Rational Reciprocity Laws

Emma Lehmer

The American Mathematical Monthly, Vol. 85, No. 6. (Jun. - Jul., 1978), pp. 467-472.

Stable URL:
http://links.jstor.org/sici?sici=0002-9890%28197806%2F07%2985%3A6%3C467%3ARRL%3E2.0.CO%3B2-U

The American Mathematical Monthly is currently published by Mathematical Association of America.

8. H. W. Gould, An identity involving Stirling numbers, Ann. Inst. Statist. Math., Tokyo, 17(1965) 265–269.

9. ———, Note on recurrence relations for Stirling numbers, Publ. Inst. Math. Belgrade, N. S., 6(20)(1966) 115–119.

10. ———, Noch einmal die Stirlingschen Zahlen, Jber. Deutsch. Math.-Verein., 73(1971) 149–152.

11. ———, Explicit formulas for Bernoulli numbers, this MONTHLY, 79(1972) 44–51.

12. ———, Research Bibliography of Two Special Number Sequences, Published by the author, Morgantown, WV, June, 1976.

13. J. A. Grunert, Über die Summirung der Reihen von der Form $A\phi(0), A_1\phi(1)x, A_2\phi(2)x^2, \ldots, A_n\phi(n)x^n, \ldots,$ wo A eine beliebige constante Grösse, A_n eine beliebige und $\phi(n)$ eine ganze rationale algebraische Function der positiven ganzen Zahl n bezeichnet, J. Reine Angew. Math., 25(1843) 240–279.

14. H. Harborth, Über Primteiler von Stirlingschen Zahlen zweiter Art, Elem. Math., 29(1974) 129–131.

15. C. Jordan, On Stirling's numbers, Tôhoku Math. J., 37(1933) 254–278.

16. E. H. Lieb, Concavity properties and a generating function for Stirling numbers, J. Combinatorial Theory, 5(1968) 203–206.

17. N. S. Mendelsohn, Those Stirling numbers again, Canad. Math. Bull., 4(1961) 149–151.

18. V. V. Menon, On the maximum of Stirling numbers of the second kind, J. Combinatorial Theory, A, 15(1973) 11–24.

19. D. S. Mitrinović and R. S. Mitrinović, Sur les nombres de Stirling et les nombres de Bernoulli d'ordre supérieur, Publ. Elektrotehn. Fakulteta, Belgrade, No. 43, 1960, 63pp.

20. L. Moser and M. Wyman, Asymptotic development of the Stirling numbers of the first kind, J. London Math. Soc., 33(1958) 133–146.

21. ———, Stirling numbers of the second kind, Duke Math. J., 25(1958) 29–44.

22. Ivan Paasche, Drei Noten über Stirlingszahlen, Univ. Beograd. Publ. Elektrotehn. Fak., No. 331 (1970) 17–21.

23. Russell V. Parker, Stirling and Stirling's numbers, Mathematics Teaching, Bull. Assoc. of Teachers of Math., England, No. 59, Summer, 1971.

24. B. Richter, Über die Stirlingschen Zahlen der zweiten Art, J. Reine Angew. Math., 266(1974) 88–99.

25. L. Toscano, Nota bibliografica sui numeri di Stirling di prima specie, Giorn. Mat. Battaglini, (6)2(92)(1964) 120–122.

26. Horst Wegner, Einige Probleme bei Stirlingschen Zahlen zweiter Art unter besonderer Berücksichtigung asymptotischer Eigenschaften, Doctoral Dissertation, Univ. of Köln, 1970.

27. ———, Über das Maximum bei Stirlingschen Zahlen zweiter Art, J. Reine Angew. Math., 262/263(1973) 134–143.

28. L. Carlitz, Note on the numbers of Jordan and Ward, Duke Math. J., 38 (1971) 783–790.

DEPARTMENT OF MATHEMATICS, WEST VIRGINIA UNIVERSITY, MORGANTOWN, WV 26506.

RATIONAL RECIPROCITY LAWS

EMMA LEHMER

Abstract. It is well known that the famous Legendre law of quadratic reciprocity, of which over 150 proofs are in print, has been generalized over the years to algebraic fields by a number of famous mathematicians from Gauss to Artin to the extent that it has become virtually unrecognizable. On the other hand, it seems to have escaped notice that in the past decade there were developed rational reciprocity laws for higher power residues which are more direct and easily recognizable generalizations of the Legendre law. These recent developments will be the subject of this report.

1. Introduction. Euler appears to have been the first to ask for what primes p is a given number a (prime to p) a quadratic residue of p. He had already obtained what is now known as Euler's criterion which can be written

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \equiv x^2 (\bmod p) \\ -1 & \text{if } a \not\equiv x^2 (\bmod p) \end{cases} \tag{1}$$

Emma Lehmer is a well-known and distinguished number-theorist. *Editors.*

from which it is quite obvious that -1 is a quadratic residue of p if and only if $p=4n+1$. He found that 2 and 3 are quadratic residues of primes p if and only if $p=8n\pm1$ and $12n\pm1$ respectively. He also made the conjecture that if p and q are distinct odd primes then q is a quadratic residue of p if and only if $-p$ is a residue of q.

Legendre extended Euler's criteria for 2 and 3 to be residues and gave for $q<100$ the arithmetical progressions for primes p having q as a quadratic residue, namely:

$$p=4qn\pm r_i,\text{ where } r_i\equiv 1(\text{mod}\,4)\text{ and }(r_i/q)=1. \tag{2}$$

He is also responsible for what is now known as the Legendre symbol used in (1), in terms of which he wrote down the reciprocity law which now bears his name:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{(p-1)(q-1)/4}. \tag{3}$$

Neither Euler nor Legendre succeeded in giving a proof of either (2) or (3). A good account of the early history and a proof of the equivalence of (2) and (3) will be found in the recent book by W. J. LeVeque [17]. While the elegance of (3) speaks for itself, (2) shows that the character of a fixed prime q to an arbitrary prime p depends on the infinite class of primes to which p belongs.

Gauss rediscovered the reciprocity law before his eighteenth birthday and was "tormented" by it for a whole year before he produced the first of his seven proofs. About a hundred years later Bachmann collected 50 proofs, and 15 years ago Gerstenhaber [8] published "The 152nd Proof of the Law of Quadratic Reciprocity" in this MONTHLY. In all likelihood there are another dozen proofs in existence by now.

Gauss was the first to consider extending the quadratic reciprocity law to higher power residues. If we let $p=kn+1$, then (1) becomes

$$a^{(p-1)/k}=\left(\frac{a}{p}\right)_k\equiv\zeta^{\text{ind}\,a}(\text{mod}\,p), \tag{4}$$

where ζ is a primitive kth root of unity and where the index of a is taken with respect to some primitive root g of p.

For $k=4$ we have $p=4n+1=a^2+b^2=(a+ib)(a-ib)=p_1p_2$. This led Gauss to the study of what is now known as the Gaussian primes $p_1=a+ib$ and to the discovery of a quartic reciprocity law for these complex primes. This law was proved by Eisenstein who wrote it in the elegant form which parallels (3), namely

$$\left(\frac{p_1}{q_1}\right)_4\left(\frac{q_1}{p_1}\right)_4=(-1)^{(p_1-1)(q_1-1)/16}. \tag{5}$$

This statement should be supplemented by the fact that -1 is a quartic residue of p if and only if $p=8n+1$ and that 2 is a quartic residue of p if and only if $p=a^2+64b_1^2$. Gauss was not only aware of this, but gave conditions for all primes $q\leqslant 19$ to be quartic residues of p in terms of the permissible ratios of a/b modulo q.

Kummer considered the problem for prime k and developed the theory of cyclotomic fields in order to prove a reciprocity law in such fields. Hilbert reinterpreted the reciprocity law in terms of the norm residue symbol and generalized it to arbitrary algebraic number fields. In his ninth problem, Hilbert asks for "the most general law of reciprocity in an arbitrary algebraic number field." In his 1969 account of Hilbert's ninth problem Faddeev [7] credits Šafarevič with the solution of the problem in 1949. On the other hand, in the 1976 AMS volume on Hilbert's problems Tate [20] does not even mention Šafarevič, but credits Artin with the solution in 1927, although he goes on to discuss further generalizations. It should be noted that in recent years the reciprocity problem has been restated in terms of the splitting of a general polynomial into factors modulo p. This is a generalization of the obvious fact that the quadratic equation splits into two distinct linear factors if and only if its discriminant is a quadratic residue of p. In an expository paper in this MONTHLY with the fetching title "What is a reciprocity law?" Wyman [26] discusses the reciprocity problem from this point of view and concludes the paper with the following remark:

"Finally I have to confess that I still do not know what a reciprocity law is or what it should be. The reciprocity problem like many other number-theory problems can be stated in a fairly simple and concrete way. However the simply stated problems are often the hardest and a complete solution seems to be very far out of reach. In fact, we probably will not know what we are looking for until we have found it."

It is the purpose of this report to speak for those number-theorists who believe that they know what a reciprocity law is and not only know what they are looking for but have actually been discovering new rational reciprocity laws in the past decade.

2. Rational quartic reciprocity laws. We have already seen that Legendre's reciprocity law can be interpreted in at least three different ways and that none of the generalizations led to a rational reciprocity law. For our purposes we will simply define a reciprocity law as a reciprocal relation between the characters of two odd primes, or more generally between the characters of some function of such primes. To obtain a rational reciprocity law, we must put some conditions on the primes to insure that the product of these characters is ±1.

In the quartic case, $p=q=1 \pmod 4$ and so the assumption that $(p/q)=1$ would insure that $(p/q)_4$ and $(q/p)_4$, and hence their product, are ±1. The problem of determining these signs would give a generalization of either (2) or (3) or both. Some 20 years ago I combed the literature and asked my co-workers whether such a rational law was known to them with negative results.

Because Gauss and others have found binary quadratic forms representing p in terms of q and μ, where $\mu \equiv a/b \pmod q$, it seemed reasonable to try to find a general expression for q to be a residue of p in terms of these forms. This was done in 1958 [9] thus giving a generalization of (2). Unfortunately, the reciprocity law which was equivalent to these criteria did not appear to be rational and was not even stated in [9]. It reads:

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4=\left(\frac{2}{q}\right)\left(\frac{a+\sqrt{p}}{q}\right). \tag{6}$$

It was a decade later that Burde [6] gave a very elegant rational reciprocity law which is as follows:

Let $p=a^2+b^2$ and $q=A^2+B^2$ with $a\equiv A\equiv 1 \pmod 4$ and let $(p/q)=1$, then

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4=(-1)^{(q-1)/4}\left(\frac{aB-bA}{q}\right). \tag{7}$$

Although (6) was not recognized at first as a rational reciprocity law, it is not hard to show that (6) and (7) are equivalent. This fact proved in [11] provides a totally different proof of (7) and shows that the rational quartic reciprocity law is equivalent to the fact that the quartic character $(q/p)_4$ depends on the class of binary quadratic forms of discriminant $-pq$ which represent p and not on p itself.

Another rational form of the quartic reciprocity law for those primes which are represented by the form $p=c^2+qd^2$ was given independently and by entirely different methods by Ezra Brown [3] and myself [11] as follows:

If $p\equiv q\equiv 1 \pmod 4$ are such that $p=c^2+qd^2$, then

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4=\begin{cases}1 & \text{if } q\equiv 1 \pmod 8\\ (-1)^d & \text{if } q\equiv 5 \pmod 8\end{cases}. \tag{8}$$

For $q=5$, 13, and 37 every prime p is represented as $p=c^2+qd^2$ if $(p/q)=1$. Brown [4, 5] also gave similar reciprocity laws for primes represented by other quadratic forms.

Meanwhile, another kind of reciprocity law which is very closely connected with the quartic law has been resurrected and is now known as the Scholz reciprocity law. The history of this law is as follows:

In 1969 Barrucand and Cohn [1] proved that the quadratic unit $\epsilon_2=1+\sqrt{2}$ is a quadratic residue of p if and only if $p=c^2+32d^2$. Jacob Brandler [2] showed that $\epsilon_5=(1+\sqrt{5})/2$ and $\epsilon_{13}=(3+\sqrt{13})/2$ are quadratic residues of $p=c^2+qd^2$ if and only if d is even and that $\epsilon_{17}=4+\sqrt{17}$ is always a quadratic residue of p.

Comparing this with (8) it was not hard to conjecture that

$$\left(\frac{\epsilon_q}{p}\right)=\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 \quad \text{if} \quad \left(\frac{p}{q}\right)=1 \tag{9}$$

from which it would immediately follow from symmetry that

$$\left(\frac{\epsilon_q}{p}\right)=\left(\frac{\epsilon_p}{q}\right). \tag{10}$$

I again combed the literature and asked my friends, but nobody knew whether this elegant result was true or false. Only after I devised a cyclotomic proof of (9) and therefore of (10) in **[10]** did I discover a verbal statement of (10) as part four of a complicated five-part theorem in class field theory in Scholz **[19]**. Since then, a completely elementary proof has been devised by Williams **[25]**.

3. Rational octic and higher reciprocity laws. Results and conjectures about quartic characters of quadratic units will be found in my paper **[12]**. Recently Leonard and Williams **[15, 16]** proved some of these conjectures. They have made a detailed study of the quartic character of these units in these papers, but have not yet proved a quartic analogue of Scholtz' reciprocity law (10). We would expect that such a law would be intimately connected with an octic reciprocity law which was obtained independently by K. S. Williams **[24]** and P. Y. Wu **[27]** as follows:

Let $p=a^2+b^2=c^2+2d^2\equiv 1(\text{mod}\,8)$ and $q=A^2+B^2=C^2+2D^2\equiv 1(\text{mod}\,8)$, $a\equiv c\equiv A\equiv C\equiv 1(\text{mod}\,4)$, with $(p/q)_4=(q/p)_4=1$; then

$$\left(\frac{p}{q}\right)_8\left(\frac{q}{p}\right)_8=\left(\frac{aB-bA}{q}\right)_4\left(\frac{cD-dC}{q}\right). \tag{11}$$

This should be supplemented by the well-known fact that

$$\left(\frac{2}{p}\right)_8=1 \quad \text{if and only if} \quad \begin{cases} p=a^2+256b^2 & \equiv 1(\text{mod}\,16) \\ p=a^2+\;\;64b^2 & \equiv 9(\text{mod}\,16), b \text{ odd.}\end{cases} \tag{12}$$

Similar criteria have been worked out for all primes $q\leqslant 47$ in terms of $p=a^2+b^2=c^2+2d^2\equiv 1(\text{mod}\,8)$ by von Lienen **[19]**, but no explicit conditions were given for a general q to be an octic residue of p in terms of the corresponding sets of binary quadratic forms, although obviously such criteria must exist and be equivalent to (11).

Leonard and Williams now have just published 16th power reciprocity law **[14]** which involves representation of p and q by a quaternary quadratic form, so that the work on kth power reciprocity laws is still in progress.

In this connection we must mention another form of the $2k$th power law which was derived from a recent generalization of the Gauss Lemma **[13]**, which was used by Gauss in his third proof of the quadratic reciprocity law. This generalization states that if λ is a kth power residue of p, and if the product of the first half of the residues of p by λ taken modulo p contains $\mu_p(\lambda)$ residues which exceed $p/2$ then

$$(-1)^{\mu_p(\lambda)}=\left(\frac{\lambda}{p}\right)_{2k}. \tag{13}$$

Applying this lemma with $\lambda=q$, and then with $\lambda=p$ and p replaced by q, we obtain:

$$\left(\frac{p}{q}\right)_{2k}\left(\frac{q}{p}\right)_{2k}=(-1)^{\mu_p(q)+\mu_q(p)}, \qquad \left(\frac{p}{q}\right)_k=\left(\frac{q}{p}\right)_k=1. \tag{14}$$

This reduces to (3) for $k=1$, since $\mu_p(q)+\mu_q(p)\equiv(p-1)(q-1)/4(\text{mod}\,2)$. For $k=2$ and $k=4$ comparison of (14) with (7) and (11) relates the parity of the numbers $\mu_p(q)$ and $\mu_q(p)$ with a,b,c,d in the quadratic partitions of p. No direct proof of this fact has so far been obtained.

4. Rational reciprocity laws for odd powers. Because the character $(a/p)_k$ is never -1, we can no longer expect rational reciprocity laws, but we can still obtain criteria for q to be a kth power residue of p in terms of quadratic forms. This has been done by Jacobi for $k=3$ and $q\leqslant 37$, in terms of the partition of $4p=L^2+27M^2$. General conditions and quadratic forms for p in terms of q and the ratios $\mu\equiv L/M(\text{mod}\,q)$ similar to those obtained for $k=4$ will be found in [9]. Recently K. S. Williams [23] separated the remaining cases of $L/M(\text{mod}\,q)$ to correspond with the two non-residue classes.

For quintic residues the case is complicated by the fact that the criteria depend on the representation

$$16p=x^2+50u^2+50v^2+125w^2 \quad \text{with} \quad 4xw=v^2-u^2-4uv. \tag{15}$$

Recently K. S. Williams extended the known criteria to $q\leqslant 19$ in terms of the ratios of u/w and v/w [21].

He also returned to Euler's criterion and gave rational expressions for $a^{(p-1)/3}$ in terms of L and M in [22] and for $a^{(p-1)/5}$ in terms of the x,u,v,w in [23], and so we have come full circle back to Euler. For arbitrary k there appears to be no better way of finding out whether a given number is a kth power residue of a large prime p than by raising it to the $(p-1)/k$th power $(\text{mod}\,p)$ and asking whether it is one or not, especially with the advent of high-speed computing.

5. Applications. Far from concluding that our more elaborate criteria are of no value, we can turn the tables around and use Euler's criterion to obtain conditions on the variables

$$a,b,c,d \quad \text{in} \quad p=a^2+b^2=c^2+qd^2.$$

These conditions are useful, for example, in proving a number to be a prime by representing it uniquely by one of these quadratic forms.

Another application of the criteria for kth power residuacity is to the divisibility by p of the $(p-1)/k$th term of a second order recurring series [10].

The connection between the criteria for the quadratic unit and the solvability of $u^2-Du^2=-4$ was established in [19].

Beginning with [1], in [3], [11], [15], [16] and others the kth power residuacity of units was connected with the parity of class numbers in various quadratic fields both real and imaginary.

Finally, a relation was recently established between the $2k$th character of λ and the parity of the permutation arising from multiplying the kth power residues by λ [13]. We hope that many other connections will come to light in the future.

Presented to the annual meeting of the Northern Section of the MAA in San Francisco on Feb. 26, 1977.

References

1. P. Barrucand and H. Cohn, Note on primes of the type x^2+32y^2, J. Reine Angew. Math., 238 (1969) 67–70.
2. Jacob Brandler, Residuacity properties of quadratic units, J. Number Theory, 5 (1973) 271–287.
3. Ezra Brown, A theorem on biquadratic reciprocity, Proc. Amer. Math. Soc., 30 (1971) 220–222.
4. ———, Biquadratic reciprocity laws, Proc. Amer. Math. Soc., 37 (1973) 374–376.
5. ———, Quadratic forms and biquadratic reciprocity, J. Reine Angew. Math., 253 (1972) 214–220.
6. Klaus Burde, Ein rationales biquadratisches Reziprozitätsgesetz, J. Reine Angew. Math., 235 (1969) 175–184.
7. D. K. Faddeev, On Hilbert's ninth problem, Hilbert's Problems, Izdat Nauka, Moskow, 1969, 131–140.
8. Murray Gerstenhaber, The 152nd proof of the law of quadratic reciprocity, this MONTHLY, 70 (1963) 397–398.

9. Emma Lehmer, Criteria for cubic and quartic residuacity, Mathematika, 5 (1958) 20–29.

10. ———, On the quadratic character of some quadratic surds, J. Reine Angew. Math., 250 (1971) 42–48.

11. ———, On some special quartic reciprocity laws, Acta Arith., 21 (1972) 367–377.

12. ———, On the quartic character of quadratic units, J. Reine Angew. Math., 268/269 (1974) 294–301.

13. ———, Generalizations of Gauss' Lemma, Number Theory and Algebra, Academic Press, New York, 1977, 187–194.

14. P. A. Leonard and K. S. Williams, A rational sixteenth power reciprocity law, Acta Arith., 33 (1977) 365–377.

15. ———, The quadratic and quartic character of certain quadratic units, Pacific J. Math., 71 (1977) 101–106.

16. ———, ibid. II (submitted for publication).

17. W. J. LeVeque, Number Theory (to appear). Fundamentals of Number Theory, 1977, 103–109.

18. Horst von Lienen, Primzahlen als achte Potenzreste, J. Reine Angew. Math., 266 (1974) 107–117.

19. Arnold Scholz, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, Math. Z., 39 (1934) 95–111.

20. J. Tate, The general reciprocity law, Proc. Amer. Math. Soc., Symposium in Pure Math., 28 (1976) 311–322.

21. K. S. Williams, Explicit criteria for quintic residuacity, Math. Comp., 30 (1974) 1–6.

22. ———, On Euler's criterion for cubic non-residues, Proc. Amer. Math. Soc., (1975) 277–283.

23. ———, On Euler's criterion for quintic non-residues, Pacific J. Math., 61 (1975) 543–550.

24. ———, A rational octic reciprocity law, Pacific J. Math., 63 (1976) 564–570.

25. ———, On Scholz's Reciprocity Law (submitted for publication).

26. B. F. Wyman, What is a reciprocity law? this MONTHLY, 79 (1972) 571–586.

27. Ping-Yuan Wu, A Rational Reciprocity Law, Ph.D. thesis, Univ. Southern Calif., 1975.

1180 MILLER AVENUE, BERKELEY, CA 94708.

CORRECTIONS TO
"The Rational Cuboid Revisited"

(This MONTHLY, 84 (1977) 518-533)

JOHN LEECH

J. Lagrange has pointed out the following correction to my article. At the top of p. 523, for $x_i = 550{,}576$ read $x_i = 520{,}576$. See also his article [17], in which he gives another parametric solution of (3.2) and announces a complete proof of impossibility for the case Spohn [16] left incomplete. Two minor misprints: in the middle of p. 524, for $(x_2x_3)^3$ read $(x_2x_3)^2$; in the middle of p. 530 for $\alpha + b$ read $\alpha + \beta$.

References

17. J. Lagrange, Sur le cuboïde entier, Sémin. Delange–Pisot–Poitou (Groupe d'étude de théorie des nombres) 17e année 1975/76 no. G1, 5p. (1977).

DEPARTMENT OF COMPUTING SCIENCE, UNIVERSITY OF STIRLING, STIRLING, SCOTLAND.

MISCELLANEA

10. The efforts of computer engineers have already produced a mechanized Briggs (who spent his lifetime computing logarithms) and a mechanized Barlow (whose famous Tables were his life's work) but no one has ever conceived of a mechanized Napier (for he *invented* logarithms).

B. V. Bowden, *Faster Than Thought*, London, 1953, p. 321