = \left(\frac{B}{q}\right).$$

Prove that $\left(\frac{2d}{q}\right) = 1$, so that $\left(\frac{q}{m}\right)_4\left(\frac{m}{q}\right)_4 = \left(\frac{ac-bd}{q}\right)$; multiplying over those $q$ dividing $n$, deduce the general Burde law:

$$\left(\frac{n}{m}\right)_4 \left(\frac{m}{n}\right)_4 = \left(\frac{ad-bc}{n}\right).$$

**Exercise 48.** Let $m = p_1 \ldots p_r$ be a product of distinct primes $p_i \equiv 1 \pmod 4$, and suppose that the fundamental unit $\epsilon_m$ of $\mathbf{Q}(\sqrt{m})$ has norm $-1$. Let $p \equiv 1 \pmod 4$ be a prime with $\left(\frac{p}{p_j}\right) = 1$ for all $j = 1, 2, \ldots, r$.

(i) Prove that

$$\left(\frac{\epsilon_m}{p}\right) = \left(\frac{m}{p}\right)_4 \left(\frac{p}{m}\right)_4, \quad \text{hence } \left(\frac{\epsilon_m}{n}\right) = \left(\frac{m}{n}\right)_4 \left(\frac{n}{m}\right)_4 \tag{73}$$

if $n$ is a product of (not necessarily distinct) primes $p$ with these properties. (*Hint:* Apply the general reciprocity law with $C = 1$ and $A, B$ determined by $A + B\sqrt{m} = \epsilon_m^3\sqrt{m}$.)

(ii) Using the second equality in (73), show that if $m$ and $n$ are as above, then

$$\left(\frac{\epsilon_m}{n}\right) = \left(\frac{\epsilon_1}{n}\right)\left(\frac{\epsilon_2}{n}\right)\cdots\left(\frac{\epsilon_r}{n}\right).$$

The result in (ii) is due to Furuta [32].

The next three exercises describe Lemmermeyer's proof ([76], [77]) of the universal rational quartic law. The outlined proof of Exercise 49 is taken from [78, Proof of Lemma 5.14]. These exercises assume familiarity with the classification of abelian extensions of $\mathbf{Q}$ in terms of Dirichlet characters; see. e.g., [78, §4.5] or [102].

**Exercise 49** (A Lemma from Galois Theory)**.** Let $k/\mathbf{Q}$ and $K/k$ be quadratic extensions, and write $K = k(\sqrt{\mu})$. Let $\sigma$ denote the nontrivial automorphism of $k/\mathbf{Q}$. We also write $\mu^{1+\sigma} := \mu\cdot\sigma\mu$ and we work always with a fixed value of $\sqrt{\sigma(\mu)}$.

(i) Prove that

$$K/\mathbf{Q} \text{ is normal} \iff \sigma \text{ extends to an automorphism of } K/\mathbf{Q}$$
$$\iff \sqrt{\sigma(\mu)} \text{ exists in } K \iff \sqrt{\sigma(\mu)} = \beta\sqrt{\mu} \text{ for some } \beta \in k \iff \mu^{1+\sigma} \in k^2.$$

(ii) Suppose that $\mu^{1+\sigma}$ is in $k^2$, and let $\hat{\sigma}$ denote an extension of $\sigma$ to an automorphism of $K/\mathbf{Q}$. Show that

$$\mathrm{Gal}(K/\mathbf{Q}) \cong \mathbf{Z}/2 \oplus \mathbf{Z}/2 \Leftrightarrow \hat{\sigma} \text{ has order } 2 \Leftrightarrow \hat{\sigma} \text{ fixes } \sqrt{\mu^{1+\sigma}} \Leftrightarrow \mu^{1+\sigma} \in \mathbf{Q}^2,$$

and that $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathbf{Z}/4$ otherwise.

**Exercise 50** (Proof of the Universal Rational Quartic Reciprocity Law)**.** Assume the hypotheses of Theorem 8.1. Let $k = \mathbf{Q}(\sqrt{m})$ and $K = k(\sqrt{A + B\sqrt{m}})$. Use the preceding exercise to prove that $K/\mathbf{Q}$ is a cyclic quartic extension. Then show that $K$ is actually a subfield of $\mathbf{Q}(\zeta_m)$ as follows:

(i) Show that the conductor of $k$ is equal to $m$, hence the conductor of $K$ is a multiple of $m$.

(ii) Using the Kummer-Dedekind theorem [85, Theorem 4.3.3] or the theory of prime splitting in Kummer extensions of prime degree ([78, Theorem 4.12], [50, §39]), prove that the only odd primes that can ramify in $K/\mathbf{Q}$ are primes $p$ dividing $A^2 - mB^2 = mC^2$. Observing that

$$2(A + B\sqrt{m})(A + C\sqrt{m}) = (A + B\sqrt{m} + C\sqrt{m})^2,$$

so that we may also write $K = k(\sqrt{2(A + C\sqrt{m})})$,

show that $K/\mathbf{Q}$ is unramified for all odd primes $p$ not dividing $A^2 - mC^2 = mB^2$. Conclude that $p$ is unramified if $p \nmid 2m$.

(iii) Prove that $A + B\sqrt{m} \equiv 1 \pmod 4$ in the ring of integers of $k$, and use this to show that $K/\mathbf{Q}$ is unramified at 2. Thus $K$ is ramified only at primes dividing $m$, and so only these primes can divide the conductor of $K$.

(iv) Show that we can choose a cyclic quartic extension $L/\mathbf{Q}$ contained in $\mathbf{Q}(\zeta_m)$. If $KL$ is cyclic, prove that $K = L$ and hence that $K$ has conductor dividing $m$.

(v) We may therefore suppose that $KL$ is not cyclic. Prove that $KL$ has a quadratic subfield $k'$ distinct from $k = \mathbf{Q}(\sqrt{m})$, and that the conductor of $KL$ is the least common multiple of the conductors of $L$ and $k'$. Show that no $p \nmid m$ ramifies in $k'$, and deduce that the conductor of $k'$ divides $m$. Therefore the conductor of $KL$ divides $m$.

(vi) Complete the proof by showing that the conductor of $KL$ is the same as the conductor of $K$.

**Exercise 51** (continued)**.** Let $X$ be the group of Dirichlet characters corresponding to our quartic extension $K/\mathbf{Q}$. By Exercise 50, $X$ is a subgroup of the group of characters corresponding to $\mathbf{Q}(\zeta_m)/\mathbf{Q}$, which is just the group of characters of conductor dividing $m$.

(i) Show that $X$ is generated by a character $\chi$ of order 4 and conductor $m$.

(ii) Since $K$ contains $k = \mathbf{Q}(\sqrt{m})$, the group $X$ must contain the character group corresponding to $k$. Show that this latter group is generated by the element $\chi_1\chi_2\dots\chi_r$, where $\chi_i$ is the quadratic character modulo $p_i$.

(iii) Let $\psi_i$ (for $i = 1, 2, \dots, r$) denote a fixed quartic character modulo $p_i$. Show that $\chi^2 = \chi_1 \dots \chi_r$ and deduce that $\chi = \psi_1 \dots \psi_r \psi'$, where $\psi'$ is a quadratic character of conductor dividing $m$.

(iv) Let $q$ be a prime for which $\left(\frac{q}{p_i}\right) = 1$ for all $i$. Prove that

$$\chi(q) = \psi_1(q) \dots \psi_r(q)\psi'(q) = \left(\frac{q}{p_1}\right)_4 \cdots \left(\frac{q}{p_r}\right)_4 = \left(\frac{q}{m}\right)_4$$

and deduce that $q$ splits in $K$ if and only if $\left(\frac{q}{m}\right)_4 = 1$.

(v) Using either of the theorems mentioned in Exercise 50 (ii), prove that an odd prime $q$ for which $\left(\frac{q}{p_i}\right) = 1$ for all $i = 1, 2, \ldots, r$ splits if and only if

$$\left(\frac{A + B\sqrt{m}}{\mathfrak{q}}\right) = 1 \text{ for some prime } \mathfrak{q} \mid q \Longleftrightarrow$$
$$\left(\frac{A + B\sqrt{m}}{q}\right) = 1 \text{ when } \sqrt{m} \in \mathbf{F}_q \text{ is chosen so that } A + B\sqrt{m} \neq 0 \text{ in } \mathbf{F}_q.$$

## 13. Notes

In March of 1940, during a four-month imprisonment stemming from “a disagreement with the French authorities on the subject of [his] military ‘obligations,”’ Weil [56] penned the following words to his sister:

> . . . one can say that *everything* that has been done in arithmetic since Gauss up to recent years consists in variations on the law of reciprocity; beginning with Gauss’s law; and ending with and crowning the work of Kummer, Dedekind, Hilbert is Artin’s law, *it is all the same law.* This is beautiful, but a bit vexing. We know a little more than Gauss, without doubt; but what we know more (or a bit more) is just that we do not know more.

Though an example of unbridled hyperbole (cf. [65], where S. Lang “urge[s] people to get a more accurate view of number theory up to 1940 elsewhere”), it is doubtless true that the quest for higher reciprocity laws played a significant (and perhaps dominating) role in the early development of algebraic number theory.

However, it would be farcical for this author to pretend to a level of expertise sufficient to describe these later developments. Those wishing to get a feel for the Artin reciprocity law spoken of so glowingly by Weil are encouraged to peruse the accounts of Wyman [110], Lenstra & Stevenhagen [80], and Cox [15, Chapter 2], all of which were written with the neophyte in mind.

The rational reciprocity laws considered here can be considered the evolutionary ancestors of the usual cubic and biquadratic reciprocity laws. These latter received rather short shrift in the introduction; rather than go into detail here, we refer to the excellent book of Ireland & Rosen [51], which contains a full discussion of both. For the history of all these laws one should consult the extensive notes in Lemmermeyer’s book as well as the articles of Collision [13] (who recounts the basic history of the cubic and biquadratic reciprocity laws), Rowe [91] (whose charming article focusing on the biquadratic reciprocity law sparkles with personal details about Gauss and Dirichlet) and Frei [30] (who surveys the history of reciprocity laws up to the discovery of Eisenstein’s $l$th power law).

For the remainder of this section we content ourselves with drawing attention to some relatives of the rational reciprocity laws we have discussed. For further references and results, one should consult Lehmer’s excellent expository article [75], as well as the accounts of rational residuacity given in Chapters 5-7 of Lemmermeyer’s book [78] and Chapters 7 & 8 of the book of Berndt, Evans & Williams [5].

None too far removed in the family tree from the theorems discussed in this chapter are the rational octic reciprocity laws. To describe these we need the rational octic residue symbol. This is defined (in complete analogy with the corresponding quartic symbol) for $a$ a nonzero fourth power modulo $p$ according to the rule

$$\left(\frac{a}{p}\right)_8 = \begin{cases} 1 & \text{if } a \text{ is an eighth power mod } p, \\ -1 & \text{otherwise.} \end{cases}$$

With this definition in place, we can state the following octic analogs of Burde's law and the Schönemann-Scholz-Lehmer law:

**Theorem 13.1** (Burde's Octic Reciprocity Law)**.** *Let $p \equiv q \equiv 1 \pmod 8$ be prime. Write*

$$p = a_1^2 + b_1^2 = a_2^2 + 2b_2^2 = a_3^2 - 2b_3^2, \quad q = c_1^2 + d_1^2 = c_2^2 + 2d_2^2 = c_3^2 + 2d_3^2$$

*with $a_1$ and $c_1$ odd. Suppose that $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$. Then*

$$\begin{aligned}\left(\frac{p}{q}\right)_8 \left(\frac{q}{p}\right)_8 &= \left(\frac{a_1 d_1 - b_1 c_1}{q}\right)_4 \left(\frac{a_2 d_2 - b_2 c_2}{q}\right) && \text{(Williams [106], Wu [109])} \\ &= \left(\frac{a_1 d_1 - b_1 c_1}{q}\right)_4 \left(\frac{a_3 d_3 - b_3 c_3}{q}\right) && \text{(Kwon [60])}\end{aligned}$$

**Theorem 13.2** (Schönemann-Scholz-Lehmer Octic Law (Buell & Williams [8], [9]))**.** *Let $p \equiv q \equiv 1 \pmod 8$ be prime, and suppose $\left(\frac{q}{p}\right)_4 = \left(\frac{p}{q}\right)_4 = 1$. Then*

$$\left(\frac{p}{q}\right)_8 \left(\frac{q}{p}\right)_8 = \begin{cases} \left(\frac{\epsilon_p}{q}\right)_4 \left(\frac{\epsilon_q}{p}\right)_4 & \textit{if } N(\epsilon_{pq}) = 1, \\ (-1)^{h(pq)/4} \left(\frac{\epsilon_p}{q}\right)_4 \left(\frac{\epsilon_q}{p}\right)_4 & \textit{if } N(\epsilon_{pq}) = -1. \end{cases}$$

(These laws are discussed in detail in [78, §§9.1, 9.5].) Leonard & Williams [81] later proved a sixteenth-power analog of Burde's law, and a general $2^n$-th power analog was given by Evans [29].

What about the cubic law's side of the family? Here we might ask for criteria on $q$ necessary and sufficient for it to be a 5th power mod $p$, a 7th power, or in general an $e$th power (for prime values of $e$). The method we used to prove Jacobi's reciprocity law carries over to some extent. Here we take the case $e = 5$, which has been treated in some detail in the literature. Then we have the following result of Dickson [17, Theorem 8] in analogy with Lemma 1.1:

**Theorem 13.3.** *Let $p \equiv 1 \pmod 5$. Then there are exactly four integer solutions $(x, u, v, w)$ to the simultaneous equations*

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2, \quad 4xw = v^2 - u^2 - 4uv.$$

*for which $x \equiv 1 \pmod 5$. If $(x, u, v, w)$ is one solution, then the other solutions are $(x, -u, -v, w)$, $(x, v, -u, -w)$ and $(x, -v, u, -w)$.*

In [68], [72] Lehmer expressed the coefficients and discriminant of the quintic period polynomial as polynomials in $x, u, v$ and $w$. Thus one can compute, for any fixed $q$, precise congruence conditions on $x, u, v$ and $w$ corresponding to the period equation possessing a root mod $q$ (or having its discriminant divisible by $q$). In this way, using Kummer's criterion together with extensive computer work, Williams [104] was able to give explicit necessary and sufficient conditions for $q$ to be a fifth power mod $p \equiv 1 \pmod 5$ for every prime $q \leq 17$. As the simplest result in this theory, we have for example that 2 is a quintic residue modulo $p$ if and only if $x, u, v$ and $w$ are all even. A general theorem of Muskat [84, Theorem 3] implies that for $q$ to be a quintic residue it is sufficient (but not necessary!) that $q$ divides $u$ and $v$; see also [111] for related results.

Another answer for general prime $e$ was given by Ankeny [2]:

**Theorem 13.4.** *Fix a prime $e$, and let $p$ be a prime with $p \equiv 1 \pmod{e}$. Let $q$ be a prime distinct from $p$ and $e$, and let $\chi\colon \mathbf{F}_p^* \to \overline{\mathbf{F}}_q^*$ be a multiplicative character of order $e$ taking values in a fixed algebraic closure $\overline{\mathbf{F}}_q$ of $\mathbf{F}_q$. Let $\zeta_e$ and $\zeta_p$ denote primitive $e$th and $p$th roots of unity in $\overline{\mathbf{F}}_q$. If $\tau(\chi)$ denotes the Gauss sum*

$$\tau(\chi) := \sum_{n=1}^{p-1} \chi(n)\zeta_p^n \in \overline{\mathbf{F}}_q,$$

*then $\tau(\chi)^e \in \mathbf{F}_q(\zeta_e)$, and $q$ is an $e$th power residue of $p$ if and only if $\tau(\chi)^e$ is an $e$th power in $\mathbf{F}_q(\zeta_e)$.*

It is interesting to contrast this with Kummer's criterion: In the notation of the preceding theorem, the degree $e$ period polynomial having a root in $\mathbf{F}_q$ amounts to the assertion that

$$\tau(\chi) + \tau(\chi^2) + \cdots + \tau(\chi^{e-1}) = \sum_{\chi \text{ of order } e} \tau(\chi)$$

belongs to $\mathbf{F}_q$.

As an example of Theorem 13.4, when $e = 2$ the character $\chi$ is the Legendre symbol (but $\overline{\mathbf{F}}_q$-valued) and $\tau(\chi)^2 = p^*$; this can be obtained from our calculation of the reduced quadratic period polynomial in §3.5. Hence $q$ is a square modulo $p$ if and only if $p^*$ is a square modulo $q$ (the quadratic reciprocity law). When $e = 3$, it can be shown (e.g., cf. [51, §8.3]) that

$$\tau(\chi)^3 = p\pi \in \mathbf{F}_q(\zeta_3) = \mathbf{F}_q(\sqrt{-3}),$$

where $\pi = \frac{L+3M\sqrt{-3}}{2}$ for integers $L, M$ satisfying $L^2 + 27M^2 = 4p$ and $L \equiv 1 \pmod{3}$. In the proofs of §4.3 we have already seen that $p\pi$ being a cube is equivalent to Jacobi's reciprocity law. See Exercises 19 and 20 for a sketch of the proof of Theorem 13.4 and more details concerning these examples.

The above result may still be thought unsatisfactory, being neither explicit enough nor "rational" enough. This defect can be remedied, at the cost of introducing considerable complication. In the same paper as above, Ankeny gives the following explicit conditions corresponding to the case when $q$ also is supposed to be $1 \pmod{e}$:

**Theorem 13.5.** *Fix an odd prime $e$. Let $p$ and $q$ be distinct primes with $p \equiv q \equiv 1 \pmod{e}$. Then there are precisely $e-1$ distinct integral solutions to the Diophantine* *system*

$$e\sum_{j=1}^{e-1} X_j^2 - \left(\sum_{j=1}^{e-1} X_j\right)^2 = (e-1)p^{e-2}, \tag{i}$$

$$\sum\nolimits_1^{(1)} X_{j_1}X_{j_2} = \sum\nolimits_i^{(1)} X_{j_1}X_{j_2}, \qquad 2 \le i \le \frac{e-1}{2}, \tag{ii}$$

$$1 + \sum_{j=1}^{e-1} X_j \equiv \sum_{j=1}^{e-1} jX_j \equiv 0 \pmod{e}, \tag{iii}$$

(iv) *not all the* $X_i \equiv 0 \pmod{p}$*, and*

$$\sum\nolimits_i^{(k)} X_{j_1}\dots X_{j_k} - \sum\nolimits_0^{(k)} X_{j_1}\dots X_{j_{k+1}} \equiv 0 \pmod{p^{e-k-1}}$$

*for* $2 \le k \le e-2, 1 \le i \le e-1$.

*Here* $\sum_i^{(k)}$ *denotes a sum over all* $j_1, \dots, j_{k+1} = 1, 2, \dots, e-1$ *such that* $j_1 + \dots + j_k - kj_{k+1} \equiv i \pmod{e}$*. If* $a_1, \dots, a_{e-1}$ *is any such solution, then*

$$e \text{ is an } e\text{th power mod } p \Longleftrightarrow \sum_{j=1}^{e-1} ja_j + \frac{1}{2}ea_{e-1} \equiv 0 \pmod{e^2}. \tag{A}$$

*Also if* $\zeta$ *denotes a primitive eth root of unity modulo q, then*

$$q \text{ is an } e\text{th power mod } p \Longleftrightarrow p\sum_{j=1}^{e-1} a_j\zeta^j \text{ is an } e\text{th power mod } q. \tag{B}$$

Actually (B) is simply a translation of Theorem 13.4 into rational terms in the special case when $q \equiv 1 \pmod{e}$ (so that $\mathbf{F}_q(\zeta_e) = \mathbf{F}_q$); the system of equations is rigged so that $p\sum a_j\zeta^j = \tau(\chi)^e$ for some $\chi$ of order $e$.

## References

1. W. Aitken and F. Lemmermeyer, *Simple counterexamples to the local-global principle*, draft; see `http://www.fen.bilkent.edu.tr/~franz/publ.html`.
2. N. C. Ankeny, *Criterion for rth power residuacity*, Pacific J. Math. **10** (1960), 1115–1124. MR MR0118708 (22 #9479)
3. Pierre Barrucand and Harvey Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity*, J. Reine Angew. Math. **238** (1969), 67–70. MR MR0249396 (40 #2641)
4. Vitaly Bergelson and Daniel B. Shapiro, *Multiplicative subgroups of finite index in a ring*, Proc. Amer. Math. Soc. **116** (1992), no. 4, 885–896. MR 93b:16001
5. Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication. MR MR1625181 (99d:11092)
6. A. I. Borevich and I. R. Shafarevich, *Number theory*, Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20, Academic Press, New York, 1966. MR MR0195803 (33 #4001)
7. Ezra Brown, *A theorem on biquadratic reciprocity*, Proc. Amer. Math. Soc. **30** (1971), 220–222. MR MR0280462 (43 #6182)
8. Duncan A. Buell and Kenneth S. Williams, *Is there an octic reciprocity law of Scholz type?*, Amer. Math. Monthly **85** (1978), 483–484.
9. ———, *An octic reciprocity law of Scholz type*, Proc. Amer. Math. Soc. **77** (1979), no. 3, 315–318. MR MR545588 (81a:10006)
10. Klaus Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. **235** (1969), 175–184. MR MR0241354 (39 #2694)

11. S. Chowla, M. Cowles, and J. Cowles, *On the difference of cubes* $(\mathrm{mod}\, p)$, Acta Arith. **37** (1980), 61–65. MR MR598864 (82c:10002)
12. Harvey Cohn, *Advanced number theory*, Dover Publications Inc., New York, 1980, Reprint of *A second course in number theory*, 1962, Dover Books on Advanced Mathematics. MR 82b:12001
13. Mary Joan Collison, *The origins of the cubic and biquadratic reciprocity laws*, Arch. History Exact Sci. **17** (1977), no. 1, 63–69. MR MR0441648 (56 #52)
14. Richard Courant and Herbert Robbins, *What Is Mathematics?*, Oxford University Press, New York, 1941. MR MR0005358 (3,144b)
15. David A. Cox, *Primes of the form* $x^2 + ny^2$, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989, Fermat, class field theory and complex multiplication. MR MR1028322 (90m:11016)
16. A. Cunningham and Th. Gosset, *4-tic* & *3-bic residuacity-tables*, Messenger Math. **50** (1920), 1–30.
17. Leonard Eugene Dickson, *Cyclotomy, higher congruences, and Waring's problem. I.*, Amer. J. Math. **57** (1935), 391–424.
18. P. G. L. Dirichlet, *Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré*, J. Reine Angew. Math. **3** (1828), 35–69.
19. ———, *Démonstration d'une propriété analogue à la loi de réciprocité qui existe entre deux nombres premiers quelconques*, J. Reine Angew. Math. **9** (1832), 379–389.
20. ———, *Über den ersten der von Gauss gegebenen Beweise des Reciprocitätsgesetzes in der Theorie der quadratischen Reste*, J. Reine Angew. Math. **47** (1854), 139–150.
21. ———, *Über den biquadratischen Charakter der Zahl „Zwei"*, J. Reine Angew. Math. **57** (1860), 187–188.
22. ———, *Lectures on number theory*, History of Mathematics, vol. 16, American Mathematical Society, Providence, RI, 1999, Supplements by R. Dedekind, Translated from the 1863 German original and with an introduction by John Stillwell. MR MR1710911 (2000e:01045)
23. G. Waldo Dunnington, *Carl Friedrich Gauss: titan of science. A study of his life and work*, Mathematical Association of America, New York, 2004.
24. G. Eisenstein, *Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen*, J. Reine Angew. Math. **27** (1844), 289–310.
25. ———, *Lois de réciprocité*, J. Reine Angew. Math. **28** (1844), 53–67.
26. Euclid, *The thirteen books of Euclid's Elements translated from the text of Heiberg. Vol. I: Introduction and Books I, II. Vol. II: Books III–IX. Vol. III: Books X–XIII and Appendix*, Dover Publications Inc., New York, 1956, Translated with introduction and commentary by Thomas L. Heath, 2nd ed. MR MR0075873 (17,814b)
27. L. Euler, *Tractatus de numerorum doctrina capita sedecim quae supersunt*, Comment. Arithm. **2** (1849), 503–575.
28. ———, *Commentationes Arithmeticae. (Opera Omnia. Series Prima: Opera Mathematica, Volumen Quintum.)*, Societas Scientiarum Naturalium Helveticae, Geneva, 1944, Volumen Quartum edidit Rudolph Fueter. MR MR0016335 (8,2m)
29. Ronald J. Evans, *Rational reciprocity laws*, Acta Arith. **39** (1981), no. 3, 281–294. MR MR640916 (83h:10006)
30. Günther Frei, *The reciprocity law from Euler to Eisenstein*, The intersection of history and mathematics, Sci. Networks Hist. Stud., vol. 15, Birkhäuser, Basel, 1994, pp. 67–90. MR MR1308080 (95k:01016)
31. Rud Fueter, *Über primitive Wurzeln von Primzahlen*, Comment. Math. Helv. **18** (1946), 217–223. MR MR0016403 (8,11e)
32. Yoshiomi Furuta, *Norm of units ofquadratic fields*, J. Math. Soc. Japan **11** (1959), 139–145. MR MR0112870 (22 #3716)
33. Carl Friedrich Gauss, *Theoria residuorum biquadraticorum, Commentatio Prima*, Comment. Soc. regiae sci. Göttingen **6** (1828).
34. ———, *Theoria residuorum biquadraticorum, Commentatio Secunda*, Comment. Soc. regiae sci. Göttingen **7** (1832), 93–148.
35. ———, *Die Lehre von den Resten. II. Allgemeine Untersuchungen über die Congruenzen*, Untersuchungen über höhere Arithmetik, Deutsch herausgegeben von H. Maser, Chelsea Publishing Co., New York, 1965, pp. 602–629. MR MR0188045 (32 #5488)

36. ———, *Letter to Dirichlet (May 30, 1828)*, (Dirichlet's) Mathematische Werke. Bände I, II, Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften von L. Kronecker, Chelsea Publishing Co., Bronx, N.Y., 1969, pp. 378–380. MR MR0249268 (40 #2514)
37. ———, *Letter to Olbers (September 3, 1805)*, Werke. Band X, Abt. I, Georg Olms Verlag, Hildesheim, 1973, Reprint of the 1906 original, pp. 24–25.
38. ———, *Notizen über cubische und biquadratische Reste*, Werke. Band VII, Georg Olms Verlag, Hildesheim, 1973, Reprint of the 1906 original, pp. 5–14.
39. ———, *Theoria residuorum biquadraticorum. comm. i*, Werke. Band II, Georg Olms Verlag, Hildesheim, 1973, Reprint of the 1906 original, pp. 165–168. MR MR616135 (82e:01122g)
40. ———, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986, Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse. MR MR837656 (87f:01105)
41. Solomon W. Golomb, *Properties of the sequences* $3\cdot 2^n+1$, Math. Comp. **30** (1976), no. 135, 657–663. MR MR0404129 (53 #7933)
42. V. A. Golubev, *Nombres de Mersenne et caractères du nombre* 2, Mathesis **67** (1958), 257–262. MR MR0101215 (21 #28)
43. Th. Gosset, *On the law of quartic reciprocity*, Messenger Math. **41** (1911), 65–90.
44. K. Grandjot, *Über die Irreduzibilität der Kreisteilungsgleichung*, Math. Zeitschrift **19** (1923), 128–129.
45. J. J. Gray, *A commentary on Gauss's mathematical diary, 1796–1814, with an English translation*, Exposition. Math. **2** (1984), no. 2, 97–130. MR MR783128 (86i:01032)
46. Detlef Gröger, *On Gauss's entry from January 6, 1809*, Amer. Math. Monthly **113** (2006), no. 5, 455–458. MR MR2225479
47. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979. MR 81i:10002
48. G.H. Hardy, *An introduction to the theory of numbers*, American Mathematical Society. Bulletin. **35** (1929), 778–818.
49. D. R. Heath-Brown and S. J. Patterson, *The distribution of Kummer sums at prime arguments*, J. Reine Angew. Math. **310** (1979), 111–130. MR MR546667 (81e:10033)
50. Erich Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Mathematics, vol. 77, Springer-Verlag, New York, 1981, Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen. MR MR638719 (83m:12001)
51. Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR 92e:11001
52. C.G.J. Jacobi, *De residuis cubicis commentatio numerosa*, J. Reine Angew. Math. **2** (1827), 66–69.
53. ———, *Letter to Gauss (February 8, 1827)*, Gesammelte Werke, Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften. Zweite Ausgabe, vol. VII, Chelsea Publishing Co., New York, 1969, pp. 393–400.
54. Pierre Kaplan, *Sur le* 2*-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. **283/284** (1976), 313–363. MR MR0404206 (53 #8009)
55. Irving Kaplansky, *The forms* $x+32y^2$ *and* $x+64y^2$, Proc. Amer. Math. Soc. **131** (2003), no. 7, 2299–2300 (electronic). MR MR1963780 (2003m:11058)
56. Martin H. Krieger, *A 1940 letter of André Weil on analogy in mathematics*, Notices Amer. Math. Soc. **52** (2005), no. 3, 334–341, Excerpted from *Doing mathematics* [World Scientific Publishing Co., Inc., River Edge, NJ, 2003; MR1961400]. MR MR2125268
57. E.E. Kummer, *De residuis cubicis disquisitiones nonnullae analyticae*, J. Reine Angew. Math. **32** (1846), 341–359.
58. ———, *Über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung entstehen*, J. Reine Angew. Math. **30** (1846), 107–116.
59. ———, *Allgemeine Reciprocitätsgesetze für beliebig hohe Potenzreste*, Collected papers, Springer-Verlag, Berlin, 1975, Volume I: Contributions to number theory, Edited and with an introduction by André Weil, pp. 345–362.
60. Soonhak Kwon, *A remark on rational octic reciprocity*, Proc. Japan Acad. Ser. A Math. Sci. **78** (2002), no. 2, 22–25. MR MR1887109 (2002j:11001)

61. J. C. Lagarias, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math. **118** (1985), no. 2, 449–461. MR MR789184 (86i:11007)

62. ———, *Errata to: "The set of primes dividing the Lucas numbers has density* 2/3*" [Pacific J. Math.* **118** *(1985), no. 2, 449–461; MR0789184 (86i:11007)]*, Pacific J. Math. **162** (1994), no. 2, 393–396. MR MR1251907 (94m:11015)

63. E. Landau, *Über die Irreduzibilität der Kreisteilungsgleichung*, Math. Zeitschrift **29** (1928), 462.

64. ———, *Elementare Zahlentheorie*, Chelsea Publishing Company, New York, New York, 1950.

65. Serge Lang, *On the AMS Notices publication of Krieger's translation of Weil's 1940 letter*, Notices Amer. Math. Soc. **52** (2005), no. 6, 612–622.

66. V. A. Lebesgue, *Note sur les congruences*, C.R. Acad. Sci. Paris **51** (1860), 9–13.

67. David B. Leep and Daniel B. Shapiro, *Multiplicative subgroups of index three in a field*, Proc. Amer. Math. Soc. **105** (1989), no. 4, 802–807. MR 89m:11127

68. Emma Lehmer, *The quintic character of* 2 *and* 3, Duke Math. J. **18** (1951), 11–18. MR MR0040338 (12,677a)

69. ———, *Criteria for cubic and quartic residuacity*, Mathematika **5** (1958), 20–29. MR MR0095162 (20 #1668)

70. ———, *On Euler's criterion*, J. Austral. Math. Soc. **1** (1959/1961), no. part 1, 64–70. MR MR0108475 (21 #7191)

71. ———, *On the quadratic character of the Fibonacci root*, Fibonacci Quart **4** (1966), 135–138. MR MR0238796 (39 #160)

72. ———, *On the divisors of the discriminant of the period equation*, Amer. J. Math. **90** (1968), 375–379. MR MR0227133 (37 #2718)

73. ———, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math. **250** (1971), 42–48. MR MR0286777 (44 #3986)

74. ———, *On some special quartic reciprocity laws*, Acta Arith. **21** (1972), 367–377. MR MR0302603 (46 #1747)

75. ———, *Rational reciprocity laws*, Amer. Math. Monthly **85** (1978), no. 6, 467–472. MR MR0498352 (58 #16482)

76. Franz Lemmermeyer, *Rational quartic reciprocity*, Acta Arith. **67** (1994), no. 4, 387–390. MR MR1301826 (95m:11010)

77. ———, *Rational quartic reciprocity. II*, Acta Arith. **80** (1997), no. 3, 273–276. MR MR1451413 (98f:11004)

78. ———, *Reciprocity laws*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000, From Euler to Eisenstein. MR MR1761696 (2001i:11009)

79. ———, *Quadratic reciprocity in number fields*, draft for *Reciprocity Laws II*; see `http://www.fen.bilkent.edu.tr/~franz/rec2.html`, February 2005.

80. H. W. Lenstra, Jr. and P. Stevenhagen, *Artin reciprocity and Mersenne primes*, Nieuw Arch. Wiskd. (5) **1** (2000), no. 1, 44–54. MR MR1760775 (2001h:11006)

81. Philip A. Leonard and Kenneth S. Williams, *A rational sixteenth power reciprocity law*, Acta Arith. **33** (1977), no. 4, 365–377. MR MR0460224 (57 #219)

82. Florian Luca, *Pascal's triangle and constructible polygons*, Util. Math. **58** (2000), 209–214. MR MR1801314 (2001i:05013)

83. L. J. Mordell, *Solvability of the equation* $ax^2 + by^2 = p$, J. London Math. Soc. **41** (1966), 517–522. MR MR0197404 (33 #5569)

84. Joseph B. Muskat, *Reciprocity and Jacobi sums*, Pacific J. Math. **20** (1967), 275–280. MR MR0210657 (35 #1543)

85. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004. MR MR2078267 (2005c:11131)

86. Hans Rademacher, *Lectures on elementary number theory*, A Blaisdell Book in the Pure and Applied Sciences, Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London, 1964. MR MR0170844 (30 #1079)

87. L. Rédei, *Die Primfaktoren der Zahlenfolge 1, 3, 4, 7, 11, 18,* $\cdots$, Portugaliae Math. **8** (1949), 59–61. MR MR0035784 (12,11c)

88. Hans Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), 12–18. MR MR0009381 (5,141c)

89. H.W. Richmond, *A construction for a polygon of seventeen sides*, Quart. J. Math. **XXVI** (1893), 206–207.
90. ______, *To construct a regular polygon of* 17 *sides*, Math. Ann. **67** (1909), 459–461.
91. David E. Rowe, *Gauss, Dirichlet, and the law of biquadratic reciprocity*, Math. Intelligencer **10** (1988), no. 2, 13–25. MR MR932158 (89e:01031)
92. D. Savitt, *The mathematics of Gauss*, Unpublished manuscript (work in progress), 2005.
93. A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - du^2 = -4$, Math. Zeitschrift **39** (1934), 95–111.
94. Theodor Schönemann, *Theorie der symmetrischen Functionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congruenzen nebst einigen Anwendungen derselben*, J. Reine Angew. Math. **19** (1839), 289–308.
95. Gert Schubring, *Dirichlet. Comment on: "Gauss, Dirichlet, and the law of biquadratic reciprocity" [Math. Intelligencer* **10** *(1988), no. 2, 13–25; MR0932158 (89e:01031)] by D. E. Rowe*, Math. Intelligencer **12** (1990), no. 1, 5–6. MR MR1034866 (90j:01024)
96. Edoardo Storchi, *Alcuni criteri di divisibilità per i numeri di Mersenne e il carattere* $6^{\text{co}}$*,* $12^{\text{mo}}$*,* $24^{\text{mo}}$*,* $48^{\text{mo}}$*, dell'interno* 2, Boll. Un. Mat. Ital. (3) **10** (1955), 363–375. MR MR0071445 (17,127h)
97. Zhi-Hong Sun, *Notes on quartic residue symbols and rational reciprocity laws*, Nanjing Daxue Xuebao Shuxue Bannian Kan **9** (1992), no. 1, 92–101. MR MR1198437 (94b:11007)
98. ______, *On the theory of cubic residues and nonresidues*, Acta Arith. **84** (1998), no. 4, 291–335. MR MR1618089 (99c:11005)
99. ______, *Supplements to the theory of quartic residues*, Acta Arith. **97** (2001), no. 4, 361–377. MR MR1823552 (2002c:11007)
100. B. A. Venkov, *Elementary number theory*, Translated from the Russian and edited by Helen Alderson, Wolters-Noordhoff Publishing, Groningen, 1970. MR MR0265267 (42 #178)
101. P.L. Wantzel, *Recherches sur les moyens de reconnaître si un problème de Géometrie se résoudre avec la règle et le compas*, J. Pures Appl. **2** (1837), 366–372.
102. Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR MR1421575 (97h:11130)
103. Kenneth S. Williams, *On Euler's criterion for cubic nonresidues*, Proc. Amer. Math. Soc. **49** (1975), 277–283. MR MR0366792 (51 #3038)
104. ______, *Explicit criteria for quintic residuacity*, Math. Comp. **30** (1976), no. 136, 847–853. MR MR0412089 (54 #218)
105. ______, *Note on a result of Barrucand and Cohn*, J. Reine Angew. Math. **285** (1976), 218–220. MR MR0417122 (54 #5182)
106. ______, *A rational octic reciprocity law*, Pacific J. Math. **63** (1976), no. 2, 563–570. MR MR0414467 (54 #2568)
107. ______, *On Scholz's reciprocity law*, Proc. Amer. Math. Soc. **64** (1977), no. 1, 45–46. MR MR0453618 (56 #11880)
108. Kenneth S. Williams, Kenneth Hardy, and Christian Friesen, *On the evaluation of the Legendre symbol* $((A + B\sqrt{m})/p)$, Acta Arith. **45** (1985), no. 3, 255–272. MR MR808025 (87b:11006)
109. P. Wu, *A rational reciprocity law*, Ph.D. thesis, Univ. Southern California, 1975.
110. B. F. Wyman, *What is a reciprocity law?*, Amer. Math. Monthly **79** (1972), 571–586; correction, ibid. **80 (1973), 281**. MR MR0308084 (46 #7199)
111. Yun Cheng Zee, *Some sufficient conditions for quintic residuacity*, Proc. Amer. Math. Soc. **54** (1976), 8–10. MR MR0389731 (52 #10562)