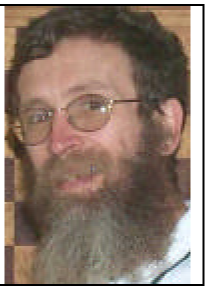
MAA Online

How Euler Did It

by Ed Sandifer



Factors of Forms

December 2005

Many number theorists think that the Quadratic Reciprocity Theorem is the most beautiful theorem in all of mathematics. It is said to be Gauss's favorite theorem. Though Euler did not discover quadratic reciprocity, nor did he prove the theorem, he gathered the observational evidence that later guided Legendre and Gauss, so that they would know what to try to prove, and he did manage to prove some preliminary results. In this month's column, we will look at Euler's first results in the subject, results that first appeared in a letter to Christian Goldbach dated August 28, 1742, [J+W] and published in 1751 [E164] in the 1744/46 volume of the journal of the St. Petersburg Academy. Harold Edwards wrote about this letter and article in 1983 in a fine paper in *Mathematics Magazine*, [Ed] and he saw the article just a bit differently.

Before we turn to Euler's article, we should remind readers what the Quadratic Reciprocity Theorem tells us. It gives us a way to find when a number a is a perfect square modulo a prime number q. For example, 1 and 4 are perfect squares modulo 7, but, some find it surprising that 2 is also a perfect square, since $3^2 = 9 \equiv 2(\text{mod}7)$. In the real numbers, $\sqrt{2}$ is irrational, but in the integers modulo 7, $\sqrt{2} = 3$. Just as in the real numbers, non-zero numbers that have square roots have two of them, and the other square root of 2, modulo 7, is 4. The other three non-zero numbers modulo 7 are 3, 5 and 6, and none of them are perfect squares. Euler later proved that modulo any odd prime q, exactly half of the numbers between 0 and p will be perfect squares and half of them will not. The ones that are perfect squares are called *quadratic residues*, and the ones that aren't are called *quadratic non-residues*.

Legendre later introduced a notation to simplify discussions. [M] The so-called *Legendre symbol*, is defined for a prime number q and another integer a not divisible by q, as follows:

$$\left(\frac{a}{q}\right) = \begin{cases} +1 & \text{if } a \text{ is a perfect square modulo } q \\ -1 & \text{if } a \text{ is not a perfect square modulo } q \end{cases}$$

The symbol is sometimes written as ($a \mid q$), and is also sometimes defined as being zero if q divides a.

Euler was the first to prove that the product of two quadratic residues or of two quadratic non-residues would be a quadratic residue, but that the product of a residue and a non-residue would be a non-residue. This fact translates into Legendre symbols as

$$\left(\frac{ab}{q}\right)=\left(\frac{a}{q}\right)\left(\frac{b}{q}\right).$$

Because of this fact, we can confine our inquiry to the cases when *a* is a prime number, since if *a* is not prime, we can factor *a* and consider the problem a factor at a time.

The prime number 2 is sometimes a problem case in number theory, being the only even prime number, and often we must deal with it separately. This formula covers the situation:

$$\begin{aligned}\left(\frac{2}{q}\right)&=\begin{cases}+1 & \text{if } q=1,7(\text{mod}8)\\ -1 & \text{if } q=3,5(\text{mod}8)\end{cases}\\ &=(-1)^{\frac{p^2-1}{8}}\end{aligned}$$

Euler knew the fact behind this formula, but he apparently never gave a proof of the fact.

The "exponent" notation given in the second line compacts the notation and simplifies calculation, but in my mind it obscures the beauty of the result. Several theorems about quadratic residues have such exponential forms as well as the "modulo" forms I prefer.

We are now ready to state the Quadratic Reciprocity Theorem, which relates the Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$, as follows:

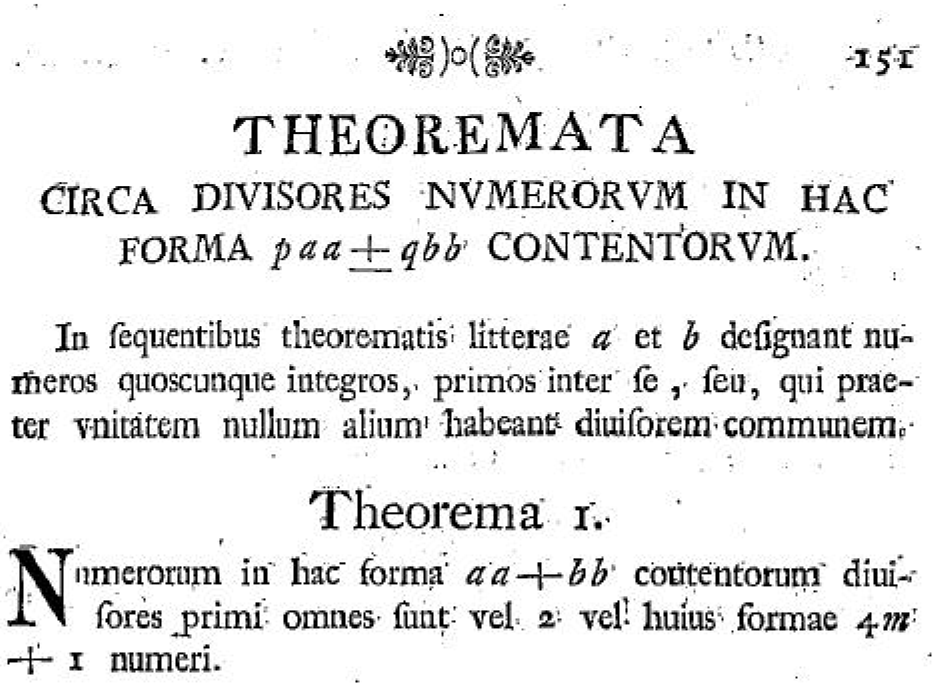
QUADRATIC RECIPROCITY THEOREM: If *p* and *q* are distinct, odd primes, then

$$\begin{aligned}\left(\frac{q}{p}\right)&=\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\\ &=\begin{cases}-\left(\frac{p}{q}\right) & \text{if } p\equiv q\equiv 3(\text{mod}4)\\ \left(\frac{p}{q}\right) & \text{otherwise}\end{cases}\end{aligned}$$

As we mentioned above, apparently Legendre first proved this, and Gauss gave several proofs. Several sources say that Euler stated the theorem in 1783, the year that he died, but nobody seems to give an explicit citation. We will leave that for another column. Here, our purpose is to see how much quadratic reciprocity Euler knew in 1742 when he wrote the letter to Goldbach, and in 1745 when he wrote E 164.

Euler's paper *Theoremata circa divisors numerorum in hac forma paa ± qbb contentorum,* "Theorems about divisors of numbers of the form *paa ± qbb,* number 164 in Eneström's index, was only Euler's tenth paper in number theory. He eventually wrote 96 papers in the area, but it is a measure of the relatively low esteem in which number theory was held at the time that half of those papers were only published posthumously.

This particular paper has a very distinctive form, different from any other paper that Euler ever wrote. It does not have the usual “paragraph” structure, but instead is a huge list of 59 “theorems,” almost always without proof or discussion, and another 17 “annotationes," rather like remarks, all preceded by a single short paragraph. Here is an image of part of the first page of the paper:



151

THEOREMATA

CIRCA DIVISORES NVMERORVM IN HAC FORMA $paa \pm qbb$ CONTENTORVM.

In ſequentibus theorematis litterae a et b deſignant numeros quoſcunque integros, primos inter ſe, ſeu, qui praeter vnitatem nullum alium habeant diuiſorem communem.

Theorema 1.

Numerorum in hac forma $aa+bb$ contentorum diuiſores primi omnes ſunt vel 2 vel huius formae $4m+1$ numeri.

This can be translated as follows:

> “In the following theorems, the letters *a* and *b* designate arbitrary relatively prime integers, that is, they have only 1 as a common divisor.
>
> “Theorem I. All of the prime divisors of numbers contained in the form $aa + bb$ are either the number 2 or are numbers of the form $4m + 1$.”

We repeat, Euler gives no proof of Theorem 1 or any of the other theorems in this paper.

After this paragraph and theorem, Euler gives his “theorems” in groups of three. Each triad begins with a theorem giving the forms of prime divisors of the form $aa + pbb$. The second theorem asserts that all of those prime divisors are themselves numbers of this form, and the third theorem is always the contrapositive of the first.

He begins with properties of sums of two square numbers, that is numbers that can be written in the form $aa + bb$. These properties that are well known now, and had been noted by Fermat almost a hundred years earlier, but in 1742 number theory was not widely studied, and probably few people other than Euler and Goldbach knew them. His first triad of theorems continues:

> “Theorem 2: All prime numbers of the form $4m + 1$ in turn are contained in numbers of this form.

> "Theorem 3: Thus the sum of two squares, that is numbers of the form $aa + bb$ are never divided by any number of the form $4m - 1$."

Note that Theorem 3 would not be true without the condition in the paragraph at the beginning of the paper that a and b must be relatively prime.

Euler does not mean these as "theorems" in the modern sense of the word. Rather, they are statements he is certain are true, having examined a large number of cases. Almost 20 years later in a paper titled *Demonstratio theorematis Fermatiani omnem numerum primum formae* $4n + 1$ *esse summam duorum quadratorum*, "Proof of a theorem of Fermat that all prime numbers of the form $4n + 1$ are the sum of two squares [E241], Euler gives a partial proof of Theorem 1, but he is only able to show that such primes are the sum of squares of two *rational* numbers, not the sum of squares of two *integers*.

He continues with his "theorems" about numbers of the form $aa + 2bb$:

> "Theorem 4: The prime divisors of numbers contained in the form $aa + 2bb$ are always either 2 or numbers contained in the form $8m + 1$, or in the form $8m + 3$.
>
> "Theorem 5: All prime numbers of the forms $8m + 1$ or $8m + 3$ are contained among the numbers of the form $aa + 2bb$.
>
> "Theorem 6: No number of the form $aa + 2bb$ can be divided by any number of the form $8m - 1$ or of the form $8m - 3$."

Euler will soon learn a lot more about numbers of the form $aa + 2bb$. In 1753, just two years after this paper is published, he will write another paper, E256, entirely devoted to the properties of such integers. For example, he tells us there, and also gives proofs, that the set of such numbers is closed under multiplication. We will perhaps devote part of a future column to this delightful paper, but there isn't room in this one.

Let us return to E 164. Euler continues listing "theorems," three at a time, each describing the divisors of a form $aa + pqq$, for p the prime numbers 3, 5, 7, 11, 13, 17, 19, and then for composite numbers 6, 10, 14, 15, 21, 30 and 35. He demonstrates by example that the theory of forms involving composite values of p is an easy corollary of the theory of forms for which p is prime. A typical example is Theorem 19, giving all the possible forms of prime divisors of a number of the form $aa + 13bb$,

> "Theorem 19: All of the prime divisors of a number of the form $aa + 13bb$ are either 2 or 13 or they are described by one of the following 12 formulas

$52m + 1$	$52m + 7$
$52m + 49$	$52m + 31$
$52m + 9$	$52m + 11$
$52m + 25$	$52m + 19$
$52m + 29$	$52m + 47$
$52m + 17$	$52m + 15$."

This seems like a disorganized jumble of numbers, but there are a great many patterns here. Some of those patterns would be easy to see if we had looked at all 59 of Euler's theorems, but others require Euler's genius to discern, as well as his immense patience and skills at calculation to prepare the data. Today it is a pleasant exercise in Maple ™ or Mathematica ™ to reproduce them. What would Euler have done with such tools?

Here are some of the easier patterns in the cases when p is prime:

- The number 1 is always among the possible remainders.

- There are 12 formulas because p is 13, and 12 is one less than that. In general, the number of formulas necessary to describe the factors of $aa + pbb$ is the number of integers less than p and relatively prime to p.

- The formulas describe numbers modulo 52 because, in general, the possible prime factors are determined by their values modulo $4p$.

- Since we are talking about *prime* factors, the remainders must obviously be relatively prime to 52, and, in general, relatively prime to $4p$. In fact, the possible remainders of prime factors (not counting the two special factors, 2 and p) of numbers of the form $aa + pbb$ are exactly half of the remainders less than $4p$ and relatively prime to $4p$. The other half of the remainders are the ones described in the third theorem of Euler's triads of theorems.

This last pattern leads to what seem to me to be more difficult observations:

- If a is a possible remainder, then $-a$ is always an impossible remainder.

Here, of course, we take the negative modulo $4p$. For example, in the case $p = 13$, we see in Theorem 19 above, we see that 7, 25 and 47 are all among the possible remainders. If we looked at Theorem 21, we would see that their negatives modulo 52, which are the values 45, 27 and 5, respectively, are all among the impossible remainders.

- If a and b are among the possible remainders, then so also is ab.

We see, for example, that 7 and 11 are possible remainders. Knowing that, modulo 52, their product 77 leaves a remainder 25, we check and see that 25 is also a remainder.

In modern terms, Euler has shown that the set of remainders of prime divisors of numbers of the form $aa + pbb$ modulo $4p$ form a subgroup of index 2 (though he hasn't been explicit about showing that it contains the necessary inverses.) Euler, of course, did not have these modern terms. They were at least a hundred years away, and came late enough that Latin had been abandoned as the international language of mathematics. Hence, mathematical Latin does not even have the vocabulary to write these results in the context of group theory.

Finally, we come to the most delicate pattern that Euler found here, and the one that links factors of forms to quadratic reciprocity. If a is relatively prime to $4p$, and also less than $4p$, then the patterns we have already described tell us that either a is among the possible remainders, or $-a$ is, but not both. Euler wants to determine which of these two is the possible remainder.

To begin to explain the pattern he sees, he gives us a table, which we give here, slightly modified:

If		$p = 3n + 1$	then	–3	is a possible remainder. Otherwise, +3 is.
If		$p = 5n + 1$			
	or	$p = 5n + 4$	then	+ 5	is a possible remainder. Otherwise, –5 is.
If		$p = 7n + 1$			
	or	$p = 7n + 2$			
	or	$p = 7n + 4$	then	–7	is a possible remainder. Otherwise, +7 is.
If		$p = 11n + 1$			
	or	$p = 11n + 3$			
	or	$p = 11n + 4$			
	or	$p = 11n + 5$			
	or	$p = 11n + 9$	then	–11	is a possible remainder. Otherwise, +11 is.

These rules all have the same form. We take p to be a prime number, and for another prime number q, we ask whether the possible remainder will be q or $-q$.

The pattern here is very subtle. Euler saw the pattern, and only then did he organize his presentation of the data to make it easier to explain the pattern. Even so, it is not very easy.

The possible forms that p might are each given modulo another prime number q. The remainders in our list are all the perfect squares modulo q. In the last list, for example, where $q = 11$, the numbers 1, 4 and 9 are obviously squares, while 3 and 5 are the squares of 5 and 4, respectively, modulo 11.

The table tells us that, for $q = 5$, $+q$ is a possible remainder if p is a perfect square modulo q. However, for $q = 3$, 7 or 11, exactly the opposite is the case; $-q$ is a possible remainder if p is a perfect square modulo q.

The pattern would be a little less obscure if Euler had extended his table to $q = 13$, so that we could see that the number 13 behaves like the number 5.

So, what property is shared by the primes 5 and 13, but not by the primes 3, 7 and 11? The one that matters is that 5 and 13 are of the form $4m + 1$, but 3, 7 and 11 are of the form $4m + 3$.

Let's try to tie this back to quadratic reciprocity now. Given a prime number p, Euler wants to be able to tell us about the prime divisors of numbers of the form $aa + pbb$. The second theorem in Euler's triads tell us that these are exactly the prime numbers that themselves can be written in this form.

Euler describes these possible prime divisors in terms of their remainders modulo $4p$, and the result that we described as being related to subgroups tells us that we can reduce the problem to remainders that are *prime* remainders.

Then whether or not q, a prime remainder modulo $4p$ is a possible remainder for a prime of the form $aa + pbb$, depends on whether or not p is a perfect square modulo q, and on whether or not q is of the form $4m + 1$. That is:

Euler's Rule:

In the case when q is of the form 4m + 1, a prime divisor of $aa + pbb$ can have the form 4n + q if p is a perfect square modulo q, that is if $\left(\frac{p}{q}\right)=+1$, but not if $\left(\frac{p}{q}\right)=-1$.

On the other hand, if q is of the form 4m + 3, the opposite rule applies and it can have the form 4n – q if p is a perfect square modulo q, that is if $\left(\frac{p}{q}\right)=+1$, but not if $\left(\frac{p}{q}\right)=-1$.

Perhaps an example would be useful. Let us pretend that we haven't seen Theorem 19, and ask if a number of the form aa + 13bb can have the form 52n + 23. Here, p = 13, q = 23, and q is of the form 4m + 3. So, we look at the second part of Euler's rule and see that a prime divisor can have the form 52n – 23 if $\left(\frac{p}{q}\right)=+1$, that is if $\left(\frac{13}{23}\right)=+1$. It turns out that $\left(\frac{13}{23}\right)=+1$ (a fact we can determine either by trying all the possibilities and finding that $6^2=36=13(\bmod 23)$, or by leaving Euler's time for our own and using the Quadratic Reciprocity Theorem). Hence, prime divisors of the form 52n – 23 are possible, and consequently, those of the form 52n + 23 are impossible.

When we check Theorem 19, we do not find the number 23 among the possible remainders, so our calculation checks out.

It's not quadratic reciprocity, but it is clearly closely related. Moreover, it is a lesson that the rich and elegant theory of quadratic reciprocity, and its tools and machinery that include modular arithmetic, quadratic forms and class fields have their origins in the ordinary and elementary questions of factoring integers into prime factors.

References:

[Ed] Edwards, Harold M., Euler and Quadratic Reciprocity, *Mathematics Magazine*, Vol. 56, No. 5. (Nov., 1983), pp. 285-291.

[E164] Euler, Leonhard, Theoremata circa divisors numerorum in hac forma *paa* ± *qbb* contentorum, *Commentarii academiae scientiarum Petropolitanae* **14** (1744/6), 1751, p. 151-181, reprinted in *Opera Omnia* Series I vol 2 p. 194-222. Available through The Euler Archive at www.EulerArchive.org.

[E241] Euler, Leonhard, Demonstratio theorematis Fermatiani omnem numerum primum formae 4n + 1 esse summam duorum quadratorum, *Novi Commentarii academiae scientiarum Petropolitanae* **5**, (1754/55) 1760, p. 3-13, reprinted in *Opera Omnia* Series I vol 2 p. 328-337. Available through The Euler Archive at www.EulerArchive.org.

[E256] Euler, Leonhard, Specimen de usu observationum in mathesi pura, *Novi Commentarii academiae scientiarum Petropolitanae* **6**, (1756/57) 1761, p. 185-230 , reprinted in *Opera Omnia* Series 1, Volume 2, pp. 459 – 492. Available through The Euler Archive at www.EulerArchive.org.

[J+W] Juskevic, A. P., and E. Winter, eds., *Leonhard Euler und Christian Goldbach, Briefwechsel 1729-1764*, Akademie-Verlag, Berlin, 1965.

[M] Miller, Jeff, Earliest Uses of Symbols in Number Theory, http://members.aol.com/jeff570/nth.html, consulted November 24, 2005.

Ed Sandifer (SandiferE@wcsu.edu) is Professor of Mathematics at Western Connecticut State University in Danbury, CT. He is an avid marathon runner, with 33 Boston Marathons on his shoes, and he is Secretary of The Euler Society (www.EulerSociety.org)

How Euler Did It is updated each month.