21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc Tartar, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

37- Monday December 5, 2011.

Remark 37.1: The next step in the theory of quadratic residues is to prove the *law of quadratic reciprocity*, Lemma 37.3. It was conjectured by Euler, and by Legendre, who could not prove it. Gauss published six different proofs, and two more were found in his papers after he died.[1]

Lemma 37.2: Let p and q be distinct odd primes, and a a positive integer not a multiple of p or q. If $q = p \pmod{4a}$ or $q = -p \pmod{4a}$, then $\big(\frac{a}{p}\big) = \big(\frac{a}{q}\big)$.[2]
Proof: For $p = 2m+1$ let $S = \{a, 2a, \ldots, m\,a\}$, so that by Gauss's lemma $\big(\frac{a}{p}\big) = (-1)^M$ where M is the number of elements of S which fall into one of the open intervals $\big(\frac{p}{2}, p\big), \big(\frac{3p}{2}, 2p\big), \ldots, \big(\frac{(2c-1)\,p}{2}, c\,p\big)$,[3] and one wants the value c to be optimal, so that $\frac{(2c-1)\,p}{2} < j\,a < c\,p$ implies $j \le m$ and $\frac{(2c+1)\,p}{2} < j\,a < (c+1)\,p$ implies $j > m$: the answer is $c = \frac{a}{2}$ if a is even,[4] and $c = \frac{a-1}{2}$ if a is odd,[5] and it is important that c does not depend upon p, since one will use the same value of c after replacing p by q. By dividing by a, one finds that M is the number of positive integers which fall into one of the open intervals $\big(\frac{p}{2a}, \frac{p}{a}\big), \big(\frac{3p}{2a}, \frac{2p}{a}\big), \ldots, \big(\frac{(2c-1)\,p}{2a}, \frac{c\,p}{a}\big)$. Similarly, $\big(\frac{a}{q}\big) = (-1)^N$ where N is the number of positive integers which fall into one of the open intervals $\big(\frac{q}{2a}, \frac{q}{a}\big), \big(\frac{3q}{2a}, \frac{2q}{a}\big), \ldots, \big(\frac{(2c-1)\,q}{2a}, \frac{c\,q}{a}\big)$.

If $q = p \pmod{4a}$, then $q = p + 4a\,r$ for some $r \in \mathbb{Z}$, and one observes that for any j the number M_j of positive integers which fall into the interval $\big(\frac{(2j-1)\,p}{2a}, \frac{j\,p}{a}\big)$ has the same parity that the number N_j of positive integers which fall into the interval $\big(\frac{(2j-1)\,q}{2a}, \frac{j\,q}{a}\big)$, so that M and N have the same parity, implying the equality of the Legendre symbols. Indeed, one notices that $\big(\frac{(2j-1)\,q}{2a}, \frac{j\,q}{a}\big) = \big(2r + \frac{(2j-1)\,p}{2a}, 4r + \frac{j\,p}{a}\big)$, and that the number of integers in an open interval (x,y) and the number of integers in the open interval $(x+2r_1, y+2r_2)$ have the same parity if $x < y$ and $x+2r_1 < y+2r_2$, and $r_1, r_2 \in \mathbb{Z}$.[6]

If $q = -p \pmod{4a}$, then $q = -p + 4a\,s$ for some $s \in \mathbb{Z}$, and one observes that for any j the number M_j of positive integers in the interval $\big(\frac{(2j-1)\,p}{2a}, \frac{j\,p}{a}\big)$ has the same parity than the number N_j of positive integers in the interval $\big(\frac{(2j-1)\,q}{2a}, \frac{j\,q}{a}\big)$, so that M and N have the same parity, implying the equality of the Legendre symbols. Indeed, one notices that $\big(\frac{(2j-1)\,q}{2a}, \frac{j\,q}{a}\big) = \big(2s - \frac{(2j-1)\,p}{2a}, 4s - \frac{j\,p}{a}\big)$, and that if $x < y < x+2k$ the number of integers in (x,y) and the number of integers in $(-x-2k, -y)$ have the same parity if y is not an integer, since by symmetry $(-x-2k, -y)$ and $(y, x+2k)$ have the same number of integers, and that the number of integers in (x,y) plus the number of integers in $(y, x+2k)$ is the number of integers in $(x, x+2k)$, i.e. $2k$.

Lemma 37.3: (law of quadratic reciprocity) One has $\big(\frac{p}{q}\big)\big(\frac{q}{p}\big) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$ for p and q distinct odd primes, i.e. $\big(\frac{q}{p}\big) = \big(\frac{p}{q}\big)$ if p or q has the form $4n+1$, and $\big(\frac{q}{p}\big) = -\big(\frac{p}{q}\big)$ if both p and q have the form $4n+3$. Analytically, it means that if p and q are distinct odd primes, one has $\big(\frac{q}{p}\big) = \big(\frac{p}{q}\big)(-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$.

[1] It is worth pointing out that Gauss did not know about the Legendre symbol, and that Legendre and Euler did not know about congruences, introduced by Gauss.

[2] Lemma 37.2 follows from the law of quadratic reciprocity, but it is here a step towards its proof, and it will be used for proving the law of quadratic reciprocity.

[3] The intervals are chosen to be open since $j\,a$ cannot be a multiple of $\frac{p}{2}$.

[4] If $a = 2\alpha$, then $c = \alpha$ is the right answer because $\frac{(2\alpha-1)\,p}{2} < 2\alpha\,j < \alpha\,p$ implies $2j < p = 2q+1$, i.e. $j \le m$, and $\frac{(2\alpha+1)\,p}{2} < 2\alpha\,j < (\alpha+1)\,p$ implies $2j > p + \frac{1}{2\alpha\,p} > 2q+1$, so that $j \ge m+1$.

[5] If $a = 2\beta+1$, then $c = \beta$ is the right answer because $\frac{(2\beta-1)\,p}{2} < (2\beta+1)\,j < \beta\,p$ implies $j < \frac{\beta}{2\beta+1}\,p < \frac{p}{2} = m + \frac{1}{2}$, i.e. $j \le m$, and $\frac{(2\beta+1)\,p}{2} < (2\beta+1)\,j < (\beta+1)\,p$ implies $j > \frac{p}{2} = m + \frac{1}{2}$, so that $j \ge m+1$.

[6] If $x < y$, and n is a positive integer, each of the open intervals $(x-n, y)$ and $(x, y+n)$ contain n more integers than the open interval (x,y); one deduces that if $x_1 < y_1$, $x_2 < y_2$ with $x_1 - x_2 \in \mathbb{Z}$ and $y_1 - y_2 \in \mathbb{Z}$, then the number of integers in the open interval (x_1, y_1) has the same parity than the number of integers in the open interval (x_2, y_2) if (and only if) $(x_1 - x_2) \pm (y_1 - y_2)$ is even.

Proof: If $q = p \pmod 4$, one has $q = p + 4r$, so that $\left(\frac{q}{p}\right) = \left(\frac{p+4r}{p}\right) = \left(\frac{4r}{p}\right) = \left(\frac{r}{p}\right)$, and $\left(\frac{p}{q}\right) = \left(\frac{q-4r}{q}\right) = \left(\frac{-4r}{q}\right) = \left(\frac{-r}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{r}{q}\right)$. By Lemma 37.2 one has $\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right)$, and one concludes by noticing that $\left(\frac{-1}{q}\right) = +1$ if both p and q have the form $4n+1$, and $\left(\frac{-1}{q}\right) = -1$ if both p and q have the form $4n+3$.

If $q = -p \pmod 4$ (i.e. among p and q one has the form $4n+1$ and the other has the form $4n+3$), one has $q = -p + 4s$, and one deduces that $\left(\frac{q}{p}\right) = \left(\frac{s}{p}\right)$, and $\left(\frac{p}{q}\right) = \left(\frac{s}{q}\right)$, and by Lemma 37.2 one has $\left(\frac{s}{p}\right) = \left(\frac{s}{q}\right)$, hence $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.

Lemma 37.4: For p an odd prime, one has $\left(\frac{3}{p}\right) = +1$ if and only if p has the form $12n \pm 1$, and $\left(\frac{3}{p}\right) = -1$ if and only if p has the form $12n \pm 5$, so that one has $\left(\frac{-3}{p}\right) = +1$ if and only if p has the form $12n+1$ or $12+7$, and $\left(\frac{-3}{p}\right) = -1$ if and only if p has the form $12n+5$ or $12n-1$.
Proof: If p has the form $4n+1$, then by the law of quadratic reciprocity (Lemma 37.3) $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$, which is $= +1$ if $p = 1 \pmod 3$ (i.e. p has the form $12n+1$) and which is $= -1$ if $p = 2 \pmod 3$ (i.e. p has the form $12n+5$); for those primes $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)$ since $\left(\frac{-1}{p}\right) = +1$.

If p has the form $4n+3$, then by the law of quadratic reciprocity $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$, which is $= -1$ if $p = 1 \pmod 3$ (i.e. p has the form $12n+7$) and which is $= +1$ if $p = 2 \pmod 3$ (i.e. p has the form $12n-1$); for those primes $\left(\frac{-3}{p}\right) = -\left(\frac{3}{p}\right)$ since $\left(\frac{-1}{p}\right) = -1$.

Lemma 37.5: There are infinitely many primes of the form $12n-1$, and there are infinitely many primes of the form $6n+1$.
Proof: If there were only a finite number of primes $11 = p_1 < \ldots < p_k$ of the form $12n-1$, then for $N = p_1 \cdots p_k$ any prime factor s of $12N^2 - 1$ would be either of the form $12n+1$ or of the form $12n-1$ by Lemma 37.4, since 3 is a quadratic residue modulo s, because $3(12N^2-1) = 0 \pmod s$ means $(6N)^2 = 3 \pmod s$; since the prime factors of $12N^2-1$ cannot all be of the form $12n+1$, because their product would have this form, there would be at least one prime factor s of the form $12n-1$, which could not belong to the list $\{p_1, \ldots, p_k\}$ made of divisors of N.

If there were only a finite number of primes $7 = q_1 < \ldots < q_k$ of the form $6n+1$, then for $M = q_1 \cdots q_k$ any prime factor t of $12M^2+1$ would be either of the form $12n+1$ or of the form $12n+7$ by Lemma 37.4 (hence of the form $6n+1$), since -3 is a quadratic residue modulo t, because $3(12M^2+1) = 0 \pmod t$ means $(6N)^2 = -3 \pmod t$, and it would contradict the fact that all primes of the form $6n+1$ divide M.

Lemma 37.6: For p an odd prime, one has $\left(\frac{5}{p}\right) = +1$ if and only if p has the form $5n \pm 1$, and $\left(\frac{5}{p}\right) = -1$ if and only if p has the form $5n \pm 2$.
Proof: Since 5 has the form $4n+1$, the law of quadratic reciprocity (Lemma 37.3) gives $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, which is $+1$ if p has the form $5n \pm 1$, and is -1 if p has the form $5n \pm 2$.

Lemma 37.7: There are infinitely many primes of the form $5n-1$.
Proof: If there were only a finite number of primes $19 = p_1 < \ldots < p_k$ of the form $5n-1$, then for $N = p_1 \cdots p_k$ any prime factor s of $5N^2-1$ would be of the form $5n \pm 1$ since 5 is a quadratic residue modulo s, because $5N^2 - 1 = 0 \pmod s$ implies $(5N)^2 = 5 \pmod s$; not all prime factors s would be of the form $5n+1$ since it would imply that $5N^2-1$ has this form, and a prime factor of the form $5n-1$ could not be in the list $\{p_1, \ldots, p_k\}$, made of divisors of $5N^2$.

Remark 37.8: DIRICHLET's proof that the arithmetic progression $a\,n+b$ contains infinitely many primes whenever $a \geq 3$ and $(a,b) = 1$ uses a special type of Dirichlet series (called a Dirichlet L-series) associated to a completely multiplicative function (called a *Dirichlet character*).

Definition 37.9: A *representation* of a group G on a vector space V over a field F is a group homomorphism ρ from G to $GL(V)$, the general linear group on V (invertible F-linear mappings from V into V), i.e. satisfying $\rho(g_1 g_2) = \rho(g_1)\,\rho(g_2)$ for all $g_1, g_2 \in G$; the representation is *faithful* if ρ is injective; the representation has *dimension* (or degree) n if V has dimension n, and it $n = 1$ it is called a *multiplicative character* (or *linear character*, or character). A representation ρ is *irreducible* if there are non non-trivial invariant subspace, i.e. if a subspace W of V is such that $\rho(g)$ maps W into W for all $g \in G$, then either $W = \{0\}$ or $W = V$. The *character* of a representation ρ of finite dimension is the mapping $g \mapsto \chi_\rho(g) = Trace\big(\rho(g)\big)$.[7]

[7] It is not in general an homomorphism of G into F^*.