Quadratic Reciprocity

March 7, 2008

Gauss lied, almost

Gauss provides a proof of Quadratic Reciprocity in his *Disquisitiones Arithmeticae* — actually, he provides two. As he points out, this was the first time that any proof at all had been stated publicly. The nature of mathematical proof is somewhat mystified today, not in small thanks to how Gauss set forth his proofs. The *way* Gauss discovered those principles that he published in all his public works, is not the same as *how* he explained them. He was quite concerned with 1) not revealing his true, Keplerian method of scientific work, and 2) ensuring that what he did discover was rendered bulletproof against all possible slings and arrows thrown from a British Fascist dominated scientific community. It was politically dangerous to announce radical breakthroughs in science, whose discovery necessitated methods that differed from the pure empiricism of Euler, Lagrange, and Laplace. Therefore, Gauss's only defense, since he could not keep all of his discoveries secret without going nuts, was to present them as results of mathematically logical proofs.

A proof is not a discovery. Also, a proof is not *proof* that the discovery made is actually a true, valid principle that is efficient in the Creator's universe. The method of discovery, itself, is proof, which includes reference to an experiment whose success depends on the existence of that principle of the universe. What Gauss presented to his scientific audience, was thus a smokescreen, which, more often than not, did not include either the crucial experiment, or the description of how Gauss came to discover that, for which he was presenting proof. For example, Gauss recognized the validity of the principle of Quadratic Reciprocity before he completed his first proof in 1796. His proof does not resemble how he discovered that it was valid. This is also true for his next 7 proofs of the same theorem! He says as much in his introduction to his third proof:

> The questions of higher arithmetic often present a remarkable characteristic which seldom appears in more general analysis, and increases the beauty of the former subject. While analytic investigations lead to the discovery of new truths only after the fundamental principles of the subject (which to a certain degree

> open the way to these truths) have been completely mastered; on the contrary in arithmetic the most elegant theorems frequently arise experimentally as the result of a more or less unexpected stroke of good fortune, while their proofs lie so deeply embedded in the darkness that they elude all attempts and defeat the sharpest inquiries...
>
> The theorem which we have called in sec. 4 of the *Disquisitiones Arithmeticae*, the *Fundamental Theorem*, because it contains in itself all the theory of quadratic residues, holds a prominent position among the questions of which we have spoken...I discovered this theorem independently in 1795 at a time when I was totally ignorant of what had been achieved in higher arithmetic, and consequently had not the slightest aid from the literature on the subject. For a whole year this theorem tormented me and absorbed my greatest efforts until at last I obtained a proof given in the fourth section of the above-mentioned work.

With Gauss's method of providing proofs, instead of descriptions of his method, a true scientist has to flank the problem. It is necessary to understand how Gauss thought, in order to not only gain insight into the work of Riemann, Einstein, Vernadsky, and LaRouche, but also to gain insight into how a truly creative mind functions. That understanding cannot come from memorizing proofs. We will thus avoid Gauss's proofs (until the end), and instead investigate what exactly Quadratic Reciprocity is. Let us begin by looking at one man who missed its importance: that turncoat, Leonhard Euler.

Leonhard "Turncoat" Euler

Euler (1707-1783) began his life in the most hopeful of circumstances — as the star student of Gottfried Leibniz's closest collaborator, Johann Bernoulli. His earliest scientific paper was on the construction of isochronous curves in a resistant medium, and he went on to develop Leibniz's study of differential and integral calculus. At about 1740, it became clear that this young, seeming champion of Leibniz's ideas, had gone over the edge. Euler moved from his post at Leibniz's St. Petersburg Academy to Leibniz's Berlin Academy, to help initiate the wrecking of the legacy of science in Europe left by Leibniz.[1] Euler thence participated in taking Leibniz's beautiful ideas, one by one, and degrading their meaning.

Though Euler became such a despicable turncoat, he produced an enormous volume of writings. While reading through them, if observant, the reader will get the sense that Euler was becoming frustrated with the concept of Man's ability to discover the mind of the Creator. He got to the verge of making serious, important breakthroughs repeatedly,

[1] See David Shavin's article, etc.

but then always pulled back. Therefore, if his later work had not existed, it would not have hindered the progress of science much.

This is nowhere more clear than in the writings of Gauss on arithmetic. Gauss takes pains to reference which of the proofs in his *Disquisitiones Arithmeticae* were due first to Euler, as also to Fermat, Lambert, Lagrange, and Legendre. But, Gauss says in the introduction of that work, that

> ... [A]s one result led to another I had completed most of what is presented in the first four sections of this work before I came into contact with similar works of other geometers. ...
>
> After a while I began to consider publishing the fruits of my investigations. And I allowed myself to be persuaded not to omit any of the early results, because at that time there was no book that brought together the works of the other geometers, scattered as they were among Commentaries of learned Academies.

This type of situation recurred throughout the works of Gauss: Gauss made major, independent breakthroughs through some "natural" method, which he never revealed, and then found that Euler had done all the mathematics necessary to come just short of those breakthroughs. Of course, the mathematics must not be mistaken for the actual discovery. Mathematical derivation, such as is found all over Euler's works, is not how a creative mind makes discoveries. Logical derivation in mathematics can be used to *disprove* discoveries, but it does not prove the validity of any discovery. Gauss's method was, first, to make the discovery, and then to write down a bunch of mathematical derivations that would appear to corroborate the discovery. Euler was just the opposite, and spent his time doing mathematical derivations, hoping that the mind of the creator would be revealed to him through that arduous task. He went blind in at least one eye while doing these types of calculations.

Gauss references just exactly this problem, after he presents the first proof ever of the fundamental theorem of modular arithmetic, the Law of Quadratic Reciprocity

> The fundamental theorem must certainly be regarded as one of the most elegant of its type. No one has thus far presented it in as simple a form as we have done above. This is even more surprising since Euler already knew other propositions which depend on it and from which it can easily be recovered... [A]ll his attempts at demonstration were in vain, and he succeeded only in giving a greater degree of verisimilitude to the truth that he had discovered by induction.[2]

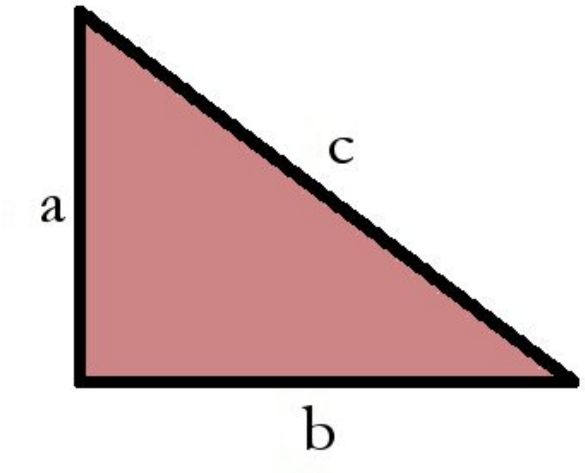
Gauss then gives several examples of Euler's work in this direction, and then the futile attempts of Euler's follower, Napoleon Bonaparte's "Great Volcano of the Mathematical Sciences," Joseph Louis Lagrange.

[2] *Disquisitiones Arithmeticae* §151

Let us look deep into the history of arithmetic, to see what it really means to make a discovery, rather than play with your mathematicals.

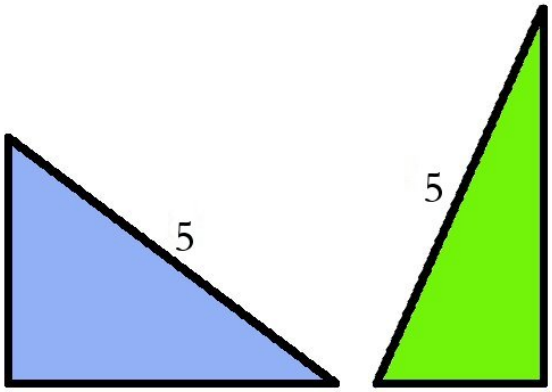
Pythagorean Arithmetic

Everybody learns the Pythagorean Theorem in school: $a^2 + b^2 = c^2$, where c is the length of the hypotenuse of a triangle whose other sides, a and b, meet at a right angle.



Given a triangle and two of the sides, the student is saddled with the problem of calculating the length of the other side using this formula. What gets passed over, is a more profound insight into the nature of space, which Pythagoras' discovery points at.

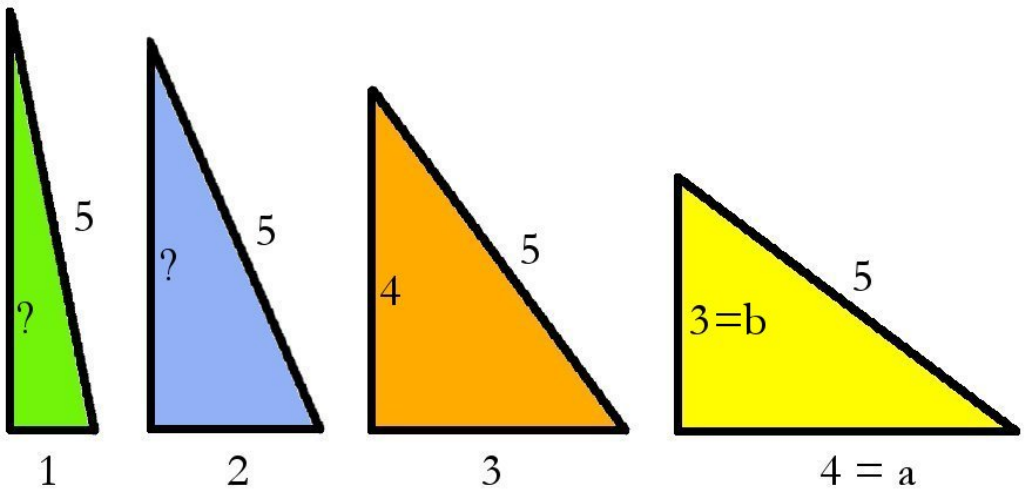
Draw a right triangle with a hypotenuse of length 5 cm. Now, draw a different right



triangle, but with the same hypotenuse. How are the lengths of the sides of the two triangles related? Draw yet another right triangle with that same hypotenuse. What we see is, that the lengths of either of the two "legs" is bounded by the length of the hypotenuse. So, if one of the lengths of the legs is very close to the length of the hypotenuse, the other leg will be very, very short, and vice versa. This can be illustrated by using a circle.

[ANIMATION: ROTATING RADIUS OF CIRCLE, WITH SINE AND COSINE]

We see that the hypotenuse is actually that which connects the center to the circumference of the circle, and the two other legs are just the distances of the end of the hypotenuse from horizontal and vertical lines drawn through the center. The lengths of these sides, the *sine* and *cosine*, continuously proceed through every possible length between 0 and 5 cm. Now, draw four other triangles with hypotenuse 5 cm, with one leg being successively 1 cm, 2 cm, 3 cm, 4 cm. We will call that leg a.



For the first one, where $a = 1$ cm, how long is the other leg (which we will call b)? It's obviously less than 5. To use our trusty old Pythagorean Theorem (which we have all proved, right?), we must find some number whose square, when added to $1^2 = 1$ is equal to $5^2 = 25$. In other words, $25 - 1 = 24$ is the square of the length of that side. Now, we break out our trusty old calculator and calculate $\sqrt{24}$, which is approximately 4.8989795... (of course, Pythagoras couldn't do it like this, but that's OK).

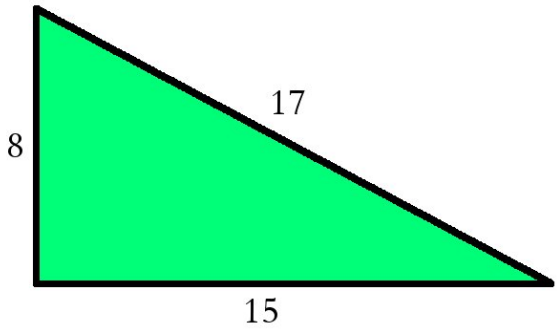
What is the length of b when $a = 2$? The square of b will have to be $25 - 4 = 21$, or approximately $b = 4.5825757\ldots$. Depending on what kind of digital calculating device you're using, you will get more or less numbers after the decimal point, since they will keep going as long as you care to calculate them.[3] Are we to assume, now, that one of the legs will *always* be one of these infinite decimals? Let's try one more, $a = 3$. Ah! Now, we get

[3]In other words, the more digits your computer can count up to, the longer the hypotenuse will get!

$25 - 9 = 16$, which is a square number. This triangle is what we will call the 3-4-5 triangle.

Since the legs of the right triangle with hypotenuse 5 can be any length between 0 and 5, the 3-4-5 triangle is really a special case within a *continuum* of possibilities. We have selected one instant out of a continuous change, represented by the circle animation above. In this sense, the length 5 has a special property. The reader will find that, not all whole number hypotenuses are capable of being in a right triangle with two legs of whole number lengths.

These special cases have since been called *Pythagorean Triples*, because of the emphasis Pythagoras, himself, placed on them. How many sets of Pythagorean Triples are there? There is the 3-4-5 triangle, and all of its multiples, such as the 6-8-10 triangle. But, these triangles are all similar to each other. Another Pythagorean Triple is the triangle with legs 8, 15, and hypotenuse 17. Those whole numbers that can be the hypotenuse of a



Pythagorean Triple thus separate themselves from the rest of the counting numbers by this property, which is related to the *transcendental* difference between the circle and the straight line.[4]

Since not all whole numbers will fit together into a Pythagorean Triple, can we find some method of locating any of the particular sets we wish? This is the type of problem that Gauss concerned himself with throughout his entire life: *the inverse problem*.[5] A number of singularities, selected out of some continuous process, can be accessed by human experimental work. Only the human mind is capable of conjecturing what that continuous domain must be, which would generate those singularities. If a person discovers the nature of that continuous domain — that universal physical principle — he can apply that knowledge to generate any singularity he wishes. He has thus gained a power.

Pythagoras did find a set of whole numbers that could construct a right triangle. Pick some odd square number, like 49, whose root is 7 (can you prove that every odd number

[4]It is for this reason, that Lyndon LaRouche once poked at his friends that, since 5 is one of these special numbers, it is actually an *irrational* number!

[5]Gauss himself called it "Indefinite Analysis."

has an odd square?). Subtract 1 from that square, and then divide it in half, leaving three pieces: 1, 24, and 24. Now, arrange these numbers into a *gnomon*, or an "L" shape with the 1 at the intersection, as in the animation below. Now, the gnomon is surrounding another square shape, whose side length is 24. We've thus just constructed two new squares, of side lengths 24 and 25. Hence, we have three lengths that would construct a right triangle, $7^2 + 24^2 = 25^2$. The crafty reader should figure out how to begin with an even square, instead of an odd.

[ANIMATION OF PYTHAGORAS' CONSTRUCTION OF PYTHAGOREAN TRIPLES]

Interlude on Fermat

Pierre de Fermat's name pops up regularly in the *Disquisitiones Arithmeticae*. Usually, Gauss cites Fermat as the originator of the most beautiful theorems in the book, and then usually says that either Euler tried to prove them, or did prove them. One of these most important theorems relates to our development of the Pythagorean Triples, and the curious relationship between square numbers and the primes.

As we saw before, the sum of two square numbers does not necessarily have to be a square number, although there are special cases of this, such as $3^2 + 4^2 = 5^2$. Most of the time, when adding two square numbers, we get a number that is not square, such as $3^2 + 5^2 = 9 + 25 = 34$, which is 2 less than the nearest square. 34 itself is a composite number, being made up of $17 \cdot 2$. Let us develop the sum of every pair of square numbers up to 100:

Sums of Squares

	1	4	9	16	25	36	49	64	81	100
1	2	5	10	17	26	37	50	65	82	101
4		8	13	20	29	40	53	68	85	104
9			18	25	34	45	58	73	90	109
16				32	41	52	65	80	97	116
25					50	61	74	89	106	125
36						72	85	100	117	136
49							98	113	130	149
64								128	145	164
81									162	181
100										200

Among these numbers, we find only *one* that is a true square number, 25. The others are either composite numbers, or prime numbers. Let us collect the prime numbers:

5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97,
101, 109, 113, 137, 149, 173, 181, 193, 197

The alert reader will recognize that, not only are each of these $4n+1$ numbers, but they are *all* of the $4n+1$ numbers below 200.[6] In other words, those prime numbers that would be part of a Pythagorean Triple, were they square numbers, are those primes who have -1 as a quadratic residue! Fermat claimed to have proved that all of the prime numbers of the form $4n+1$ are the sum of two squares, and that all the rest of the primes are not. Hence, we have another geometric insight into these primes:

> all $4n+1$ primes perform the same function as the square of the hypotenuse of a Pythagorean Triangle, and also cause -1 to function as a special type of square number.

Perhaps they are not prime numbers at all, but themselves a type of square number, for which the concept of *number, itself* must be expanded. This will have profound implications later, when we look at Gauss's treatment of Biquadratic Residues, but let this suffice as a lead-in to the principle of Quadratic Reciprocity.

Reciprocity

Gauss begins his discussion of Quadratic Reciprocity by tacitly applying his method of *inversion*: It is relatively simple to calculate all the quadratic residues of a given modulus, but, to find all those moduli for which a given number is a quadratic residue, is much more difficult. What is the principle which determines the distribution of quadratic residues among the moduli?

We have already answered this question for the case of -1. -1 is always a quadratic residue of prime numbers of the form $4n+1$, and never one for prime numbers of the form $4n+3$. We have seen some geometrical hints as to why this is the case, though Gauss presents a merely mathematical proof of this. This also has a general implication for our problem here. If a number r is a quadratic residue of a prime modulus of the form $4n+1$, then, since -1 is already a quadratic residue, $-r$ will also be a quadratic residue. We saw earlier, that this caused the modulus circle to be symmetric around the diameter.

How about 2? If you look at your modulus circles, or your table of residues of powers, you will see which primes under 100 have 2 as a quadratic residue, namely 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, and 97. The other primes have 2 as a quadratic nonresidue. Some of these are of the form $4n+1$, but some are also $4n+3$. -2 is a quadratic residue of 3, 17, 11, 19, 41, 43, 59, 67, 73, 83, 89, 97. These also contain both forms of prime.

At this point, Gauss begins introducing further forms for the prime numbers. For the numbers $4n+1$ and $4n+3$, we can restrict n to only those values that are even, or equal to 2 times some other number, $n=2m$. Now, our $4n+1$ numbers become $4\cdot 2m+1 = 8m+1$, and our $4n+3$ numbers become $4\cdot 2m+3 = 8m+3$. If we restrict n to only odd numbers,

[6] notice, also, that 25 is a $4n+1$ number

or $n = 2m + 1$, then $4n + 1$ becomes $4 \cdot (2m + 1) + 1 = (8m + 4) + 1 = 8m + 5$, and $4n + 3$ becomes $4 \cdot (2m + 1) + 3 = (8m + 4) + 3 = 8m + 7$. We can distribute all prime numbers into these four classes

$8m+1$	$8m+3$	$8m+5$	$8m+7$
17	3	5	7
41	11	13	23
73	19	29	31
89	43	37	47
97	59	53	71
	67	61	79
	83		

Looking back now at 2 and -2, we see that 2 is always a quadratic residue of prime number moduli of the forms $8m + 1$ and $8m + 7$. Since $8m + 1$ numbers are also $4m + 1$ numbers (which always has -1 as a quadratic residue), -2 will also always be a quadratic residue of these moduli, but it will be a quadratic nonresidue of those primes of the form $8m + 7$. And, since 2 is a quadratic nonresidue of primes of the forms $8m + 3$ and $8m + 5$, -2 will be a quadratic residue of $8m + 3$ numbers (because -1 is a quadratic nonresidue of $8m + 3$ numbers), but a quadratic nonresidue of $8m + 5$ numbers.

Gauss continues on to interrogate the numbers 3 and -3. 3 is a quadratic residue of 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, and 97. -3 is a quadratic residue of 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, and 97. Notice that both are quadratic residues of 3, which is equal to $4 \cdot 0 + 3$, which is an anomaly. Gauss generates yet more forms of numbers $(12n + 5,\ 12n + 7,\ 12n + 11)$, but presents a first inkling of something startling: -3 is always a quadratic residue of prime numbers *which are themselves quadratic residues of +3*. For example, 7 is a quadratic residue of 3, and -3 is congruent to 4 (mod 7), which is obviously a quadratic residue. Our circle of modulus 3 will show that, only those numbers congruent to 1 modulus 3 will be quadratic residues, which are all equal to $3n + 1$ for some n (not including 3 itself). In other words, all prime numbers of the form $3n + 1$ have -3 as a quadratic residue, and if they are also of the form $4n + 1$, then $+3$ is also a quadratic residue. On the other hand, if the $3n + 1$ number is also a $4n + 3$ number, then $+3$ is not a quadratic residue. This is complete.

For 5 and -5, the reader can consult their own chart. There is an elegant relationship here, too: $+5$ is a quadratic residue of all prime numbers that are themselves quadratic residues of $+5$. A similar relationship exists between 7 and -7 also: -7 is a quadratic residue of all primes that are quadratic residues of $+7$, and it is a quadratic nonresidue for all prime quadratic nonresidues of $+7$.

At this point, Gauss stops this *inductive* investigation, and begins constructing a general principle. Let a and a' be two numbers of the form $4n + 1$, and let b and b' be numbers of the form $4n + 3$. If a is a quadratic residue of a', then we will write $a\mathrm{R}a'$, and if a is

a quadratic nonresidue of a', we will write $a\mathrm{N}a'$. We saw that when $a\mathrm{N}a'$ (or, what is the same, $-a\mathrm{N}a'$), then $a'\mathrm{N}a$ and $-a'\mathrm{N}a$. When $+a\mathrm{R}b$, then $-a\mathrm{N}b$ (by anti-symmetry), but both $+b\mathrm{R}a$ and $-b\mathrm{R}a$. Conversely, when both $+b\mathrm{N}a$ and $-b\mathrm{N}a$, then $+a\mathrm{N}b$ and $-a\mathrm{R}b$. When $+b\mathrm{R}b'$ $(-b\mathrm{N}b')$, then $+b'\mathrm{R}b$ $(-b'\mathrm{N}b)$. If you observe the relationships between more moduli, you will see that what we have found seems to always be the case.

The complex of these reciprocal relationships were what Gauss called the *Fundamental Theorem*, "[s]ince almost everything that can be said about quadratic residues depends on this theorem."[7] It is today known as the *Principle of Quadratic Reciprocity*. With a bit of deduction, all of the reciprocal relationships can now be determined. Here is Gauss's chart of relationships:

	If	we have
1.	$\pm a\ R\ a'$	$\pm a'\ R\ a$
2.	$\pm a\ N\ a'$	$\pm a'\ N\ a$
3.	$+a\ R\ b$ $-a\ N\ b$	$\pm b\ R\ a$
4.	$+a\ N\ b$ $-a\ R\ b$	$\pm b\ N\ a$
5.	$\pm b\ R\ a$	$+a\ R\ b$ $-a\ N\ b$
6.	$\pm b\ N\ a$	$+a\ N\ b$ $-a\ R\ b$
7.	$+b\ R\ b'$ $\neg b\ N\ b'$	$+b'\ N\ b$ $-b'\ R\ b$
8.	$+b\ N\ b'$ $-b\ R\ b'$	$+b'\ R\ b$ $-b'\ N\ b$

Let's look at some examples, because this is pretty confusing. The quadratic residues of 17 are 1, 2, 4, 8, 9, 13, 15, and 16. We want to find which of the prime numbers from 1 to 100 have 17 as a quadratic residue — this is Gauss's inverse problem. $17 = 4 \cdot 4 + 1$, so we know, according to the law of Quadratic Reciprocity, that it should be a quadratic residue of only those numbers that 1) are $= 4n + 1$ and are quadratic residues of 17, and 2) are $= 4n + 3$ and are quadratic nonresidues of 17.

The prime numbers that are quadratic residues of 17 are 13, 19, 43, 47, 53, 59, 67, 83, and 89. The primes that are quadratic nonresidues are 3, 5, 7, 11, 23, 29, 31, 37, 41, 61, 71, 73, 79, and 97. We will collect these according as they are $4n + 1$ numbers or $4n + 3$ numbers:

[7] *Disquisitiones Arithmeticae*, p. 88

Modulus 17

Quadratic Residues		Quadratic Nonresidues	
$4n+1$	$4n+3$	$4n+1$	$4n+3$
13	19	5	3
53	43	29	7
67	47	37	11
89	59	41	23
	83	61	31
		73	71
		97	79

According to Quadratic Reciprocity, $17 = 4 \cdot 4 + 1$ is a quadratic residue of all of its quadratic residues. Therefore, in modulus 13, 17 is congruent to 4, which is a square number. In modulus 43, 17 is congruent to $19^2 = 361$.

17 is supposed to be a quadratic nonresidue for all of its quadratic nonresidues. In modulus 5, 17 is congruent to 2, which is a quadratic nonresidue, and in modulus 7, 17 is congruent to 3, which is also a quadratic nonresidue. The reader should check the rest of them.

Hence, 17 is a quadratic residue of all of its quadratic residues, and a quadratic nonresidue of all of its quadratic nonresidues. Pretty simple! This also tells us when -17 is a quadratic residue, from the difference between the $4n+1$ numbers and the $4n+3$ numbers. -17 will remain a quadratic residue for all of those quadratic residues of 17 of the form $4n + 1$, but will become a quadratic nonresidue of the $4n + 3$ quadratic residues of 17, because of antisymmetry. Thus, in modulus 13 (a $4n + 1$ quadratic residue of 17), -17 is congruent to 9, a square. But, in modulus 19 (a $4n + 3$ quadratic residue of 17), it is congruent to -2 which is a quadratic nonresidue, since 2 is a quadratic residue of 19 and -1 is not.

-17 should also be a quadratic nonresidue of the $4n + 1$ quadratic nonresidues of 17, and a quadratic *residue* of the $4n + 3$ quadratic nonresidues. The reader should try these cases.

Now, a $4n+3$ number, according to Quadratic Reciprocity, should be the same character as its $4n + 1$ residues, but opposite the character of its $4n + 3$ residues. The primes that are quadratic residues of 19 are 5, 7, 11, 17, 23, 43, 47, 61, 73, and 83. Here is a chart for $19 = 4 \cdot 4 + 3$:

Modulus 19

Quadratic Residues		Quadratic Nonresidues	
$4n+1$	$4n+3$	$4n+1$	$4n+3$
5	7	13	3
17	11	29	31
61	23	37	59
73	43	41	67
	47	53	71
	83	89	79
		97	

Of its $4n+1$ quadratic residues, 19 should also be a quadratic residue. This is true for modulus 5, where 19 is congruent to 4, and also for modulus 17, where 19 is congruent to $36 = 6^2$. 19 should then be a quadratic nonresidue of all of its $4n+3$ quadratic residue. So, for modulus 7, 19 is congruent to 5, which is indeed a quadratic nonresidue of 7.

Of its $4n+1$ quadratic nonresidues, 19 should be a quadratic nonresidue also. The reader can check that, because more interesting are the $4n+3$ quadratic nonresidues, which should each have 19 as a quadratic *residue*. This is true for 31, where 19 is congruent to $9^2 = 81$.

Such an elaborately complex principle was called by Gauss, in his private writings, the *Golden Theorem*. Principles of the universe are rarely simple to state, yet they are always efficient.