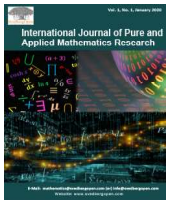
https://doi.org/10.51483/IJPAMR.2.1.2022.15-39 ISSN: 2789-9160

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Pure and Applied Mathematics Research

Publisher's Home Page: https://www.svedbergopen.com/



Research Paper **Open Access**

Quadratic, Cubic, Biquadratic, and Quintic Reciprocity

Darrell Cox[1], Sourangshu Ghosh[2] and Eldar Sultanow[3*]

[1]Department of Mathematics, Grayson County College, United States. E-mail: darrellcox97@gmail.com
[2]Department of Civil Engineering, Indian Institute of Technology Kharagpur, India. E-mail: sourangshug123@gmail.com
[3]Potsdam University, Chair of Business Informatics, Processes and Systems, Potsdam, Germany. E-mail: Eldar.Sultanow@wi.uni-potsdam.de

Article Info

Volume 2, Issue 1, April 2022
Received : 19 February 2022
Accepted : 22 March 2022
Published : 05 April 2022
doi: 10.51483/IJPAMR.2.1.2022.15-39

Abstract

A method for determining which natural numbers satisfy reciprocity is given. The method is applicable to quadratic, cubic, quintic, and in general "prime" reciprocity. The method is also applicable to biquadratic reciprocity. The even powers of a primitive root of a prime are quadratic residues and the odd powers are quadratic nonresidues. This is generalized to cubic residues and nonresidues, etc. Let n denote the "degree" of prime reciprocity (2 for quadratic reciprocity, 3 for cubic reciprocity, 5 for quintic reciprocity, etc.). The residues and nonresidues are determined for the degree $2n$ and applied to the degree of n. For example, the residues and nonresidues for biquadratic reciprocity are used to analyze quadratic reciprocity. For a degree of $2n$, there are 2 groups of residues of the same size and $2n-2$ groups of nonresidues all the same size as each of the two groups of residues. Each of the $2n$ groups is mapped to certain differences modulo p of the sorted least residues of one of the groups of nonresidues. This is a one-to-one transformation since it does not change the elements of a group. When certain counts associated with the differences are not distinct, groups are effectively merged together. The number of distinct difference counts will be referred to as the "degrees of freedom". For quadratic reciprocity, there are either 1 or 2 degrees of freedom. For quintic reciprocity, there are up to 5 degrees of freedom and as few as 2 degrees of freedom. This transformation is useful for identifying properties of the residues and nonresidues. Also, reciprocity is not entirely restricted to primes. Reciprocity is interpreted as being a collection of finite commutative groups.

Keywords: *Quadratic reciprocity law, Supplemental reciprocity laws, Perron's theorem, Gaussian sum*

1. Introduction

Let p be an odd prime. If the congruence $x^2 \equiv n \pmod{p}$ has a solution, we say that n is a quadratic residue mod p and write nRp. If the congruence has no solution we say that n is a quadratic nonresidue mod p and write $n\bar{R}p$. If $n \not\equiv 0 \pmod{p}$ we define Legendre's symbol $(n|p)$ as follows: $(n|p) = +1$ if nRp or -1 if $n\bar{R}p$. If $n = 0 \pmod{p}$ we define $(n|p) = 0$.

The quadratic reciprocity law (first proved by Gauss) states that if p and q are distinct odd primes, then $(p|q) = (q|p)$ unless $p \equiv q \equiv 3 \pmod{4}$, in which case $(p|q) = -(q|p)$.

* *Corresponding author: Eldar Sultanow, Potsdam University, Chair of Business Informatics, Processes and Systems, Potsdam, Germany. E-mail: Eldar.Sultanow@wi.uni-potsdam.de*

A form of rational cubic reciprocity dates back to Jacobi. He reportedly proved the following:

Theorem 1: Let $q > 3$ be a prime. Then there is a set S of $\frac{1}{3}\left(q-\left(\frac{-3}{q}\right)\right)$ elements of $Z/qZ \bigcup \infty$ with the following property. If p is a prime distinct from q with $p \equiv 1 \pmod 3$ and $4p = L^2 + 27M^2$ (and $L, M > 0$), then q is a cube modulo $p \leftrightarrow \frac{L}{3M} \pmod q \in S$.

For example, for $q = 37$, $S = \{0, \pm 1, \pm 3, \pm 4, \pm 10, \pm 15, \infty\}$. There are $(q-1)/3$ classes if $q \equiv 1 \pmod 3$ and $(q+1)/3$ classes otherwise. This can be written in a unified way as $\frac{1}{3}\left(q-\left(\frac{-3}{q}\right)\right)$ since $\left(\frac{-3}{q}\right)$ equals 1 if $q \equiv 1 \pmod 3$ or -1 if $q \equiv -1 \pmod 3$. Also, if $p \equiv 1 \pmod 3$ we can write $4p = L^2 + 27M^2$. In this representation, L and M are unique up to the choice of sign. The Sun (1998) Rational Cubic Reciprocity Law is:

Theorem 2: Let $q > 3$ be a prime. If $p \neq q$ is a prime congruent to 1 (mod 3) where $4p = L^2 + 27M^2$ with positive L and M, then q is a cube modulo $p \leftrightarrow \frac{L}{3M}$ is a cube in G.

G is defined as follows. Take $Z/qZ \bigcup \infty$ and remove any square root of -3 and let $G(q)$ be the resulting set. In general, #G = $q-\left(\frac{-3}{q}\right)$. For x and y residue classes mod q contained in G, we define $x * y = \frac{xy-3}{x+y}$, the computation taking place in Z/qZ. If the denominator but not the numerator vanishes, the result is set to ∞. We also define $x * \infty = \infty * x$ and $\infty * \infty = \infty$. This operation is commutative. An identity element is ∞. The inverse of x is $-x$ and the inverse of ∞ is ∞. Also, * is associative so * makes G into a finite commutative group. The group G has a unique cyclic subgroup of order #G/3 $= \frac{1}{3}\left(q-\left(\frac{-3}{q}\right)\right)$. It is just the subgroup of "cubes" $g * g * g$ with $g \in G$.

Sun's (2001) Rational Quartic Reciprocity Law is similar. Nothing this sophisticated is needed in this paper. When q is a nth power modulo p is determined using primitive roots.

1.1. Primitive Roots

An integer g is called a primitive root of a prime q if q does not divide g and $g^d \not\equiv 1 \pmod q$ for any natural number d less than $q - 1$. Primitive roots exist for prime powers. Theorem 10.6 of Apostol's (1976) book is:

Theorem 3: Let p be an odd prime. Then we have:

a) If g is a primitive root mod p then g is also a primitive root mod p^α for all $\alpha \geq 1$ if, and only if, $g^{p-1} \not\equiv 1 \pmod{p^2}$.

b) There is at least one primitive root g mod p which satisfies (5), hence there exists at least one primitive root mod p^α if $\alpha \geq 2$.

Theorem 10.5 of Apostol's book is

Theorem 4: Let g be a primitive root mod p, where p is an odd prime. Then the even powers $g^2, g^4, \ldots, g^{p-1}$ are the quadratic residues mod p, and the odd powers $g, g^3, \ldots, g^{p-2}$ are the quadratic nonresidues mod p.

A generalization of this result is relevant to higher order reciprocity.

1.2. A Partitioning of the Natural Numbers 1, 2, 3, ..., Q–1 into N Set, Q is a Prime, N Divides Q – 1

If q is a prime and x is an natural number where q does not divide x, then $x^{q-1} \equiv 1 \pmod q$ (Fermat's "little" theorem). Let g be a primitive root of q. The least residues modulo q of $g^1, g^2, g^3, \ldots, g^{q-1}$ are in some order $1, 2, 3, \ldots, (q-1)$. (If $g^i = g^j \pmod q$, $1 \leq i \leq q-1$, $1 \leq j \leq q-1$, $j < i$, then $g^{i-j} \equiv 1 \pmod q$, $1 \leq i - j \leq q - 1$, a contradiction to the definition of a primitive root. The least residues modulo q of $g^1, g^2, g^3, \ldots, g^{q-1}$ must then be a permutation of $1, 2, 3, \ldots, q-1$). Denote

$(q-1)/n$ by r. Let T_i, $i = 1, 2, 3, ..., n$ denote the least residues modulo q of $g^i, g^{i+n}, g^{i+2n}, ..., g^{i+(r-1)n}$. This is the partitioning of the natural number 1, 2, 3, ..., $q-1$ into n sets that will be discussed in this paper. Let s_i denote the number of consecutive integers in T_i (after sorting). For example, 2 is a primitive root of 13, so for $q = 13$, $n = 3$, and $g = 2$, $T_1 = \{2, 3, 11, 10\}$, $T_2 = \{4, 6, 9, 7\}$, $T_3 = \{8, 12, 5, 1\}$, $s_1 = 2$, $s_2 = 1$, and $s_3 = 0$ (If, for example, $x, x+1$, and $x+2$ are elements of a set, then the number of consecutive integers in this sequence is considered to be 2. Similar counting of consecutive integers in a set applies for longer sequences). A prime greater than 2 has more than one primitive root, but using a different primitive root makes no essential difference; the indices of the sets are just permuted. If g_1 is another primitive root of q, then $g_1 \equiv g^h \pmod q$ where h and $q-1$ are relatively prime. The least residues modulo q of $g^i, g^{i+n}, g^{i+2n}, ..., g^{i+(r-1)n}$ are in some order the least residues modulo q of $g_1^j, g_1^{j+n}, g_1^{j+2n}, ..., g_1^{j+(r-1)n}$ where $j \equiv k_i \pmod n$ and k and n are relatively prime. For example, 6 is another primitive root of 13 and $T_1 = \{6, 9, 7, 4\}$, $T_2 = \{10, 2, 3, 11\}$, and $T_3 = \{8, 12, 5, 1\}$ in this case. The T_n set is always the same no matter which primitive root is used.

The least residues modulo q of $g^i, g^{i+n}, g^{i+2n}, ..., g^{i+(r-1)n}$ are the roots of the congruence $x^{(q-1)/n} \equiv y \pmod q$, $0 < x < q, y^n \equiv 1 \bmod q$, $0 < y < q$. This is another way of interpreting the sets $T_1, T_2, T_3, ..., T_n$. If $n = 2$, the set T_1 consists of the quadratic non-residues mod q and the set T_2 consists of the quadratic residues of q. If $n > 2$, the set T_n consists of residues and the other sets consists of non-residues, but there is no advantage in lumping the non-residue sets together.

1.3. Application of Method to Quadratic Reciprocity

For $p = 113$ and $n = 4$ the above partitioning of the natural numbers is

3	9	5	1
6	11	10	2
12	13	19	4
17	18	20	7
21	22	27	8
23	25	33	14
24	26	35	15
29	31	37	16
34	36	38	28
42	41	39	30
45	44	40	32
46	50	43	49
48	51	47	53
55	52	54	56
58	61	59	57
65	62	66	60
67	63	70	64
68	69	73	81
71	72	74	83
79	77	75	85
84	82	76	97
89	87	78	98
90	88	80	99
92	91	86	105

96	95	93	106
101	100	94	109
107	102	103	111
110	104	108	112

$s_1 = 4$, $s_2 = 6$, $s_3 = 8$, and $s_4 = 9$. (The number of degrees of freedom is four. Primes for $n = 4$ usually have two or four degrees of freedom). The pairs of consecutive integers in the first column are (23, 24), (45, 46), (67, 68), and (89, 90). The objective is to find other differences modulo 113 where the number of pairs of integers in the first column having this difference is also four. Pairs of integers with a difference of 2 are (21, 23), (46, 48), (65, 67), and (90, 92) and the criterion is satisfied. Pairs of integers with a difference of 15 are (6, 21), (92, 107), (101, 3), and (110, 12) and the criterion is satisfied. Note that in the last two pairs, the differences are modulo 113. These and other similar differences constitute the first column in the following table. The procedure is repeated (again for integers in the first column) where the number of pairs of integers having the specified difference is 6. These differences constitute the second column in the following table, etc. A table of the differences is:

1	5	9	3
2	10	11	6
4	19	13	12
7	20	18	17
8	27	22	21
14	33	25	23
15	35	26	24
16	37	31	29
28	38	36	34
30	39	41	42
32	40	44	45
49	43	50	46
53	47	51	48
56	54	52	55
57	59	61	58
60	66	62	65
64	70	63	67
81	73	69	68
83	74	72	71
85	75	77	79
97	76	82	84
98	78	87	89
99	80	88	90
105	86	91	92
106	93	95	96
109	94	100	101
111	103	102	107
112	108	104	110

The counts for column 1 are 4, the counts for column 2 are 6, the counts for column 3 are 8, and the counts for column 4 are 9. The transformation just permutes the columns. See the appendix (the Methods section) for *C* code that does the transformation in the $n = 4$ case. The primes in columns 1 and 3 are quadratic residues modulo 113 and the primes in columns 2 and 4 are quadratic non-residues. 113 is a quadratic residue modulo the primes in columns 1 and 3 and a non-residue of the primes in columns 2 and 4. This is a result consistent with the quadratic reciprocity law. Note that the case where p and q are both of the form $4k + 3$ is not considered here. The differences modulo p are completely multiplicative. This can be proved for classical quadratic reciprocity using the Chinese remainder theorem. See Chapter 5 of Mollin's (1998) book for an introduction to the applicability of the Chinese remainder theorem to quadratic reciprocity. The differences modulo p are a finite commutative group having multiplication as the binary operation. A table of the reciprocity in general is

2	11
4	13
7	22
8	26
14	31
16	41
28	44
32	52
49	61
53	62
56	77
64	82
83	88
97	91
98	104
106	
109	
112	

The first column corresponds to the integers in the first column of the previous table and the second column corresponds to the integers in the third column of the previous table. A group of entries in the first column is 2, 2^2, 2^3, 2^4, 2^5, and 2^6. Another group of entries is 7, $2 \cdot 7$, $2^2 \cdot 7$, $2^3 \cdot 7$, and $2^4 \cdot 7$. Another group of entries is 7^2 and $2 \cdot 7^2$. Another group is 53 and $2 \cdot 53$. Finally, there is the group of primes 83, 97, and 109. A "basis" for the entries in the first column could be said to be 2, 7, 53, 83, 97, and 109. A group of entries in the second column is 11, $2 \cdot 11$, $2^2 \cdot 11$, and $2^3 \cdot 11$. A similar group is 13, $2 \cdot 13$, $2^2 \cdot 13$, and $2^3 \cdot 13$. Another group is $7 \cdot 11$ and $7 \cdot 13$. Note that 7 is a prime in the first column. Another group is 31 and $2 \cdot 31$. Another group is 41 and $2 \cdot 41$. Note that 2 is a prime in the first column. Finally, there is the prime 61. Considering the columns together, the basis is just the primes 2, 7, 11, 13, 31, 41, 53, 61, and 83, 97, and 109. The first two primes are relatively small and will be designated as being "primary units". None of the elements are divisible by 3 or 5, so all the primes up to 11 are accounted for. Secondary and tertiary units will be defined for higher order reciprocity.

Note that infinitely many examples of prime quadratic reciprocity can be generated from the above values using Dirichlet's theorem that there are infinitely many primes in an arithmetic progression. For example, in the arithmetic progression $2 + 113k$, primes occur for $k = 9, 13, 15, 39, \ldots$.

A distinguishing feature of quadratic reciprocity is that the bases consist of primes. Bases in cubic reciprocity for example, can include composite numbers. That 2 is in the basis follows from the following theorem.

The Supplement to the Quadratic Reciprocity Law is

Theorem 5: $\left(\frac{2}{p}\right)=(-1)^{\left(p^2-1\right)/8}$

See Mollin's (1999) book. Here, the Legendre symbol is denoted differently.

For $p = 109$ and $n = 4$, $s_1 = 7$, $s_2 = 6$, $s_3 = 7$, and $s_4 = 6$ (there are 2 degrees of freedom). The basis is just the primes 3, 5, 7, 29, 31, 43, 61, 71, 73, 83, 89, and 97. The method gives 4 (a square) as a solution even though 2 is not a solution. Such solutions (and multiples of them) will be designated as being "trivial".

For $p = 101$ and $n = 4$, $s_1 = 6$, $s_2 = 6$, $s_3 = 6$, and $s_4 = 6$ (there is 1 degree of freedom). The differences modulo p that satisfy reciprocity are 4, 5, 13, 17, 19, 20, 23, 25, 31, 37, 43, 47, 52, 65, 68, 71, 76, 79, 85, 92, 95, 97, and 100. In this case, 4 and 25 are trivial solutions. Other trivial solutions are $2^2 \cdot 5$, $2^2 \cdot 13$, $2^2 \cdot 17$, $2^2 \cdot 19$, and $2^2 \cdot 23$. Disregarding these solutions, there are only prime solutions and $5 \cdot 13$, $5 \cdot 17$, and $5 \cdot 19$. The basis is 5, 13, 17, 19, 23, 31, 37, 43, 47, 71, 79, and 97. When $(p - 1)/4$ is an odd square, there is only 1 degree of freedom. See Conjectures 7 and 8. By the supplemental reciprocity law, 2 cannot satisfy reciprocity in this case since $\left(p^2-1\right)/8=\frac{p+1}{2}\frac{p-1}{4}$ and $\frac{p+1}{2}$ is odd.

For $p = 197$ and $n = 4$, $s_1 = 12$, $s_2 = 12$, $s_3 = 12$, and $s_4 = 12$ (there is 1 degree of freedom). The differences modulo p that satisfy reciprocity are 4, 7, 19, 23, 28, 29, 37, 41, 43, 47, 49, 53, 59, 61, 76, 83, 92, 97, 101, 107, 109, 116, 127, 133, 137, 148, 157, 173, 181, 188, 191, 193, and 196. The only differences that are not prime are 2^2, $2^2 \cdot 7$, $2^2 \cdot 19$, $2^2 \cdot 23$, $2^2 \cdot 29$, $2^2 \cdot 37$, $2^2 \cdot 41$, $2^2 \cdot 43$, $2^2 \cdot 47$, and $2^2 \cdot 7^2$. Disregarding the trivial solutions, there are only prime solutions.

1.4. Application of Method to Rational Cubic Reciprocity

For $p = 157$ and $n = 6$ the above-mentioned partitioning of the natural numbers is

5	9	2	3	15	1
6	13	7	10	18	4
20	25	8	11	26	14
21	30	23	12	43	16
22	31	28	17	50	27
24	33	29	19	53	39
34	36	32	35	55	46
38	37	41	40	60	49
61	47	45	42	62	56
69	51	54	44	63	58
70	52	59	48	66	64
73	57	65	68	72	67
77	71	78	76	74	75
80	86	79	81	83	82
84	100	92	89	85	90
87	105	98	109	91	93
88	106	103	113	94	99
96	110	112	115	95	101
119	120	116	117	97	108
123	121	125	122	102	111

133	124	128	138	104	118
135	126	129	140	107	170
136	127	134	145	114	141
137	132	149	146	131	143
151	144	150	147	139	153
152	148	155	154	142	156

$s_1 = 8$, $s_2 = 6$, $s_3 = 5$, $s_4 = 4$, $s_5 = 2$, and $s_6 = 0$ (there are six degrees of freedom). A table of the differences modulo 157 (obtained from the first column above) is

1	15	3	2	9	5
4	18	10	7	13	6
14	26	11	8	25	20
16	43	12	23	30	21
27	50	17	28	31	22
39	53	19	29	33	24
46	55	35	32	36	34
49	60	40	41	37	38
56	62	42	45	47	61
58	63	44	54	51	69
64	66	48	59	52	70
67	72	68	65	57	73
75	74	76	78	71	77
82	83	81	79	86	80
90	85	89	92	100	84
93	91	109	98	105	87
99	94	113	103	106	88
101	95	115	112	110	96
108	97	117	116	20	119
111	102	122	125	121	123
118	104	138	128	124	133
130	107	140	129	126	135
141	114	145	134	127	136
143	131	146	149	132	137
153	139	147	150	144	151
156	142	154	155	148	152

Differences having a count of 8 are in the first column, differences having a count of 6 are in the second column, differences having a count of 5 are in the third column, etc. These differences are cubic residues modulo 157 (in the first and fourth columns) and cubic non-residues in the remaining columns. The transformation just permutes the columns. The differences modulo p for which reciprocity occur are

4	2
16	8
39	23
46	29
58	32
64	41
75	59
82	65
93	78
101	79
118	92
130	116
141	125
143	128
156	149
	150
	155

The first column corresponds to the integers in the first column of the previous table and the second column corresponds to the integers in the fourth column of the previous table. The units are 2, 3, 5, and 11. The only primary unit is 2. The secondary units are 3, 5, and 11. Two groups of primes are involved (disregarding the units and products consisting solely of units). The first group is 13, 31, and 47. Reciprocity occurs for $3 \cdot 13$, $3 \cdot 31$, and $3 \cdot 47$. Reciprocity also occurs for $5 \cdot 13$, $5 \cdot 31$ and $11 \cdot 13$. This is the rationale for saying that 3, 5, and 11 are secondary units. Reciprocity also occurs for the product $3 \cdot 5^2$ so that this is also considered to be a secondary unit. The second group of primes is 23, 29, 41, 59, 79, 101, and 149. Reciprocity occurs for these primes. The smallest of these primes is 23. None of the elements are divisible by 7 or 19 (primes of the form $6k + 1$), so all the primes up to 23 are accounted for.

There are usually three groups of primes (and no more) for which rational cubic reciprocity occurs. For small p-values, there may be only one or two groups of primes. Note that for $p = 157$, s_2, s_3, and s_4 are in arithmetic progression. Let r denote $(p-1)/n$. In this instance, r is even and $2^{2r} \equiv 1 (\mathrm{mod}\, p)$. Similar p-values (among many others) are 2017, 2281, 2341, and 3889.

For $p = 2017$, $s_1 = 66$, $s_2 = 58$, $s_3 = 54$, $s_4 = 50$, $s_5 = 42$, and $s_6 = 65$. The units are 2, 3, 5, 7, and 11. The only primary unit is 2. The only tertiary unit is 11. Reciprocity of the secondary units occurs for $3 \cdot 5^2$, $3^2 \cdot 5$, $5 \cdot 7^2$, $5^2 \cdot 7$, $3 \cdot 7^2$, and $3^2 \cdot 7$. The pairs $3 \cdot 5^2$ and $3^2 \cdot 5$, $5 \cdot 7^2$ and $5^2 \cdot 7$, and $3 \cdot 7^2$ and $3^2 \cdot 7$ are said to be inverses since reciprocity occurs for their respective products. One group of primes is 11, 23, 71, 73, 149, 163, 179, 251, 347, 419, 449, 467, 587, and 653. Reciprocity occurs for the respective products of these primes with 3, 5, and 7. Another group of primes is 47, 53, 59, 97, 199, 233, 293, 317, 353, 397, 431, 491, 509, 521, 599, and 613. Reciprocity occurs for the respective products of these primes with 3, 5, and 7. Another group of primes is 41, 43, 83, 107, 109, 113, 167, and 173. Reciprocity occurs for the respective products of these primes with 11. However, these products are not independent of the previous products since for example, reciprocity occurs for $3 \cdot 5 \cdot 11^2$ so that $11 \cdot 41$ is the inverse of $3 \cdot 5 \cdot 11^2$. The remaining group of primes is 17, 29, 31, 131, 137, 191, 229, 383, 563, 617, 677, 727, 971, 977, 1009, 1039, 1193, 1277, 1373, 1427, 1439, 1487, 1493, 1553, 1559, 1637, 1667, 1729, 1802, 1811, 1889, 1901, 89, 101, 181, 193, 227, 239, 257, 311, 337, 401, 443, 479, 557, 569, 577, 593, 619, 659, 701, 773, 787, 823, 863, 929, 953, 1031, 1061, 1097, 1109, 1289, 1307, 1381, 1499, 1613, 1787, 1789, 1907, and 1949. Reciprocity occurs for these primes. Note that 17 is the first of these primes. Reciprocity does not occur for 13 (a prime of the form $6k + 1$) or any product containing 13. The tertiary unit of 11 is defined so that all the primes up 17 are taken into account (at the expense of some redundancy in coverage).

For $p = 3889$, $s_1 = 90$, $s_2 = 102$, $s_3 = 108$, $s_4 = 114$, $s_5 = 126$, and $s_6 = 107$. The units are 2, 3, 5, 11, 17, 23, 29, 41, 47, 53, and 67. The only primary units are 2, 3, 23, 41, and 47. The only tertiary units are 53 and 67. Reciprocity of the secondary units occurs for $5 \cdot 11$, $11 \cdot 17$, $5^2 \cdot 17$, $5 \cdot 17^2$, and $11^2 \cdot 29$. The first group of primes is 29, 53, 59, 79, 101, 113, 131, 179, 191, 229, 233, 241, 281, 317, 359, 389, 419, 421, 449, 479, 483, 521, 541, 557, 607, 647, 653, 701, and 773. Reciprocity occurs for the respective products of these primes with 5 and 17. The second group of primes is 67, 89, 149, 173, 193, 239, 251, 263, 269, 293, 307, 311, 313, 347, and 353. Reciprocity occurs for the respective products of these primes with 11 and 29. Another group of primes consists of the sole element 67. Reciprocity occurs for the product of this prime with 53. However, reciprocity occurs for $5 \cdot 53$ and $11 \cdot 67$ so that this product is not independent. The remaining group of primes is 71, 83, 107, 137, 163, 167, 197, 223, 227, 257, 401, 433, 491, 577, 593, 599, 617, 719, 751, 839, 859, 881, 919, 941, 1013, 1019, 1097, 1103, 1151, 1171, 1187, 1193, 1217, 1223, 1279, 1307, 1321, 1409, 1439, 1481, 1493, 1559, 1571, 1609, 1697, 1733, 1783, 1787, 1823, 1889, 1931, 1949, 1979, 1997, 2003, 2027, 2069, 2087, 2099, 2111, 2129, 2161, 2309, 2393, 2417, 2441, 2459, 2579, 2687, 2693, 2729, 2749, 2753, 2843, 2861, 2879, 2887, 2903, 2927, 2953, 3023, 3061, 3067, 3137, 3121, 3187, 3191, 3221, 3137, 3187, 3191, 3203, 3221, 3271, 3299, 3319, 3323, 3329, 3359, 3389, 3413, 3449, 3457, 3461, 3469, 3527, 3557, 3593, 3643, 3671, 3673, 3701, 3727, 3733, 3761, 3779, 3793, 3797, 3863, and 3881. Reciprocity occurs for these primes. The smallest of these primes is 71. Reciprocity does not occur for 7, 13, 19, 31, 37, 43, or 61 (all of the form $6k + 1$) or any product containing these primes. The tertiary units of 53 and 67 are defined so that all the primes up to 71 are taken into account.

There are three possibilities for $n = 6$. Either r is even and $2^{2r} \equiv 1 \pmod{p}$, r is even and $2^{2r} \not\equiv 1 \pmod{p}$, or r is odd. See Conjectures 10 and 11. The case where r is even and $2^{2r} \not\equiv 1 \pmod{p}$ will now be considered. There are only four degrees of freedom for this case.

When $p = 2857$ and $n = 6$, $s_1 = 74$, $s_2 = 91$, $s_3 = 74$, $s_4 = 74$, $s_5 = 72$, and $s_6 = 90$ (there are four degrees of freedom). The units are 2, 3, 5, 7, 11, and 17. There are no primary or tertiary units. Reciprocity of the secondary units occurs for $2 \cdot 3$, $2 \cdot 7$, $2 \cdot 17$, $3 \cdot 5$, $3 \cdot 11$, $5 \cdot 7$, $5 \cdot 17$, $7 \cdot 11$, $11 \cdot 17$, $2 \cdot 5^2$, $2 \cdot 11^2$, $3 \cdot 7^2$, $3 \cdot 17^2$, $5 \cdot 11^2$, and $7 \cdot 17^2$. The first group of primes is 23, 59, 73, 89, 103, 107, 137, 149, 197, 211, 229, 263, 281, 347, 349, 389, 467, 479, 491, 509, 631, 647, 769, 797, 809, 827, 929, 947, 953, 977, 983, 997, 1009, 1013, 1031, 1151, 1163, 1181, 1187, 1193, 1321, and 1409. Reciprocity occurs for the respective products of these primes with 2, 5, and 11. The second group of primes is 29, 47, 71, 127, 163, 173, 179, 227, 269, 283, 311, 317, 401, 409, 431, 439, 443, 449, 503, 521, 563, 593, 599, 619, 641, 659, 661, 683, 701, 719, 743, 761, 811, 821, 853, 857, 859, 881, 887, and 941. Reciprocity occurs for the respective products of these primes with 3, 2^2, 7, and 17. The remaining group of primes is 19, 37, 41, 53, 67, 83, 101, 109, 113, 131, 139, 167, 191, 233, 239, 251, 257, 293, 313, 353, 359, 383, 419, 461, 557, 569, 587, 617, 653, 677, 739, 773, 839, 863, 911, 971, 1019, 1061, 1063, 1103, 1129, 1223, 1229, 1283, 1289, 1307, 1319, 1361, 1433, 1439, 1453, 1493, 1511, 1583, 1613, 1667, 1811, 1823, 1907, 1913, 1949, 2063, 2129, 2137, 2141, 2203, 2213, 2237, 2339, 2341, 2387, 2381, 2399, 2423, 2441, 2473, 2477, 2591, 2593, 2609, 2647, 2659, 2663, 2711, 2741, 2837, and 2843. Reciprocity occurs for these primes. The smallest of these primes is 19. Reciprocity does not occur for 13 or any product containing 13 so all primes up to 19 are taken into account.

The case where r is odd will now be considered.

For $p = 1423$ and $n = 6$, $s_1 = 37$, $s_2 = 44$, $s_3 = 37$, $s_4 = 37$, $s_5 = 44$, and $s_6 = 37$ (there are two degrees of freedom). The units are 2, 3, 5, 11, and 17. The only primary units are 2 and 5. There are no tertiary units. Reciprocity of the secondary units occurs for $3 \cdot 11^2$, $3 \cdot 17$, and $11 \cdot 17$. The first group of primes is 59, 83, 101, 139, 149, 179, 193, 227, 233, 241, 277, 281, 311, 359, 367, 379, 383, 389, 409, and 461. Reciprocity occurs for the respective products of these primes with 3 and 11. The second group of primes is 41, 43, 47, 71, 79, 107, 113, 131, and 151. Reciprocity occurs for the respective products of these primes with 3^2 and 17. Reciprocity also occurs for the primes 23, 29, 53, 61, 89, 137, 173, 181, 239, 263, 269, 283, 347, 349, 401, 443, 467, 503, 557, 569, 587, 617, 619, 683, 761, 89, 839, 857, 863, 877, 883, 911, 1031, 1049, 1061, 1103, 1193, 1223, 1277, 1283, 1301, 1307, 1321, 1367, 1373, and 1409. The smallest of these primes is 23. Reciprocity does not occur for 7, 13, or 19 or any products containing these primes so all primes up to 23 are taken into account.

1.5. Application of Method to Rational Quintic Reciprocity

For $p = 751$ and $n = 10$, $s_1 = 5$, $s_2 = 7$, $s_3 = 11$, $s_4 = 6$, $s_5 = 8$, $s_6 = 5$, $s_7 = 7$, $s_8 = 11$, $s_9 = 6$, and $s_{10} = 8$ (there are 5 degrees of freedom). In the differences modulo p (as computed above) there are five columns. The integers in the first column are quintic residues modulo 751 and the integers in the other columns are quintic non-residues modulo 751. The primes for which 751 is not a quintic residue are of the form $10k + 1$. The basis of the differences modulo p for which reciprocity occur involves five group of primes. The units are 2, 3, 5, 7, 13, 19, 23, 29, 37, and 43. There are no primary units. The tertiary units are 23, 29, 37, and 43. Reciprocity of the secondary units occurs for $2 \cdot 17$, $2^2 \cdot 13$, $2^2 \cdot 19$, $2^3 \cdot 13$, $2^3 \cdot 7^2$,

$2^4 \cdot 3$, $2^4 \cdot 5$, $2^4 \cdot 7$, $3 \cdot 17$, $3^2 \cdot 13$, $3^2 \cdot 19$, $3^3 \cdot 5^2$, $3^4 \cdot 7$, $5 \cdot 17$, $5^2 \cdot 13$, $5^2 \cdot 19$, $7 \cdot 17$, and $7^2 \cdot 13$. Reciprocity of the tertiary units occurs for $2^3 \cdot 23$, $2^3 \cdot 29$, $2^3 \cdot 37$, and $2 \cdot 43$. The first group of primes is 43, 97, 157, 173, 233, 239, 277, 317, and 349. Reciprocity occurs for the respective products of these primes with 2, 3, 5, and 7. The second group of primes is 113, 127, 139, and 167. Reciprocity occurs for the respective products of these primes with 2^2. The third group of primes is 23, 29, 37, 67, and 79. Reciprocity occurs for the respective products of these primes with 2^3, $2^2 \cdot 3$, 13, and 19. The fourth group of primes consists of the sole element 71. Reciprocity occurs for the products $2^2 \cdot 71$ and $3^2 \cdot 71$. Reciprocity also occurs for the primes 53, 73, 83, 107, 163, 179, 193, 197, 223, 229, 251, 307, 331, 337, 359, 373, 379, 467, 499, 503, 557, 569, 643, 673, and 719. The smallest of these primes is 53. Reciprocity does not occur for 11, 31, 41, or 61 (all primes of the form $10 \cdot k + 1$) or any product containing these primes. The tertiary units account for all the primes less than 53 except for 47.

When $p = 1471$, the s_i values equal 15 or 14 (two degrees of freedom). The units are 2, 3, 5, 7, 13, 17, 19, 23, 29, 37, 43, 47, 53, 59, 71, and 73. The primary unit is 3. The secondary units are 2, 3, 5, 7, 13, 17, 19, 23, 29, and 37. The tertiary units are 43, 47, 53, 59, 71, and 73. Reciprocity of the secondary units occurs for $2 \cdot 5 \cdot 13$, $2 \cdot 7 \cdot 13$, $2 \cdot 7 \cdot 29$, $2 \cdot 19$, $2 \cdot 23$, $2 \cdot 37$, $2^2 \cdot 5$, $2^2 \cdot 7$, $2^3 \cdot 17$, $2^3 \cdot 5 \cdot 19$, $2^3 \cdot 5 \cdot 23$, $2^3 \cdot 13 \cdot 17$, $2^3 \cdot 7 \cdot 19$, $2^3 \cdot 7 \cdot 23$, $2^3 \cdot 13^2$, $2^3 \cdot 19^2$, $2^4 \cdot 13$, $2^4 \cdot 29$, $5 \cdot 17$, $5 \cdot 7 \cdot 19$, $5 \cdot 7 \cdot 23$, $5 \cdot 7 \cdot 37$, $5 \cdot 13^2$, $7 \cdot 17$, $7 \cdot 13^2$, $7^2 \cdot 19$, $7^2 \cdot 23$, $13 \cdot 19$, $13 \cdot 23$, $13 \cdot 37$, and $23 \cdot 29$. Reciprocity of the tertiary units occurs for $2^4 \cdot 47$, $2^4 \cdot 53$, $2^4 \cdot 59$, $2^4 \cdot 73$, $2^2 \cdot 43$, $2^2 \cdot 71$, and $2 \cdot 17 \cdot 43$. The first group of primes is 67, 83, 173, 179, 193, 197, 239, 283, 293, 307, and 367. Reciprocity occurs for the respective products of these primes with 2^2. The second group of primes is 43, 71, 89, 103, 157, and 163. Reciprocity occurs for the respective products of these primes with 2^3, 5, and 7. The third group of primes is 127, 199, 227, 313, 337, 349, 353, 359, 397, 433, 457, 557, 617, 619, and 631. Reciprocity occurs for the respective products of these primes with 2. The fourth group of primes is 47, 53, 59, 73, 97, 107, 137, and 139. Reciprocity occurs for the respective products of these primes with 19, $2 \cdot 5$, and $2 \cdot 7$. Reciprocity occurs for the primes 79, 101, 109, 113, 149, 167, 229, 233, 263, 277, 401, 439, 449, 503, 587, 607, 647, 677, 683, 709, 719, 773, 797, 809, 947, 1009, 1063, 1129, 1217, 1249, 1289, 1433, and 1439. The smallest of these primes is 79. Reciprocity does not occur for 11, 31, 41, or 61 or any products containing these primes. The tertiary units account for all the primes less than 79.

See Conjectures 17, 18, 19, and 20 for properties of the s_i values when $n = 10$.

1.6. Application of Method to Rational Septumic Reciprocity

When $p = 1051$, and $n = 14$, $s_1 = 6$, $s_2 = 3$, $s_3 = 4$, $s_4 = 9$, $s_5 = 5$, $s_6 = 8$, and $s_7 = 2$. The units are 2, 3, 5, 77, 11, 13, 17, 19, 23, 31, 37, 41, 47, 53, 59, 61, and 67. There are no primary units. The tertiary units are 23, 31, 37, 41, 47, 53, 59, 61, and 67. Reciprocity of the secondary units occurs for $2 \cdot 7$, $3 \cdot 7$, $3 \cdot 5^2$, $3^3 \cdot 11$, $3^3 \cdot 13$, $3^4 \cdot 5$, $3^3 \cdot 17$, $2 \cdot 5^2$, $2^4 \cdot 5$, $2^3 \cdot 11$, $2^3 \cdot 13$, $2^3 \cdot 17$, $2^6 \cdot 3$, $2^5 \cdot 3^2$, $2^4 \cdot 3^3$, $2^3 \cdot 3^4$, $2^2 \cdot 3^5$, $5 \cdot 11$, $5 \cdot 13$, $5 \cdot 17$, $2^3 \cdot 3 \cdot 5$, $2^2 \cdot 3 \cdot 11$, $2^2 \cdot 3 \cdot 11$, $2^2 \cdot 3 \cdot 13$, $2^2 \cdot 3^2 \cdot 5$, $2 \cdot 3^2 \cdot 11$, $2^2 \cdot 3 \cdot 17$, $2 \cdot 3^2 \cdot 13$, $2 \cdot 3^3 \cdot 5$, $2 \cdot 3^2 \cdot 17$, $2^2 \cdot 5 \cdot 19$, $2 \cdot 11 \cdot 19$, $2 \cdot 13 \cdot 19$, $2 \cdot 3 \cdot 5 \cdot 19$, $3 \cdot 11 \cdot 19$, $2 \cdot 17 \cdot 19$, $2^2 \cdot 5^2 \cdot 7$, $3 \cdot 13 \cdot 19$, $2 \cdot 5 \cdot 7 \cdot 11$, $3^2 \cdot 5 \cdot 19$, $2 \cdot 5 \cdot 7 \cdot 13$, $24 \cdot 3 \cdot 19$, $3 \cdot 17 \cdot 19$, $7 \cdot 11 \cdot 13$, and $2 \cdot 3 \cdot 5^2 \cdot 7$. Reciprocity of the tertiary units occurs for $2 \cdot 23$, $2 \cdot 41$, $2 \cdot 47$, $3 \cdot 5 \cdot 31$, $3 \cdot 5 \cdot 37$, $3 \cdot 5 \cdot 61$, $3 \cdot 5 \cdot 67$, $7 \cdot 59$, and $2^3 \cdot 53$. Seven groups of primes are involved in the reciprocity of the differences modulo p. The first group of primes is 23, 41, 47, 157, 199, 227, 293, and 367. Reciprocity occurs for the respective products of these primes with 2 and 3. The second group of primes is 53, 83, 149, and 179. Reciprocity occurs for the respective products of these primes with 5, 2^3, 3^3, $2^2 \cdot 3$, and $2 \cdot 3^2$. The third group of primes is 31, 37, 61, 67, 71, and 103. Reciprocity occurs for the respective products of these primes with 11, 13, 17, 2^4, $2 \cdot 5$, $3 \cdot 5$, and $2^3 \cdot 3$. The fourth group of primes is 59, 89, and 109. Reciprocity occurs for the products of these primes with 7. The fifth group consists of the sole element 107. Reciprocity occurs for the products of this prime with 2^2, 3^2, and $2 \cdot 3$. The sixth group consists of the sole element 131. Reciprocity occurs for the products of this prime with 2^2 and $2 \cdot 3$. The final group is the primes 79, 97, 139, 163, 181, 307, 317, 409, 443, 557, 619, 653, 797, 859, 919, 914, and 971. Reciprocity occurs for these primes. The smallest element of this group is 79. No reciprocity occurs for 29 or 43 or any products containing these primes. The tertiary units account for all the primes less than 79 except 73.

See Conjecture 21 for properties of the s_i values when $n = 14$.

1.7. Application of Method to Rational Biquadratic Reciprocity

Tertiary units are not applicable to biquadratic reciprocity. For $p = 1153$ and $n = 8$, $s_1 = 14$, $s_2 = 22$, $s_3 = 12$, $s_4 = 17$, $s_5 = 26$, $s_6 = 20$, $s_7 = 24$, and $s_8 = 8$ (there are eight degrees of freedom). The units are 2, 3, 11, and 13. The only primary unit is 2. Reciprocity of the secondary units occurs for 3^2, $3 \cdot 11$, $3 \cdot 13$, $11 \cdot 13$, 11^2, and 13^2. The first group of primes is 43, 89, 109, 131, 139, 223, 271, 281, 313, 349, 379, and 383. Reciprocity occurs for the respective products of these primes with 3, 11, and 13. Reciprocity occurs for the second group of primes 23, 47, 67, 199, 239, 307, 419, 443, 499, 503, 523, 619, 859, 911, 941, 983, 997, 1013, 1061, and 1087. Note that there are two groups of primes other than the units.

For $p = 1801$ and $n = 8$, the si values equal 27 or 29. The units are 2, 3, 5, 7, and 17. The primary units are 2, 3, and 7. Reciprocity of the secondary units occurs for 5^2, 17^2, and $5 \cdot 17$. The first group of primes is 43, 101, 103, 107, 199, 223, 227, 263, 283, 331, and 359. Reciprocity occurs for the respective products of these primes with 5 and 17. Reciprocity occurs for the second group of primes 67, 113, 193, 197, 211, 233, 239, 257, 271, 367, 401, 467, 487, 503, 563, 599, 601, 643, 751, 773, 837, 863, 887, 911, 919, 937, 997, 1123, 1153, 1163, 1201, 1223, 1259, 1283, 1289, 1291, 1297, 1307, 1399, 1423, 1451, 1549, 1579, 1601, 1657, 1667, 1693, 1747, 1759, 1783, 1787, and 1789.

For $p = 2393$, the s_i values equal 39, 35, or 36. The units are 2, 13, 17, and 23. The only primary unit is 2. Reciprocity of the secondary units occurs for 13^2, 17^2, 23^2, $13 \cdot 17$, $13 \cdot 23$, and $17 \cdot 23$. The first group of primes is 71, 127, 131, 137, 151, and 179. Reciprocity occurs for the respective products of these primes with 13, 17, and 23. Reciprocity occurs for the second group of primes 73, 79, 83, 107, 139, 163, 199, 233 239, 263, 271, 283, 311, 331, 367, 369, 431, 439, 521, 547, 569, 593, 607, 619, 647, 673, 691, 727, 811, 877, 887, 919, 1009, 1031, 1049, 1061, 1093, 1097, 1153, 1213, 1283, 1307, 1373, 1481, 1511, 1531, 1543, 1597, 1613, 1721, 1831, 1867, 1877, 1901, 1951, 1979, 2003, 2039, 2083, 2087, 2113, 2129, 2137, 2179, 2203, 2207, 2351, and 2377.

Reciprocity of the secondary units occurs for squares of primes and products of pairs of these primes. When $n = 8$, there are two degrees of freedom when $(p-1)/8$ is an odd square and $2^{(p-1)/4} \equiv 1 \pmod{p}$. See Conjectures 12 and 13. In addition to $p = 1801$, these conditions are satisfied for $p = 3529$ and $p = 8713$ (for p less than 10000).

1.8. Elementary Properties of the Number of Consecutive Elements in a Set

Theorems concerning $s_1, s_2, s_3, ..., s_n$ will now be proved. The proofs are not difficult, but some are fairly lengthy and details will be omitted.

Theorem 6: $s_1 + s_2 + s_3 + ... + s_n = r - 1$.

Proof: The congruence $x^{\frac{p-1}{n}} \equiv (x+1)^{\frac{p-1}{n}}$, $0 < x < p-1$, has exactly $\frac{p-1}{n} - 1$ roots.

Theorem 7: If r is odd and n is even, $s_i = s_{i+n/2}$, $i = 1, 2, 3, ..., (n/2)$.

Proof: If $y^n \equiv 1 \pmod{p}$ and n is even $(p-y)^n = 1 \pmod{p}$.

Theorem 8: If $n = 2$ and r is even, $s_1 = s_2 + 1$.

Proof: Let q be an odd natural number and suppose the integers 1, 2, 3, ..., $(q-1)$ are sorted at random into two sets A and B of $(q-1)/2$ elements each. Let σ_1 be the number of pairs of consecutive integer in A and σ_2 the number of pairs on consecutive integers in B. Let $\xi_1, \xi_2, ..., \xi_{(q-1)/2}$ be the elements of A arranged in ascending order and let x_{2i-1} and x_{2i}, $i = 1, 2, 3, ..., k$ be the first and last integers of the groups of consecutive integers in $\xi_1, \xi_2, ..., \xi_{(q-1)/2}$. Count an element of $\xi_1, \xi_2, ..., \xi_{(q-1)/2}$ not consecutive to its adjacent elements as being a group of one consecutive integer. For example, if $q = 13$ and $\xi_1, \xi_2, ..., \xi_6$ equal 1, 3, 4, 9, 10, 12 respectively, then $x_1 = x_2 = 1, x_3 = 3, x_4 = 4, x_5 = 9, x_6 = 10$, and $x_7 = x_8 = 12$. There are $x_{2i} - x_{2i-1}$ pairs of consecutive integers in the group having x_{2i-1} and x_{2i} as its first and last integers, therefore $\sum_1^k (x_{2i} - x_{2i-1}) = \sigma_1$. Also, since $x_{2i} - x_{2i-1} + 1$ is the number of elements in the group having x_{2i-1} and x_{2i} as its first and last integers, $\sum_{i=1}^k (x_{2i} - x_{2i-1} + 1) = \frac{q-1}{2}$. Therefore $\frac{q-1}{2} - k = \sigma_1$.

Case (1): 1 is in A and $q-1$ is in A:

$\sum_{i=1}^{k-1} (x_{2i+1} - x_{2i} - 2) = \sigma_2$ therefore $-\sum_{i=1}^k (x_{2i} - x_{2i-1}) - x_1 + x_{2k} - 2(k-1) = \sigma_2$.

Then $-\left(\frac{q-1}{2} - k\right) - 1 + (q-1) - 2(k-1) = \sigma_2$, $\left(\frac{q-1}{2} - k\right) + 1 = \sigma_2$, and $\sigma_1 + 1 = \sigma_2$.

Case (2): 1 is in B and $q-1$ is in B:

The logic is the same as for Case (1), so $\sigma_2 + 1 = \sigma_1$.

Case (3): 1 is in A, $(q-1)$ is in B:

$\sum_{i=1}^k (x_{2i+1} - x_{2i} - 2) + [(q-1) - x_{2k} - 1] = \sigma_2$,

therefore $-\sum_{i=1}^k (x_{2i} - x_{2i-1}) - x_1 + x_{2k} - 2(k-1) + (q-1) - x_{2k} - 1 = \sigma_2$.

Then $-\left(\frac{q-1}{2}-k\right)-1-2(k-1)+(q-1)-1=\sigma_2$, and $\sigma_1=\sigma_2$.

Case (4): 1 is in B, $(q-1)$ is in A:

The logic is the same as for Case (3), so $\sigma_2=\sigma_1$.

If $(p-1)/2$ is even, 1 and $p-1$ are roots of $x^{(p-1)/2}\equiv 1 \pmod p$, therefore $s_2+1=s_1$. If $(p-1)/2$ is odd, $p-1$ is not a root of $x^{(p-1)/2}\equiv 1 \pmod p$, therefore $s_2=s_1$.

Theorem 9: If 6 does not divide r and $2^r \not\equiv 1 \pmod q$, then 6 divides s_n. If 6 divides r and $2^r \not\equiv 1 \pmod q$, then $s_n \equiv 2 \pmod 6$. If 6 does not divide r and $2^r \equiv 1 \pmod q$, then $s_n \equiv 3 \pmod 6$. If 6 divides r and $2^r \equiv 1 \pmod q$, then $s_n \equiv 5 \pmod 6$.

The following is a brief explanation of this theorem. Let x^{-1} denote an integer such the $xx^{-1} \equiv 1 \pmod q$. Let $C(x)$ denote the least residues modulo q of x, $1-x$, $(1-x)^{-1}$, $-x(x-1)^{-1}$, $-x^{-1}(1-x)$, and x^{-1} (the formal values of the cross-ratio function). If one element of $C(x)$ is a root of $x^{(q-1)/n}\equiv 1 \pmod q$, then every element of $C(x)$ is a root and is one larger than another root. The elements of $C(x)$ are distinct unless 2 is an element of $C(x)$ (in which case the distinct elements are 2, $(q+1)/2$, and $q-1$) or a root of $x^2-x+1\equiv 0 \pmod q$, $0<x<q$ is an element of $C(x)$ (in which case the distinct elements are the two root of $x^2-x+1\equiv 0 \pmod q$, $0<x<q$). $x^2-x+1\equiv 0 \pmod q$ has a root if and only if 6 divides $q-1$.

1.9. Non-Elementary Properties of the Number of Consecutive Elements in a Set

There are an abundance of non-elementary properties of $s_1, s_2, s_3, ..., s_n$. Some empirical results for $n \le 16$ and $q < 40000$ are

Conjecture 1: If $n=3$, r is a square, and $2^r \not\equiv 1 \pmod q$, then $s_1-s_2=s_2-s_3$ (or $s_2-s_1=s_1-s_3$ for some other primitive root of q).

Conjecture 2: If $n=3$, then $s_1-s_2=s_2-s_3$ (or $s_2-s_1=s_1-s_3$) only if r is a square.

Conjecture 3: If $n=3$, r is a square, and $2^r \equiv 1 \pmod q$, then $s_1-s_2+2=s_1-s_3$.

Conjecture 4: If $n=3$, then $s_1-s_2+2=s_1-s_3$ only if r is a square.

Conjecture 5: If $n=3$, then $s_1=s_3$ (or $s_2=s_3$) only if $n/2$ is odd.

Conjecture 6: If $n=3$, then $s_1 \ne s_2$.

Conjecture 7: If $n=4$ and r is an odd square, then $s_1=s_2=s_3=s_4$.

Conjecture 8: If $n=4$, then $s_1=s_2=s_3=s_4$ only if r is an odd square.

Conjecture 9: If $n=4$ and r is even, then $s_1-s_2=s_2-s_3$.

Conjecture 10: If $n=6$, r is even, and $2^{2r} \not\equiv 1 \pmod q$, then $s_1=s_3=s_4$ (or $s_2=s_3=s_5$ for some other primitive root of q).

Conjecture 11: If $n=6$, r is even, and $2^{2r} \equiv 1 \pmod q$, then $s_2-s_3=s_3-s_4$ and $s_1-s_2=s_4-s_5=2(s_2-s_3)$ (or $s_2-s_3=s_3-s_4$ and $s_1-s_2=s_4-s_5=2(s_3-s_4)$ for some other primitive root of q).

Conjecture 12: If $n=8$, r is an odd square, and $2^{2r} \equiv 1 \pmod q$, then $s_1=s_3=s_5=s_7$ and $s_2=s_4=s_6=s_8$.

Conjecture 13: If $n=8$, then $s_1=s_3=s_5=s_7$ and $s_2=s_4=s_6=s_8$ only if r is an odd square.

Conjecture 14: If $n=8$, r is odd, and $2^{2r} \equiv 1 \pmod q$, then $s_1=s_3$ and $s_5=s_7$.

Conjecture 15: If $n=8$, r is even, and $2^{2r} \not\equiv 1 \pmod q$, then $s_1=s_3=s_5=s_7$.

Conjecture 16: If $n=8$, r is even, and $2^{2r} \equiv 1 \pmod q$, then $s_1-s_3=s_5-s_7$.

Conjecture 17: If $n=10$, r is even, and $2^{2r} \not\equiv 1 \pmod q$, then $s_1=s_6=s_7$ and $s_3=s_5=s_8$ (for some primitive root of q).

Conjecture 18: If $n=10$, r is even, and $2^{2r} \equiv 1 \pmod q$, then $s_1-s_2=s_8-s_9$, $s_3-s_4=s_6-s_7$, and $s_2-s_3-s_7+s_8=-2(s_4-s_5-s_5+s_6)$.

Conjecture 19: If $n=10$, r is odd, and $2^{2r} \equiv 1 \pmod q$, then $s_1-s_2=s_3-s_4$ and $s_6-s_7=s_8-s_9$ (for some primitive root of q).

Conjecture 20: If $n = 10$, r is odd, and $2^{2r} \not\equiv 1 \pmod{q}$, then $s_1 - s_4 = s_4 - s_2$ and $s_6 - s_9 = s_9 - s_7$ (for some primitive root of q).

Conjecture 21: If $n = 14$, r is odd, and $2^{2r} \not\equiv 1 \pmod{q}$, then $s_1 = s_8$ and $s_5 = s_{12}$ (for some primitive root of q).

That the condition $2^r = 1 \pmod{q}$ (or $2^r \not\equiv 1 \pmod{q}$) has an effect on the s_i values is to be expected from Theorem 9. There does not appear to be any simple explanation for r being a square having an effect on the s_i values (when n equal 3, 4, or 8). When $n = 2$, there is a definite connection between the s_i values and quadratic reciprocity and this connection is provided by Perron's theorem.

1.10 Perron's Theorem

Theorem 8.4 in Vermani's (1996) book is

Theorem 10: If $p = 4k + 1$, then $\theta^2 = p$.

Theorem 8.5 is

Theorem 11: If $p = 4k - 1$, then $\theta^2 = -p$.

Here, the Gaussian sum is defined by $\theta = \sum_{i=1}^{p-1} \chi(i)\alpha^i$ where $\chi(i)$ is the Legendre symbol and α is a primitive p^{th} root of unity in some extension of the field GF(s). s is another prime which is a quadratic residue mod p. A finite field is called a Galois field and if F is a field of order p^n, we write $F = GF(p^n)$. $\chi(i) = 0$ if i is a multiple of p, 1 if i is q quadratic residue mod p, or -1 if i is a non-residue mod p. Vermani uses Perron's theorem to prove these theorems.

Perron's theorem is

Theorem 12: (1) Suppose $p = 4k - 1$. Let $r_1, r_2, r_3, \ldots, r_{2k}$ be the $2k$ quadratic residues modulo p together with 0, and let a be a number relatively prime of p. Then among the $2k$ numbers $r_i + a$, there are k residues (possibly including 0) and k non-residues. (2) Suppose $p = 4k - 1$. Let $n_1, n_2, n_3, \ldots, n_{2k-1}$ be the $2k - 1$ non-residues. Then among the $2k - 1$ numbers $n_i + a$, there are k residues (possibly including 0) and $k - 1$ non-residues. (3) Suppose $p = 4k + 1$. Among the $2k + 1$ numbers $r_i + a$ are, if a is itself a residue, $k + 1$ residues (including 0) and k non-residues; and, if a is a non-residue, k residues (not including 0) and $k + 1$ non-residues. (4) Suppose $p = 4k + 1$. Among the $2k$ numbers $n_i + a$ are, if a is itself a residue, k residues (not including 0) and k non-residues; and, if a is a non-residue, $k + 1$ residues (including 0) and $k - 1$ non-residues.

Vermani does not include the proof of this theorem (or include it in his bibliography). Theorem 8 can be used to prove the theorem for the case $a = 1$. From there, the theorem can be proved for general a values.

1.11. An Algorithm for Computing Generalized Gauss Sums

See the appendix for *C* code for computing quadratic and cubic Gauss sums. Other than the arithmetic in the different fields and the number of iterations, the algorithm is essentially the same for quadratic and all higher order Gauss sums. For $p = 11$ and quadratic Gauss sums, the output is 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, –10. The normalized (divided by p) Gauss sum is taken to be 1. For $p = 13$ and quadratic Gauss sums, the output is –1, –1, –1, –1, –1, –1, –1, –1, –1, –1, –1, –1, 12. The normalized Gauss sum is taken to be –1. For $p = 13$ and cubic Gauss sums, the output after the first iteration is (3, –1), (–4, –3), (–4, –3), (1, 4), (3, –1), (1, 4), (1, 4), (3, –1), (1, 4), (–4, –3), (–4, –3), (3, –1), (0, 0). The output after the second and final iteration is (4, 3), (4, 3), (4, 3), (4, 3), (4, 3), (4, 3), (4, 3), (4, 3), (4, 3), (4, 3), (4, 3), (–48, –36). The normalized cubic Gauss sum is taken to be (4, 3). Note that $(13 - 1)/3$ is a square (of 2) so that Conjecture 1 is applicable. Denote the square roots of these values by s. In this case, $(2s, s + 1) = (4, 3)$. For $p = 13$, 193, 769, 1201, 1453, 2029, 3469, 3889, 4801, and 10093, $(p - 1)/3$ is a square. The following conjecture is based on this data.

Conjecture 22: If $n = 3$ and $(p - 1)/n$ is square, then either $(2s, s + 1)$, $(-s - 1, s + 1)$, or $(-2s, -s + 1)$ equals the normalized cubic Gauss sum.

For $p = 5$ and biquadratic Gauss sums, the output after the third and final iteration is (3, –4), (3, –4), (3, –4), (3, –4), (–12, 16). The normalized biquadratic Gauss sum is taken to be (3, –4). Note that $(5 - 1)/4$ is a square (of 1) so that Conjecture 7 is applicable. In this case $(p - 2, -4s) = (3, -4)$. For $p = 5$, 37, 101, and 197 $(p - 1)/4$ is an odd square. The following conjecture is based on this data.

Conjecture 23: If $n = 4$ and $(p - 1)/n$ is an odd square, then either $(p - 2, -4s)$ or $(p - 2, 4s)$ equals the normalized biquadratic Gauss sum.

1.12. Cubic Reciprocity

Let ξ be a primitive p^{th} root of unity. The principal quadratic Gaussian sum is $\sum(j/p)\xi^j$ where the summation is from $j = 1$ to $p - 1$ and j/p denotes the Legendre symbol. The generalization of Gaussian sums for $n > 2$ is straight forward; instead of multiplying powers of ξ by 1 or –1 (roots of $x^2 - 1$), powers of ξ are multiplied by powers of a primitive nth root of unity. For $n = 3$, $\rho = e^{(2/3)\pi i} = (1/2)\left(-1 + i\sqrt{3}\right)$ is a primitive n^{th} unity of unity. The numbers $\xi = a + b\rho$ where a and b are rational integers are called the integers of the field $k(\rho)$. The norm of the integer $a + b\rho$ is $a^2 - ab + b^2$. An integer whose norm is a rational prime is a prime in $k(\rho)$. If $\xi \equiv \pm(\text{mod } 3)$, then ξ is said to be primary. For example, for $p = 13$, $n = 3$, and $g = 2$ (a primitive root of 13), the least residues modulo p of g^1, g^4, g^7, and g^{10} are 2, 3, 11, and 10, and these powers of ξ are multiplied by 1, the least residues modulo p of g^2, g^5, g^8, and g^{11} are 4, 6, 9, and 7, and these powers of ξ are multiplied by ρ, and the least residues modulo g^3, g^6, g^9, and g^{12} are 8, 12, 5, and 1, and these powers of ξ are multiplied by ρ^2. The generalized Gaussian sum is $\rho^2\xi^1 + \xi^2 + \xi^3 + \rho\xi^4 + \rho^2\xi^5 + \rho\xi^6 + \rho\xi^7 + \rho^2\xi^8 + \rho\xi^9 + \xi^{10} + \xi^{11} + \rho^2\xi^{12}$. The cube of the generalized Gaussian sum is $p\pi$ where p is a primary prime in $k(\rho)$ having a norm of p. Let R be the set of primes of the form $3i + 1$. For distinct primes p and q in R, q is a rational cube modulo p (this is an abbreviated way of saying that q is congruent to the cube of an integer modulo p) if and only if $p\pi_p$ is a cube of an integer in $k(\rho)$ modulo q. Also, p is a rational cube modulo q if and only if $q\pi_q$ is a cube of an integer in $k(\rho)$ modulo p. Therefore q is a cube modulo p and p is a cube modulo q if and only if π_p is a cube of an integer (in $k(\rho)$) modulo q and π_q is a cube of an integer (in $k(\rho)$) modulo p.

See Chapter 5.1 of Mollin's (1998) book for a rigorous treatment of cubic reciprocity.

1.13. Biquadratic Reciprocity

For $n = 4$, the generalized Gaussian sum would be similarly formed. The fourth power of this generalized Gaussian sum is $p\pi^2$ where π is a prime in $k(i)$ having a norm of p. See Chapter 5.2 of Mollin's book for a rigorous treatment of biquadratic reciprocity.

2. Results

A connection between the numbers of pairs of consecutive roots of the congruences $x^{(p-1)/n} \equiv y(\text{mod } p)$, $0 < x < p$, $y^n \equiv 1(\text{mod } p)$, $0 < y < p$, and n^{th} order reciprocity is made. An algorithm for computing generalized Gaussian sums is given. The number of pairs of consecutive roots of the congruences are shown to be relevant to these generalized Gaussian sums. A simplified explanation of cubic reciprocity (not necessarily rational) is given. Empirical observations are made.

3. Conclusion

When q is a n^{th} power modulo p is determined using the primitive roots of p, but whether there is reciprocity is determined empirically. That there are $n/2$ groups of primes other than the units for quadratic ($n = 2$) and biquadratic ($n = 4$) reciprocity would be difficult to prove. Similarly, that there are n groups of primes other than units for nth order reciprocity, $n = 3, 5, 7, 11, ...$, for sufficiently large p would be difficult to prove. Even rigorously defining the units would be difficult.

References

Apostol, T.M. (1976). *Introduction to Analytic Number Theory*. Springer, New York, NY. DOI: https://doi.org/10.1007/978-1-4757-5579-4.

Sun, Zhi-Hong. (1998). On the theory of cubic residues and nonresidues. *Acta Arith*, *84*(4), 291-335.

Sun, Zhi-Hong. (2001). Supplements to the theory of quartic residues. *Acta Arith. 97*(4), 361-377.

Mollin, Richard, A. (1998). *Fundamental Number Theory with Applications*. CRC Press.

Vermani, Lekh, R. (1996). *Elements of Algebraic Coding Theory: 12 (Chapman and Hall Mathematics Series). Springer.*

Mollin, Richard, A. (1999). *Algebraic Number Theory. Second Edition. CRC Press.*

Appendix

```
TESTX2_C.htm[3/30/2022 9:46:54 AM]
/*****************************************************************************/
/* */
/* QUADRATIC RECIPROCITY (transformation) */
/* 12/11/21 (dkc) (n=4) */
/* */
/* The input is the first group of nonresidues. The distinct s[i] values */
/* are in the "select" array. "degree" is set accordingly. */
/* */
/*****************************************************************************/
#include <stdio.h>
#include <math.h>
//#include "out2a.h" // p=193
//#include "out2b.h" // p=2917
//#include "out2c.h" // p=97
//#include "out2d.h" // p=109
//#include "out2e.h" // p=113
//#include "out2f.h" // p=1889
//#include "out2g.h" // p=997
//#include "out2h.h" // p=521
//#include "out2i.h" // p=113, column[4] selected
#include "out2j.h" // p=101
int main () {
//unsigned int size=28; // size of n, p=113
//unsigned int size=48; // size of n, p=193
//unsigned int size=729; // size of n, p=2917
//unsigned int size=24; // size of n, p=97
//unsigned int size=27; // size of n, p=109
//unsigned int size=472; // size of n, p=1889
//unsigned int size=249; // size of n, p=997
//unsigned int size=130; // size of n, p=521
unsigned int size=25; // size of n, p=101
unsigned int p=101;
unsigned int degree=1; // size of select
//unsigned int select[4]={4,6,8,9}; // p=113
//unsigned int select[3]={8,11,14}; // p=193
//unsigned int select[1]={182}; // p=2917
//unsigned int select[4]={8,7,6,2}; // p=97
//unsigned int select[2]={7,6}; // p=109
//unsigned int select[4]={130,120,110,111}; // p=1889
//unsigned int select[2]={66,58}; // p=997
//unsigned int select[3]={36,31,26}; // p=521
unsigned int select[1]={6}; // p=101
unsigned int norec=1; // if set, no reciprocity
```

Appendix (Cont.)

```
unsigned int del;
unsigned int h,i,j,k,r,count,sel,q;
unsigned int f[6000],v[6000],in[6000];
unsigned int qp,t,indf,indv,index;
FILE *Outfp;
Outfp = fopen("outx2.dat","w");
index=0;
for (k=1; k<=degree; k++) {
 sel=select[k-1];
 for (h=1; h<p; h++) {
  del=h;
  count=0;
 for (i=0; i<size; i++) {
  r=(unsigned int)n[i]+del;
 if (r>=p) {
  r=r-(r/p)*p;
// printf("r=%d \n",r);
 for (j=0; j<i; j++) {
  if ((unsigned int)n[j]==r)
 count=count+1;
  }
 }
 else {
 for (j=i+1; j<size; j++) {
 if ((unsigned int)n[j]==r)
 count=count+1;
    }
  }
 }
 printf("del=%d, count=%d \n",del,count);
 if (count==sel) {
 in[index]=del;
 index=index+1;
// fprintf(Outfp," %d, \n",del);
     }
   }
 }
TESTX2_C.htm[3/30/2022 9:46:54 AM]
//
// check reciprocity
//
if (index!=(p-1)) {
 printf("error: index=%d, p=%d \n",index,p);
 return(0);
```

Appendix (Cont.)

```
 }
if (norec!=0) {
    for (h=0; h<(p-1); h++)
        fprintf(Outfp," %d, \n",in[h]);
 return(0);
 }
count=0;
q=p;
qp=q;
indf=1;
for (h=1; h<q; h++) {
   p=(unsigned int)in[h-1];
  for (i=1; i<q; i++) {
    t=i*i;
    t=t-(t/q)*q;
   if (t==p) {
// printf(" %d %d %d \n",q,p,i);
// fprintf(Outfp," %d %d %d \n",q,p,i);
 f[indf-1]=p;
 indf=indf+1;
 break;
     }
  }
 }
indv=1;
for (h=1; h<qp; h++) {
 p=(unsigned int)in[h-1];
 q=qp;
 if (q>p)
 q=q-(q/p)*p;
 for (i=1; i<p; i++) {
   t=i*i;
    t=t-(t/p)*p;
   if (t==q) {
// printf(" %d %d %d \n",qp,p,i);
// fprintf(Outfp," %d %d %d \n",qp,p,i);
 v[indv-1]=p;
 indv=indv+1;
 break;
    }
  }
 }
indf=indf-1;
indv=indv-1;
```

Appendix (Cont.)

```
//printf(" %d %d %d %d \n",indf,indv,f[indf-1],v[indv-1]);
for (h=1; h<=indf; h++) {
  p=f[h-1];
 for (i=1; i<=indv; i++) {
  if (v[i-1]==p) {
   printf(" %d \n",p);
   fprintf(Outfp," %d, \n",p);
   count=count+1;
  break;
    }
  }
 }
printf("p=%d, count=%d \n",qp,count);
fprintf(Outfp,"p=%d, count=%d \n",qp,count);
fclose(Outfp);
return(0);
}
compute square of Gaussian sum
gauss2.htm[11/16/2021 10:18:21 AM]
/*************************************************************************/
/* */
/* COMPUTE SQUARES OF GAUSSIAN SUMS */
/* 11/14/97 (dkc) */
/* */
/* This C program computes squares of Gaussian sums. */
/* */
/*************************************************************************/
#include "input.h"
#include <stdio.h>
int main ()
{
/*************************************************************************/
/* p is a prime, n is a divisor of p-1, and r is a primitive root of p, */
/* the cyclotomic cosets are stored in c[n][(p-1)/n] */
/*************************************************************************/
unsigned int n, p, r;
unsigned int c[2][500]; // c[n][(p-1)/n]
unsigned int sum[1002],temp[1002],save[1002];
unsigned int k[1002];
unsigned int g, h, i, j;
FILE *Outfp;
Outfp = fopen("gauss2b.dat","w");
n=2;
for (g=0; g<100; g++) {
```

Appendix (Cont.)

```
  p=input[2*g];
  r=input[2*g+1];
/*********************************************************************/
/* generate permutation of 1,2,3...,(p-1) (by Fermat's theorem) */
/*********************************************************************/
 k[0] = r;
 for (i=1; i<p-1; i++) {
    k[i] = k[i-1]*r - ((k[i-1]*r)/p)*p;
    }
 for (i=0; i<p-2; i++) {
  if (k[i] == 1) {
    fprintf(Outfp,"error: r is not a primitive root of p \n");
   goto bskip;
    }
 }
/*********************************************/
/* sort permutation into cyclotomic cosets */
/*********************************************/
 for (h=0; h<n; h++) {
  j=0;
   for (i=h; i<p-1; i+=n) {
     c[h][j] = k[i];
     j=j+1;
     }
   }
/***************************/
/* compute Gaussian sum */
/***************************/
 j=1;
 for (h=0; h<n; h++) {
    j=j*-1;
    for (i=0; i<(p-1)/n; i++) {
     temp[c[h][i]]=j;
     }
  }
 temp[0]=0;
/***********************************/
/* compute square of Gaussian sum */
/***********************************/
/***************************/
/* initialize sum squared */
/***************************/
   for (h=1; h<=p-1; h++) {
      sum[h+1]=temp[h]*temp[1];
```

Appendix (Cont.)

```
 save[h]=temp[h];
 }
 sum[1]=0;
/*******************/
/* rotate array */
/*******************/
 for (h=p; h>1; h--) temp[h]=temp[h-1];
 temp[1]=0;
/***************************/
/* compute partial sums */
/***************************/
compute square of Gaussian sum
gauss2.htm[11/16/2021 10:18:21 AM]
 for (h=1; h<=p-2; h++) {
 j=temp[p];
 for (i=p; i>1; i--) {
 temp[i]=temp[i-1];
 }
 temp[1]=j;
 for (i=1; i<=p; i++) {
 sum[i]=sum[i]+temp[i]*save[h+1];
    }
 }
/*********************************/
/* write square of Gaussian sum */
/*********************************/
 fprintf(Outfp," p=%d r=%d sum=%d \n",p,r,sum[1]);
 printf(" p=%d r=%d sum=%d \n",p,r,sum[1]);
   for (i=2; i<p; i++) {
    if (sum[i]!=sum[1]) {
 fprintf(Outfp,"error \n");
 printf("error \n");
  goto bskip;
   }
 }
 if (((sum[1]-sum[p])!=p)&&((sum[p]-sum[1])!=p)) {
 fprintf(Outfp,"error \n");
 printf("error \n");
  goto bskip;
 }
 if ((p-1)==((p-1)/4)*4) {
 if (sum[1]!=-1) {
 fprintf(Outfp,"error \n");
 printf("error \n");
```

Appendix (Cont.)

```
 goto bskip;
   }
 }
 else {
 if (sum[1]!=1) {
 fprintf(Outfp,"error \n");
 printf("error \n");
 goto bskip;
  }
 }
 }
bskip:
fclose(Outfp);
return(0);
}
compute cube of Gaussian sum
gauss3.htm[11/16/2021 1:27:45 PM]
/*****************************************************************************/
/* */
/* COMPUTE CUBES OF GAUSSIAN SUMS */
/* 11/14/97 (dkc) */
/* */
/* This C program computes cubes of generalized Gaussian sums. */
/* */
/*****************************************************************************/
#include "input.h"
#include <stdio.h>
int main ()
{
/*****************************************************************************/
/* p is a prime, n is a divisor of p-1, and r is a primitive root of p */
/* the cyclotomic cosets are stored in c[n][(p-1)/n] */
/*****************************************************************************/
unsigned int n, p, r;
unsigned int c[3][1000]; // dimensions are [n][(p-1)/n]
unsigned int sum[3000][2],temp[3000][2],save[3000][2];
unsigned int k[3000];
unsigned int g, h, i, j, l, t, count;
int d, e;
FILE *Outfp;
Outfp = fopen("gauss3b.dat","w");
count=0;
n=3;
for (g=0; g<200; g++) {
```

Appendix (Cont.)

```
  p=input[2*g];
  r=input[2*g+1];
  if ((p-1)!=((p-1)/n)*n)
  continue;
  count+=1;
/*********************************************************************/
/* generate permutation of 1,2,3...,(p-1) (by Fermat's theorem) */
/*********************************************************************/
 k[0] = r;
 for (i=1; i<p-1; i++) {
 k[i] = k[i-1]*r - ((k[i-1]*r)/p)*p;
 }
 for (i=0; i<p-2; i++) {
  if (k[i] == 1) {
  fprintf(Outfp,"error: r is not a primitive root of p \n");
  goto bskip;
  }
 }
/*********************************************/
/* sort permutation into cyclotomic cosets */
/*********************************************/
 for (h=0; h<n; h++) {
  j=0;
 for (i=h; i<p-1; i+=n) {
  c[h][j] = k[i];
  j=j+1;
  }
 }
/*****************************/
/* compute Gaussian sum */
/*****************************/
 for (i=0; i<(p-1)/n; i++) {
  temp[c[0][i]][0]=1; // set to 1
  temp[c[0][i]][1]=0;
 }
 for (i=0; i<(p-1)/n; i++) { // set to rho
  temp[c[1][i]][0]=0;
  temp[c[1][i]][1]=1;
 }
 for (i=0; i<(p-1)/n; i++) {
  temp[c[2][i]][0]=-1; // set to rho**2
  temp[c[2][i]][1]=-1;
 }
 temp[0][0]=0;
```

Appendix (Cont.)

```
 temp[0][1]=0;
/************************************/
/* compute square of Gaussian sum */
/************************************/
/***************************/
/* initialize sum squared */
/***************************/
 for (h=1; h<=p-1; h++) {
 t=temp[1][1]*temp[h][1];
compute cube of Gaussian sum
gauss3.htm[11/16/2021 1:27:45 PM]
 sum[h+1][0]=temp[1][0]*temp[h][0]-t;
 sum[h+1][1]=temp[1][0]*temp[h][1]+temp[1][1]*temp[h][0]-t;
 save[h][0]=temp[h][0];
 save[h][1]=temp[h][1];
 }
 sum[1][0]=0;
 sum[1][1]=0;
/*******************/
/* rotate array */
/*******************/
 for (h=p; h>1; h--) {
  temp[h][0]=temp[h-1][0];
  temp[h][1]=temp[h-1][1];
 }
  temp[1][0]=0;
  temp[1][1]=0;
/***************************/
/* compute partial sums */
/***************************/
 for (h=1; h<=p-2; h++) {
  j=temp[p][0];
  l=temp[p][1];
  for (i=p; i>1; i--) {
  temp[i][0]=temp[i-1][0];
  temp[i][1]=temp[i-1][1];
 }
 temp[1][0]=j;
 temp[1][1]=l;
 for (i=1; i<=p; i++) {
  t=temp[i][1]*save[h+1][1];
  sum[i][0]+=temp[i][0]*save[h+1][0]-t;
  sum[i][1]+=temp[i][0]*save[h+1][1]+temp[i][1]*save[h+1][0]-t;
 }
```

Appendix (Cont.)

```
 }
/*****************************/
/* initialize sum cubed */
/*****************************/
 for (h=1; h<=p-1; h++) {
  temp[h+1][0]=0;
  temp[h+1][1]=0;
 }
  temp[1][0]=0;
  temp[1][1]=0;
/*****************************/
/* compute partial sums */
/*****************************/
 for (h=1; h<=p-1; h++) {
  j=sum[p][0];
  l=sum[p][1];
  for (i=p; i>1; i--) {
  sum[i][0]=sum[i-1][0];
  sum[i][1]=sum[i-1][1];
 }
 sum[1][0]=j;
 sum[1][1]=l;
 for (i=1; i<=p; i++) {
  t=sum[i][1]*save[h][1];
  temp[i][0]+=sum[i][0]*save[h][0]-t;
  temp[i][1]+=sum[i][0]*save[h][1]+sum[i][1]*save[h][0]-t;
  }
 }
/*******************************/
/* write cube of Gaussian sum */
/*******************************/
 fprintf(Outfp," %d, %d, %d, \n",p,temp[1][0],temp[1][1]);
 printf(" %d, %d, %d, \n",p,temp[1][0],temp[1][1]);
  d=(int)temp[1][0]-(int)temp[p][0];
  e=(int)p;
  if (d!=(d/e)*e) {
  fprintf(Outfp," error \n");
  printf(" error \n");
  goto bskip;
  }
 }
bskip:
fprintf(Outfp," count=%d \n",count);
printf(" count=%d \n",count);
```

Appendix (Cont.)

```
 fclose(Outfp);
 return(0);
}
```

Cite this article as: Darrell Cox, Sourangshu Ghosh and Eldar Sultanow (2022). Quadratic, Cubic, Biquadratic, and Quintic Reciprocity. *International Journal of Pure and Applied Mathematics Research*, 2(1), 15-39. doi: 10.51483/IJPAMR.2.1.2022.15-39.