Examples: Quadratic Reciprocity

John D Mangual

Analytic number theory is not my expertise. Here we work out some softball examples related to quadratic reciprocity.

Here's a question: **Can permutations be used to prove Artin reciprocity** or even parts of Class Field Theory?

The proof of quadratic reciprocity seems like a random hodge-podge of techniques.[1] Can we unify some of these arguments using:

- Geometry of Numbers
- Pigeonhole Principle

Gauss in his *Disquiciones Arithmeticae* uses Pigeonhole to prove that $a^p \equiv 0 \mod p$.

[1] This is great for a first class when I was 15 years old it is not so great when you in graduate school are trying to learn Class Field Theory.

Any other applications?

Quadratic Reciprocity is stated in the number theory of textbook by **Hardy + Wright** in a Chapter called

Fermat's Theorem and its Consequences

after his discussion of other more advanced topics

- prime numbers
- Farey fractions
- irrational numbers
- congruences

I dislike prime number theory. Papers in that subject are quite tedious to read.

Fermat's little theorem says, e.g. $27|3^{26}-1$:

$$a^p = a \mod p$$

a theorem that I really like is that $5 = 2^2 + 1^2$:

$$p = a^2 + b^2 \iff p = 4k + 1$$

For proof of Quadratic Reciprocity I always refer to

- John Conway, **The Sensual Quadratic Form**

and he will use a proof by Zolotarev, involving the permutation group.

So let's get started.

The Legendre symbol is defined to be

$$\left(\frac{a}{p}\right) \equiv \begin{cases} 1 & \text{if } a \equiv x^2 \text{ mod } p \\ 0 & \text{if } a \not\equiv x^2 \text{ mod } p \end{cases}$$

an indicator that $x^2 = a$ mod p has a solution.

$$-1 \equiv 6 \times 6 \text{ mod } 37$$

So that 35 is a perfect square mod 37.

$$5 \not\equiv x^2 \text{ mod } 37$$

This is found by exhaustive search. Therefore

$$5 \times (-1) \equiv 32 \not\equiv x^2 \text{ mod } 37$$

and maybe it is also a surprise that

$$5 \times 6 \equiv 30 = 18 \times 18 \text{ mod } 37$$

The complete list (sorted is):

$[0, 1, 1, 3, 3, 4, 4, 7, 7, 9, 9, 10, 10, 11, 11, 12, 12, 16, 16, 21, 21, 25, 25, 26, 26, 27, 27, 28, 28, 30, 30, 33, 33, 34, 34, 36, 36]$

here is how the numbers appeared in order.

$[0, 1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28, 28, 30, 34, 3, 11, 21, 33, 10, 26, 7, 27, 12, 36, 25, 16, 9, 4, 1]$

The basic susprise is that a non-square times a non-square is again a square. For example, $3 \times 7 = 21$ is not a square, so this is not true in $\mathbb{Z}$.

This is our first taste of the weirdness of $\mathbb{Z}$.

A few surprises from information theory

- non-$\square$ must be found by exhaustive search
- $\square$ stop as soon as we find one solution
- non-squares $\times$ non-square $=$ square

Then there is another surprise that we can flip the number we're square-rooting and the modulus around. There is **reciprocity**.[2]

If we have two prime numbers, we can compare the possibility these are perfect square:

$$x^2 \equiv p \bmod q$$
$$y^2 \equiv q \bmod p$$

and the outcomes depend on the parity. Sometimes

- x is $\square \leftrightarrow y$ is $\square$
- x is $\square \leftrightarrow y$ is not $\square$

[2]I am still not doing a great job of motivaing congruence arithmetic. Sure it's the stuff that encrypts your e-mail and keeps your bank info secure. But really why do you care?

Any time we talk about a **pattern** we resort to the language of periodicity and to integers. And any time we talk about frequency – how often something happens. I will take my bus/car/bicycle/walk to work and I will go back home. And these two things will happen once each day. *usually*

The odds of x being a perfect square is 50/50 in congruence arithmetic and we are asking for the overlap of two events occuring 50/50 chance.

I would guess $(\frac{p}{q}) = 1$ about half the time and $(\frac{q}{p}) = 1$ so maybe about half the time they should match up and half the time not.[3]

[3] I am just totally making this stuff up. This is not mathematics, just a bunch of equations I'm writing on the board.

The Legendre symbol is defined to be

$$\left(\frac{a}{p}\right) \equiv \begin{cases} 1 & \text{if } a \equiv x^2 \bmod p \\ 0 & \text{if } a \not\equiv x^2 \bmod p \end{cases}$$

and the theorem of quadratic reciprocity is that

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

John Conway feels that proving this result with permutations leads to a simple argument. Makes no use of the notion of a

- prime number or
- perfect square number.

He defines permutations like $\times a$ mod n

$$\times 3 \bmod 11 = (0)(1,3,9,5,4)(2,6,7,10,8)$$

this is an even permutation

this has an **even number** of cycles of even length.

So this is a very particular character of the permutation group that he defines. And he may have very good reasons for that.

I still have to show that Zolotarev's definition on the cycles of the orbits of $\times a$ are the same as deciding if $x^2 \equiv a$ has a solution.

$$
\begin{tikzcd}
 & & 4 \arrow[r, dash] \arrow[dl] & 5 \arrow[d, dash] & & 8 \arrow[r, dash] \arrow[dl, dash] & 10 \arrow[d, dash] \\
0 & 1 \arrow[r, dash] & 3 \arrow[r, dash] & 9 & 2 \arrow[r, dash] & 6 \arrow[r, dash] & 7
\end{tikzcd}
$$

There is a fair bit of sleight of hand in Conway's proof (as usual)

References

(1) Jared Weinstein. **Reciprocity laws and Galois representations: recent breakthroughs** Bull. Amer. Math. Soc. 53 (2016), 1-39

(2) David A Cox. **Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication** Wiley, 2013.

(3) **A prime ideal $\mathfrak{p}$ decomposes in $\mathbb{Q}(\zeta_{24})/\mathbb{Q}(\sqrt{-6})$ iff it is generated by $\alpha \in 1 + 2\mathbb{Z}[\sqrt{-6}]$** http://mathoverflow.net/q/234570/1358

(4) Roy L. Adler **Symbolic dynamics and Markov partitions** Bull. Amer. Math. Soc. 35 (1998), 1-56 http://www.ams.org/journals/bull/1998-35-01/S0273-0979-98-00737-X/