Quadratic reciprocity: Eisenstein's proof

Robin Chapman

22 October 2013

This is a proof due to Eisenstein in 1845. It is one of those short cunning proofs that work by apparent magic.

Recall Gauss's lemma. It relies on whether integers are "p-positive" or "p-negative". We give a trigonometric interpretation. For each odd prime p, consider the function

$$f_p(x) = \sin(2\pi x/p).$$

This function has period p: $f(x+p) = f(x)$. For integers a with $0 < a < p/2$, $f_p(a)$ is positive as then $0 < 2\pi a/p < \pi$. Similarly if $0 > a > -p/2$, then $f_p(a)$ is negative as then $0 > 2\pi a/p > -\pi$. Together with the periodicity of f_p, this means that for integers a, $f_p(a) > 0$ when a is p-positive, $f_p(a) < 0$ when a is p-negative (and $f_p(a) = 0$ when $p \mid a$). Therefore for $p \nmid a$, Gauss's lemma states that $\left(\frac{a}{p}\right) = (-1)^r$ where r is the number of integers k with $0 < k < p/2$ for which $f_p(ak) < 0$. In other words $\left(\frac{a}{p}\right)$ is the **sign** of $\prod_{k=1}^{(p-1)/2} f_p(ak)$. Here the *sign* of a positive number is 1 and the sign of a negative number is -1. We write $\operatorname{sgn}(x)$ for the sign of the nonzero number x. Therefore we get the formula

$$\left(\frac{a}{p}\right) = \operatorname{sgn}\left(\prod_{k=1}^{(p-1)/2} f_p(ak)\right) = \operatorname{sgn}\left(\prod_{k=1}^{(p-1)/2} \sin(2\pi ak/p)\right).$$

To apply this to quadratic reciprocity, where $a = q$, another odd prime, it is handy to be able to express $\sin qx$ in terms of $\sin x$. To do this we study *Chebyshev polynomials*. We claim that for each $n \geq 1$ there is a polynomial $T_n(Y)$ of degree n and leading coefficient 2^{n-1} with $\cos nx = T_n(\cos x)$. Of course $T_1(Y) = Y$, and $T_2(Y) = 2Y^2 - 1$ as $\cos 2x = 2\cos^2 x - 1$. In general for $n \geq 1$ as

$$\cos(n+1)x + \cos(n-1)x = 2\cos x \cos nx$$

we can take

$$T_{n+1}(Y) = 2YT_n(Y) - T_{n-1}(Y).$$

This gives the leading term of $T_n(Y)$ as $2^{n-1}Y^n$. When n is odd, then

$$T_n(\sin x) = T_n(\cos(x - \pi/2)) = \cos(nx - n\pi/2) = (-1)^{(n-1)/2} \sin nx.$$

Thus if we define $G_n(Y) = (-1)^{(n-1)/2}T_n(Y)$, when n is a positive odd integer, then $G_n(\sin x) = \sin nx$ and $G_n(Y)$ has leading term $(-1)^{(n-1)/2}2^{n-1}Y_n = (-4)^{(n-1)/2}Y^n$.

We now identify the roots of $G_n(Y) = 0$. If $j \in \mathbf{Z}$ then

$$G_n(\sin(2\pi j/n)) = \sin(2\pi j) = 0.$$

This means that $\sin(2\pi j/n)$ is a root of $G_n(Y) = 0$. For $-(p-1)/2 \leq j \leq (p-1)/2$ the numbers $\sin(2\pi j/n)$ are distinct, so they must be the roots of $G_n(Y) = 0$. Therefore we can factorize $G_n(Y)$ as

$$G_n(Y) = (-4)^{(n-1)/2} \prod_{j=-(n-1)/2}^{(n-1)/2} (Y - \sin(2\pi j/n)).$$

If $0 < j < (n-1)/2$ then $0 > -j > -(n-1)/2$ and $\sin(2\pi(-j)/n) = -\sin(2\pi j/n)$. We can "pair off" each positive j with $-j$ in this product to get

$$\begin{aligned} G_n(Y) &= (-4)^{(n-1)/2}Y \prod_{j=1}^{(n-1)/2} (Y^2 - \sin^2(2\pi j/n)) \\ &= 2^{n-1}Y \prod_{j=1}^{(n-1)/2} (\sin^2(2\pi j/n) - Y^2). \end{aligned}$$

Therefore

$$\sin nx = 2^{n-1} \sin x \prod_{j=1}^{(n-1)/2} (\sin^2(2\pi j/n) - \sin^2 x).$$

Let p and q be distinct odd primes. Then

$$\begin{aligned} \left(\frac{q}{p}\right) &= \operatorname{sgn}\left(\prod_{k=1}^{(p-1)/2} \sin(2\pi qk/p)\right) \\ &= \operatorname{sgn}\left(\prod_{k=1}^{(p-1)/2} 4^{(q-1)/2} \sin(2\pi k/p) \prod_{j=1}^{(q-1)/2} (\sin^2(2\pi j/q) - \sin^2(2\pi k/p))\right) \\ &= \operatorname{sgn}\left(\prod_{k=1}^{(p-1)/2} \prod_{j=1}^{(q-1)/2} (\sin^2(2\pi j/q) - \sin^2(2\pi k/p))\right) \end{aligned}$$

Swapping p and q (and j and k) gives.

$$\left(\frac{p}{q}\right) = \operatorname{sgn}\left(\prod_{j=1}^{(q-1)/2}\prod_{k=1}^{(p-1)/2}(\sin^2(2\pi k/p) - \sin^2(2\pi j/q))\right).$$

The formulae for $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$ are almost the same. Each is the sign of a double product of $\frac{1}{4}(p-1)(q-1)$ terms. The terms in the second product are the negatives of the term in the first product. Therefore

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right).$$

Unless $p \equiv q \equiv 3 \pmod 4$, $\frac{1}{4}(p-1)(q-1)$ is even so that $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. If $p \equiv q \equiv 3 \pmod 4$ then $\frac{1}{4}(p-1)(q-1)$ is odd and $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.