Rational (!) Cubic and Biquadratic Reciprocity

Paul Pollack
2005 Ross Summer Mathematics Program

It is ordinary rational arithmetic which attracts the ordinary man . . .

G.H. Hardy, *An Introduction to the Theory of Numbers*, Bulletin of the AMS 35, 1929

Quadratic Reciprocity Law (Gauss). *If p and q are distinct odd primes, then*

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

We also have the **supplementary laws**:

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

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

These laws enable us to completely characterize the primes p for which a given prime q is a square.

Question: Can we characterize the primes p for which a given prime q is a cube? a fourth power?

We will focus on cubes in this talk.

QR in Action:

From the supplementary law we know that 2 is a square modulo an odd prime p if and only if $p \equiv \pm 1 \pmod 8$.

Or take $q = 11$. We have $\left(\frac{11}{p}\right) = \left(\frac{p}{11}\right)$ for $p \equiv 1 \pmod 4$, and $\left(\frac{11}{p}\right) = -\left(\frac{p}{11}\right)$ for $p \not\equiv 1 \pmod 4$.

So solve the system of congruences

$$p \equiv 1 \pmod 4, p \equiv \blacksquare \pmod{11}.$$

OR

$$p \equiv -1 \pmod 4, p \not\equiv \blacksquare \pmod{11}.$$

Computing which nonzero elements mod p are squares and nonsquares, we find that 11 is a square modulo a prime $p \neq 2, 11$ if and only if $p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \pmod{44}$.

Observe that the p with $\left(\frac{q}{p}\right) = 1$ are exactly the primes in certain arithmetic progressions.

Cubic Reciprocity: Preliminaries.

Question: Fix a prime q. For which primes p is a q a cube modulo p?

Observation: if $p \equiv 2 \pmod 3$, then *every element* of $\mathbf{Z}/p\mathbf{Z}$ is a cube. Proof: Write $p = 3k + 2$.

Then if a is any integer,

$$\begin{aligned}(a^{2k+1})^3 &= a^{6k+3} \\ &= a^{3k+2}a^{3k+1} \\ &= a^p a^{p-1} = a,\end{aligned}$$

so we have written down a cube root of a.

So only consider primes $p \equiv 1 \pmod 3$.

Experimental Mathematics: the case $q = 2$

For which primes $p \equiv 1 \pmod 3$ is 2 a cube? `MAPLE` makes experimentation easy:

31, 43, 109, 127, 157, 223, 229, 277, 283, 307, 397, 433, 439, 457, 499, 601, 643, 691, 727, 733, 739, 811, 919, 997, 1021, 1051, 1069, 1093, 1327, 1399, 1423, 1459, 1471, 1579, 1597, 1627, 1657, 1699, 1723, 1753, 1777, 1789, 1801, 1831, 1933, 1999, 2017, 2089, 2113, 2143, 2179, 2203, 2251, 2281, 2287, 2341, 2347, 2383, 2671, 2689, 2731, 2749, 2767, 2791

List of the primes for which 2 **is a cube among the first two-hundred primes congruent to** $1 \pmod 3$

p	p mod 16	p mod 9	p mod 5	p mod 7
31	15	4	1	3
43	11	7	3	1
109	13	1	4	4
127	15	1	2	1
157	13	4	2	3
223	15	7	3	6
229	5	4	4	5
277	5	7	2	4
283	11	4	3	3
307	3	1	2	6
397	13	1	2	5
433	1	1	3	6
439	7	7	4	5
457	9	7	2	2
499	3	4	4	2
601	9	7	1	6
643	3	4	3	6
691	3	7	1	5
727	7	7	2	6
733	13	4	3	5
739	3	1	4	4
811	11	1	1	6
919	7	1	4	2
997	5	7	2	3
1021	13	4	1	6
1051	11	7	1	1
1069	13	7	4	5
1093	5	4	3	1
1327	15	4	2	4
1399	7	4	4	6

Using algebraic number theory, one can prove:

Theorem. *Congruences on p give you no useful information.*

More precisely, let m be any positive integer. Let $a \pmod{m}$ be an invertible residue class containing an integer congruent to $1 \pmod{3}$. Then there are infinitely many primes p with

$$p \equiv 1 \pmod{3} \text{ and } p \equiv a \pmod{m}$$

for which 2 is a cube, and infinitely many such p for which 2 is not a cube.

So congruences do not suffice. Or do they?

Congruences on p do not suffice . . . but we don't have to look only at p.

Theorem. *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 proof uses the arithmetic of the ring $\mathbf{Z}[(1+\sqrt{-3})/2]$.

Examples:

$$4 \cdot 31 = 124 = 4^2 + 27 \cdot 2^2,$$

$$4 \cdot 61 = 244 = 1^2 + 27 \cdot 3^2,$$

so we can choose $L = \pm 4$ and $M = \pm 2$ in the first case, and $L = \pm 1, M = \pm 3$ in the second.

We will normalize our choice by requiring that

L and M are positive.

$p \equiv 1 \pmod{3}$	L	M	2 **a cube?**
7	1	1	no
13	5	1	no
19	7	1	no
31	4	2	YES
37	11	1	no
43	8	2	YES
61	1	3	no
67	5	3	no
73	7	3	no
79	17	1	no
97	19	1	no
103	13	3	no
109	2	4	YES
127	20	2	YES
139	23	1	no
151	19	3	no
157	14	4	YES
163	25	1	no
181	7	5	no
193	23	3	no
199	11	5	no
211	13	5	no
223	28	2	YES

Conjecture. *Let* $p > 3$ *be a prime. Then* 2 *is a cube modulo* p *if and only if* L *or* M *is divisible by* 2*.*

An equivalent formulation: 2 is a cube modulo the prime $p \equiv 1 \pmod 3$ if and only if

$$p = L'^2 + 27M'^2$$

for some integers L' and M'.

$\mathbf{p \equiv 1 \pmod{3}}$	$\mathbf{L}$	$\mathbf{M}$	3 **a cube?**
7	1	1	no
13	5	1	no
19	7	1	no
31	4	2	no
37	11	1	no
43	8	2	no
61	1	3	YES
67	5	3	YES
73	7	3	YES
79	17	1	no
97	19	1	no
103	13	3	YES
109	2	4	no
127	20	2	no
139	23	1	no
151	19	3	YES
157	14	4	no
163	25	1	no
181	7	5	no
193	23	3	YES
199	11	5	no
211	13	5	no
223	28	2	no

$\mathbf{p \equiv 1 \pmod{3}}$	**L**	**M**	3 **a cube?**
10009	182	16	no
10039	148	26	no
10069	199	5	no
10093	175	19	no
10099	133	29	no
10111	59	37	no
10141	181	17	no
10159	188	14	no
10177	145	27	YES
10243	200	6	YES
10267	1	39	YES
10273	5	39	YES
10303	100	34	no
10321	109	33	YES
10333	142	28	no
10357	19	39	YES
10369	137	29	no
10399	23	39	YES
10429	82	26	no
10453	193	13	no
10459	173	21	YES
10477	29	39	YES
10501	71	37	no

$\mathbf{p \equiv 1}$ (mod $\mathbf{3}$)	$\mathbf{L}$	$\mathbf{M}$	5 **a cube?**
7	1	1	no
13	5	1	YES
19	7	1	no
31	4	2	no
37	11	1	no
43	8	2	no
61	1	3	no
67	5	3	YES
73	7	3	no
79	17	1	no
97	19	1	no
103	13	3	no
109	2	4	no
127	20	2	YES
139	23	1	no
151	19	3	no
157	14	4	no
163	25	1	YES
181	7	5	YES
193	23	3	no
199	11	5	YES
211	13	5	YES
223	28	2	no

$\mathbf{p} \equiv \mathbf{1} \pmod{\mathbf{3}}$	$\mathbf{L}$	$\mathbf{M}$	7 **a cube?**
7	1	1	—
13	5	1	no
19	7	1	YES
31	4	2	no
37	11	1	no
43	8	2	no
61	1	3	no
67	5	3	no
73	7	3	YES
79	17	1	no
97	19	1	no
103	13	3	no
109	2	4	no
127	20	2	no
139	23	1	no
151	19	3	no
157	14	4	YES
163	25	1	no
181	7	5	YES
193	23	3	no
199	11	5	no
211	13	5	no
223	28	2	YES

$\mathbf{p} \equiv \mathbf{1} \pmod{\mathbf{3}}$	$\mathbf{L}$	$\mathbf{M}$	7 **a cube?**
10009	182	16	YES
10039	148	26	no
10069	199	5	no
10093	175	19	YES
10099	133	29	YES
10111	59	37	no
10141	181	17	no
10159	188	14	YES
10177	145	27	no
10243	200	6	no
10267	1	39	no
10273	5	39	no
10303	100	34	no
10321	109	33	no
10333	142	28	YES
10357	19	39	no
10369	137	29	no
10399	23	39	no
10429	82	26	no
10453	193	13	no
10459	173	21	YES
10477	29	39	no
10501	71	37	no

Conjectures: Let $p \equiv 1 \pmod 3$ and write $4p = L^2 + 27M^2$, where $L, M > 0$. Then

3 is a cube $\Leftrightarrow 3 \mid M$,

5 is a cube $\Leftrightarrow 5 \mid L$ or $5 \mid M$,

7 is a cube $\Leftrightarrow 7 \mid L$ or $7 \mid M$.

(???) Perhaps (???)

$$q \text{ is a cube } \iff q \mid L \text{ or } q \mid M.$$

(This agrees with our conjectures even for $q = 2$ and $q = 3$, since $4p = L^2 + 27M^2$.)

$\mathbf{p \equiv 1}$ (mod $\mathbf{3}$)	$\mathbf{L}$	$\mathbf{M}$	11 **a cube?**
100003	337	103	no
100057	175	117	no
100069	458	84	no
100129	562	56	no
100153	443	87	no
100183	383	97	no
100189	209	115	YES
100207	421	91	no
100213	575	51	no
100237	194	116	no
100267	224	114	no
100279	137	119	no
100291	491	77	YES
100297	250	112	YES
100333	515	71	YES
100357	631	11	YES
100363	355	101	YES
100393	593	43	no
100411	179	117	no
100417	139	119	no
100447	404	94	no
100459	263	111	no
100483	8	122	no

$\mathbf{p \equiv 1 \pmod{3}}$	$\mathbf{L}$	$\mathbf{M}$	**11=cube?**	$\frac{\mathbf{L}}{\mathbf{3M}}$ mod **11**
100003	337	103	no	-4
100057	175	117	no	1
100069	458	84	no	4
100129	562	56	no	4
100153	443	87	no	-1
100183	383	97	no	4
100189	209	115	YES	0
100207	421	91	no	4
100213	575	51	no	-3
100237	194	116	no	1
100267	224	114	no	4
100279	137	119	no	1
100291	491	77	YES	∞
100297	250	112	YES	5
100333	515	71	YES	5
100357	631	11	YES	∞
100363	355	101	YES	-5
100393	593	43	no	4
100411	179	117	no	-3
100417	139	119	no	-3
100447	404	94	no	-2
100459	263	111	no	-4
100483	8	122	no	-1

Table of primes $p \equiv 1 \pmod 3$ **together with** L, M **and the ratio** $\frac{L}{3M}$ mod 11.

$\mathbf{p} \equiv \mathbf{1} \pmod{\mathbf{3}}$	$\mathbf{L}$	$\mathbf{M}$	11=cube?	$\frac{\mathbf{L}}{\mathbf{3M}}$ mod **11**
100501	323	105	no	-1
100519	523	69	no	-3
100537	305	107	no	4
100549	83	121	YES	∞
100591	181	117	YES	-5
100609	622	24	no	1
100621	574	52	no	1
100669	626	20	no	2
100693	475	81	no	2
100699	143	119	YES	0
100741	509	73	no	-3
100747	605	73	YES	0
100801	254	112	no	2
100927	380	98	no	-2
100957	185	117	no	2
100981	457	85	no	3
100987	595	43	no	-4
100999	452	86	no	-2
101089	542	64	YES	5
101107	560	58	YES	-5
101113	442	88	YES	∞
101119	401	95	YES	-5
101149	539	65	YES	0

(continuation): table of primes $p \equiv 1 \pmod 3$ **together with** L, M **and the ratio** $\frac{L}{3M}$ mod 11.

Conjecture. *Let* $p \equiv 1 \pmod 3$, *and write* $4p = L^2 + 27M^2$ *with* L *and* M *positive. Then* 11 *is a cube mod* p *if and only if*

$$\frac{L}{3M} \pmod{11} = 0, -5, 5 \text{ or } \infty,$$

where we say $\frac{L}{3M} = \infty$ *if* $11 \mid M$.

This implies that if 11 divides L or 11 divides M, then 11 is a cube modulo p (since then $\frac{L}{3M} = 0$ or ∞), but this is no longer necessary.

$\mathbf{p \equiv 1 \pmod{3}}$	$\mathbf{L}$	$\mathbf{M}$	13=**cube?**	$\frac{\mathbf{L}}{\mathbf{3M}}$ mod $\mathbf{13}$
100003	337	103	YES	-4
100057	175	117	YES	∞
100069	458	84	no	-2
100129	562	56	no	-3
100153	443	87	no	1
100183	383	97	YES	-4
100189	209	115	no	2
100207	421	91	YES	∞
100213	575	51	no	-1
100237	194	116	YES	-4
100267	224	114	YES	4
100279	137	119	no	-1
100291	491	77	no	1
100297	250	112	no	5
100333	515	71	no	-1
100357	631	11	no	1
100363	355	101	no	1
100393	593	43	no	5
100411	179	117	YES	∞
100417	139	119	no	-5
100447	404	94	no	3
100459	263	111	no	2
100483	8	122	YES	4

Table of primes $p \equiv 1 \pmod 3$ **together with** L, M **and the ratio** $\frac{L}{3M}$ mod 13.

$\mathbf{p \equiv 1 \pmod 3}$	$\mathbf{L}$	$\mathbf{M}$	13=cube?	$\frac{\mathbf{L}}{\mathbf{3M}}$ mod $\mathbf{13}$
100501	323	105	no	-5
100519	523	69	no	-3
100537	305	107	no	5
100549	83	121	no	-5
100591	181	117	YES	∞
100609	622	24	YES	-4
100621	574	52	YES	∞
100669	626	20	no	-3
100693	475	81	no	-5
100699	143	119	YES	0
100741	509	73	no	-1
100747	605	73	no	1
100801	254	112	no	3
100927	380	98	no	2
100957	185	117	YES	∞
100981	457	85	no	-3
100987	595	43	no	3
100999	452	86	no	-5
101089	542	64	no	-3
101107	560	58	no	-5
101113	442	88	YES	0
101119	401	95	no	2
101149	539	65	YES	∞

(continuation): table of primes $p \equiv 1 \pmod 3$ **together with** L, M **and the ratio** $\frac{L}{3M}$ mod 13.

Conjecture. *Let* $p \neq 13$ *be a prime congruent to* $1 \pmod 3$*, and write* $4p = L^2 + 27M^2$ *with* L *and* M *positive. Then* 13 *is a cube mod* p *if and only if*

$$\frac{L}{3M} \pmod{13} = 0, -4, 4 \text{ or } \infty,$$

where we say $\frac{L}{3M} = \infty$ *if* $13 \mid M$*.*

The Claims of Jacobi. Our conjectures can already be found in the work of Jacobi (1827); conjectures for $2, 3, 5$ and 6 can even be found in posthumously published work of L. Euler.

Jacobi gives the following table:

q	classes of $\frac{L}{3M} \pmod q$	# of classes
5	$0, \infty$	2
7	$0, \infty$	2
11	$0, \pm 5, \infty$	4
13	$0, \pm 4, \infty$	4
17	$0, \pm 1, \pm 3, \infty$	6
19	$0, \pm 1, \pm 3, \infty$	6
23	$0, \pm 4, \pm 5, \pm 7, \infty$	8
29	$0, \pm 3, \pm 6, \pm 10, \pm 14, \infty$	10
31	$0, \pm 2, \pm 13, \pm 14, \pm 23, \infty$	10
37	$0, \pm 1, \pm 3, \pm 4, \pm 10, \pm 15, \infty$	12

Example: $4 \cdot 219889 = 434^2 + 27 \cdot 160^2$, and $434/27 \equiv 10 \pmod{37}$, and $149146^3 \equiv 37 \pmod{219889}$.

Jacobi claimed proofs (using Jacobi sums – see Ireland & Rosen) but he never published them.

In our examples that there are $(q-1)/3$ classes if $q \equiv 1 \pmod 3$ and $(q+1)/3$ classes otherwise.

We can write this in a unified way as

$$\frac{1}{3}\left(q - \left(\frac{-3}{q}\right)\right),$$

since

$$\left(\frac{-3}{q}\right) = \begin{cases} +1 & \text{if } q \equiv 1 \pmod 3, \\ -1 & \text{if } q \equiv -1 \pmod 3, \end{cases}.$$

A Revised Conjecture. *Let $q > 3$ be prime. Then there is a set S of $\frac{1}{3}(q - \left(\frac{-3}{q}\right))$ elements of $\mathbf{Z}/q\mathbf{Z} \cup \{\infty\}$, 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*

$$q \text{ is a cube mod } p \Longleftrightarrow \frac{L}{3M} \pmod q \in S.$$

Also $-S = S$ with obvious conventions.

Notice the resemblance to QR.

Theorem (Jacobi (?))**.** *This is true!*

But what is S? Jacobi found one answer. . .

Digression: A Special Family of Groups.

Let $q > 3$ be prime. We will define a group structure on a certain subset of $\mathbf{Z}/q\mathbf{Z} \cup \{\infty\}$.

First we need a set. Take $\mathbf{Z}/q\mathbf{Z} \cup \{\infty\}$ and remove any square roots of -3; let $G(q)$ be the resulting set.

For example,

$$G(5) = \{0, 1, 2, 3, 4\} \cup \{\infty\},$$

$$G(7) = \{0, 1, 3, 4, 6\} \cup \{\infty\},$$

$$G(11) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \cup \{\infty\}.$$

In general we have $\#G = q - \left(\frac{-3}{q}\right)$.

Next we need a binary operation. For x and y residue classes mod q contained in G, we define

$$x \star y = \frac{xy - 3}{x + y},$$

the computation taking place in $\mathbf{Z}/q\mathbf{Z}$. If the denominator but not the numerator vanishes, call the result ∞. We also define

$$x \star \infty = \infty \star x = x, \text{ and } \infty \star \infty = \infty.$$

Note that we needed to remove $\sqrt{-3}$ to define this: else what is $(\sqrt{-3}) \star (-\sqrt{-3})$?

This operation is clearly commutative.
Have an identity element: ∞,
The inverse of x: $-x$ (and inverse of ∞ is ∞).

Also $\star$ is associative by direct check (or cleverness)! So $\star$ makes G into a (finite) commutative group!

Now we need some theorems!

Arithmetic in G.

A concrete example: Take $q = 7$; then $G(7) = \{0, 1, 3, 4, 6\} \cup \{\infty\}$. We can compute

$$3 \star 6 = \frac{3 \cdot 6 - 3}{3 + 6} = \frac{15}{9} = \frac{8}{2} = 4,$$

since the computation takes place in $\mathbf{Z}/7\mathbf{Z}$.

A more abstract example: Let $q > 3$ be prime. Then 1 is always an element of $G(q)$, because 1 is never a square root of -3 in the ring $\mathbf{Z}/q\mathbf{Z}$. We have

$$1 \star 1 = \frac{1 \cdot 1 - 3}{1 + 1} = \frac{-2}{2} = -1$$

and hence

$$1 \star 1 \star 1 = 1 \star -1 = \infty.$$

So 1 is an element of order 3.

Consequence: $3 \mid q - \left(\frac{-3}{q}\right)$. This gives another determination of when -3 is a square!

The Structure of G

Theorem. *G is a cyclic group.*

The proof is similar to the proof U_p is cyclic: it suffices to check that for every n, there are at most n elements g of G for which

$$\underbrace{g \star g \star g \star \cdots \star g}_{n \text{ times}} = \infty \quad \text{(the identity)}.$$

Example: if $n = 4$, then $g = \infty$ satisfies this equation, and otherwise g is an element of $\mathbf{Z}/q\mathbf{Z}$ and we have

$$g \star g \star g \star g = \frac{g^4 - 18g^2 + 9}{4g^3 - 12g};$$

this is equal to ∞ if and only if the denominator vanishes, which happens for at most three values of g. So altogether there are at most 4 such g satisfying the equation.

Same proof works for general n! (Due to D. Harden.)

The Subgroup of Cubes

Corollary. *The group G has a unique cyclic subgroup of order*

$$\frac{\#G}{3} = \frac{1}{3}\left(q - \left(\frac{-3}{q}\right)\right);$$

it just the subgroup of "cubes" $g \star g \star g$ with $g \in G$.

Example: $q = 5$. Then $G(5)$ is a six-element group $\{0, 1, 2, 3, 4\} \cup \{\infty\}$. We compute

$$0 \star 0 \star 0 = 0 \star \infty = 0.$$

Since the subgroup of "cubes" has 2 elements and includes $\infty \star \infty \star \infty = \infty$, we've found them all: $\{0, \infty\}$.

In fact, $0 \star 0 \star 0 = 0$ in every group $G(q)$. So the subgroup of cubes always contains $\{0, \infty\}$.

If $q = 7$, there are $\frac{1}{3}(7 - \left(\frac{-3}{7}\right)) = 2$ cubes, so again $\{0, \infty\}$ are all of them.

Further Examples

$q = 11$: $2\star 2\star 2 = 5$, and $(-2)\star(-2)\star(-2) = -5$.

$q = 13$: $2\star 2\star 2 = 4$, and $(-2)\star(-2)\star(-2) = -4$.

In both cases the formula $\frac{1}{3}(q - \left(\frac{-3}{q}\right))$ leads us to expect four cubes, so we have found them all: for $q = 11$, they are $\{0, \pm 5, \infty\}$ and for $q = 13$ they are $\{0, \pm 4, \infty\}$. Note that generally

$$g \star g \star g = -(-g) \star (-g) \star (-g),$$

so that the set of cubes S' always satisfies $S' = -S'$.

One last example:

$$q = 17: \quad 2 \star 2 \star 2 = 3, \quad 4 \star 4 \star 4 = 1.$$

We expect six cubes in $G(17)$, and now we've found them: $0, \pm 1, \pm 3, \infty$.

By now you can guess what's coming...

Jacobi-Z.-H. Sun Rational Cubic Reciprocity Law (1998). *Let $q > 3$ be prime. If $p \neq q$ is a prime congruent to* $1 \pmod 3$*, where* $4p = L^2 + 27M^2$ *with positive integers L and M, then*

$$q \text{ is a cube modulo p} \Leftrightarrow \frac{L}{3M} \text{ is a cube in } G.$$

Sun proves a more general result: if you normalize L and M differently, than the coset of the subgroup of cubes that $\frac{L}{3M}$ lies in corresponds to the coset of the subgroup of cubes that q lies in modulo p. This relies on the full cubic reciprocity law.

Rational Biquadratic Reciprocity at a Glance

Let p and q be distinct odd primes, and define $q^* := (-1)^{(q-1)/2}q$.

QR says exactly that

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right).$$

Z.-H. Sun's Rational Quartic Reciprocity Law (2001). *Let p and q be distinct odd primes. Suppose that $p \equiv 1 \pmod 4$, and write $p = a^2 + b^2$, with b even. Then*

$$q^* \text{ is a fourth power mod } p \Leftrightarrow \\ \frac{a}{b} \text{ is a fourth power in } H.$$

The Group H.

In Sun's quartic law, the group $H = H(q)$ is defined similarly to $G = G(q)$: we adjoin ∞ to $\mathbf{Z}/q\mathbf{Z}$, throw out square roots of -1 if they exist, and multiply according to the rule

$$x \star y = \frac{xy - 1}{x + y},$$

with the same conventions as before if x or y is ∞.

H is cyclic of order $q - \left(\frac{-1}{q}\right)$, the element 1 has order 4.

A Historical Analogy:
Cubic Law: Jacobi :: Quartic Law : Dirichlet

Proofs?

Quartic Law: Easier. Key ideas due to Dirichlet; see Venkov.

Needs only quadratic reciprocity plus a theorem of Legendre. But "a shrewd masterpiece" (Jacobi).

Legendre's theorem asserts that an equation

$$ax^2 + by^2 + cz^2 = 0$$

has solutions in nonzero integers x, y and z as long as there are no obvious conditions on a, b and c ruling this out. (Sign conditions, quadratic residue conditions.) For example, Legendre's theorem will tell you that

$$x^2 + y^2 = 3z^2 \quad \text{or} \quad 13x^2 + y^2 = -10z^2$$

has no solutions in nonzero integers x, y and z, while

$$x^2 + y^2 = 2z^2$$

does.

Proofs?

Cubic Law: Technical. Very inadequate sketch:

We first restate QR. Let p be an odd prime. Define $p^* := (-1)^{(p-1)/2}p$. (This replaces p by $\pm p$ to make it 1 (mod 4).) Then QR is equivalent to the assertion that

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

if q is an odd prime distinct from p.

A further restatement: Let p be an odd prime. Then the odd prime $q \neq p$ is a square mod p if and only the polynomial

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

has a root modulo q.

Note: discriminant $= p^*$.

This quadratic polynomial is the first in a family of so-called "period polynomials" investigated by Gauss – they all have analogous properties.

Suppose $p \equiv 1 \pmod{3}$. The "reduced period polynomial" of degree 3 corresponding to p is

$$x^3 - 3px - pL,$$

where $4p = L^2 + 27M^2$ and $L \equiv 1 \pmod{3}$. (See *Disquisitiones* §358 for an early appearance of this polynomial.)

Theorem (Kummer). *Let $q > 3$ be a prime distinct from p. Then q is a cube modulo p if and only the reduced period polynomial has a root modulo q.*

The conditions for this polynomial to have a root can be analyzed using Cardano's formula and arithmetic in finite fields.

Suggested Reading and Bibliography:

Dirichlet, P.G.L. **Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré**. J. Reine Angew. Math. 3. 1828. 35-69.

Ireland, Kenneth; Rosen, Michael. *A classical introduction to modern number theory*. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

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

Lemmermeyer, Franz. *Reciprocity laws. From Euler to Eisenstein*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

Sun, Zhi-Hong. **On the theory of cubic residues and nonresidues**. Acta Arith. 84 (1998), no. 4, 291–335.

Sun, Zhi-Hong. **Supplements to the theory of quartic residues**. Acta Arith. 97 (2001), no. 4, 361–377.

Venkov, B. A. *Elementary number theory*. Translated from the Russian and edited by Helen Alderson. Wolters-Noordhoff Publishing, Groningen 1970.