Quadratic congruences: The quadratic reciprocity law

We are now in position to state and prove the celebrated *quadratic reciprocity law* discovered by Gauss, which facilitates decision about existence of solutions of most quadratic congruences.

Theorem 1 (The quadratic reciprocity law of Gauss)**.** *If p and q are distinct odd primes, then $(\frac{p}{q}) = (\frac{q}{p})$ unless $p \equiv q \equiv 3 \pmod 4$, in which case $(\frac{p}{q}) \neq (\frac{q}{p})$.*

Proof. Let $\alpha(p)$ denote the number of integers i, $1 \leq i \leq (q-1)/2$, such that $\rho_q(ip) < 0$. That is, $\alpha(p)$ is equal to the number of negative least residues mod q of the first $(q-1)/2$ multiples of p. Similarly, let $\alpha(q)$ denote the number of integers j, $1 \leq j \leq (p-1)/2$, such that $\rho_p(jq) < 0$. By Proposition 5.3 we have $(\frac{p}{q}) = (-1)^{\alpha(p)}$ and $(\frac{q}{p}) = (-1)^{\alpha(q)}$. The theorem will be proved if we show that $\alpha(p) + \alpha(q)$ is odd if and only if $p \equiv q \equiv 3 \pmod 4$.

Consider the interior H of the plane hexagon obtained as the intersection of the rectangle $ABCD$ where $A = (0,0)$, $B = (p/2, 0)$, $C = (p/2, q/2)$, $D = (0, q/2)$, with the strip bounded by the lines $py = q(x - 1/2)$ and $p(y - 1/2) = qx$. For lattice points (i.e., points with integer coordinates) in H, there is an involutory bijection given by $(m, n) \mapsto (-m + (p+1)/2, -n + (q+1)/2)$. This involution has a fixed point if and only if $p \equiv q \equiv 3 \pmod 4$, in which case the fixed point is unique and has coordinates $((p+1)/4, (q+1)/4)$. We conclude that the number of lattice points in H is odd if and only if $p \equiv q \equiv 3 \pmod 4$.

We will now count the lattice points in H. First, note that there are no lattice points in H on its main diagonal $py = qx$. Let (m, n) be a lattice point in H above the main diagonal. Then, $pn > qm$ and $p(n - 1/2) < qm$, which is equivalent to $-p/2 < mq - np < 0$. But this precisely means that mq has a negative least residue modulo p, that is, $\rho_p(mq) < 0$. Conversely, if for some m such that $1 \leq m \leq (p-1)/2$ the number mq has a negative least residue mod p, then there is a unique n such that $-p/2 < mq - np < 0$, and it is easy to show that then $1 \leq n \leq (q-1)/2$, that is, the point (m, n) is in H and above the main diagonal. It follows that the number of lattice points in H above the main diagonal is equal to the number of negative least residues mod p of the first $(p-1)/2$ multiples of q, which is equal to $\alpha(p)$. A similar argument shows that the number of lattice points in H below the main diagonal is equal to $\alpha(q)$.

Summing up, $\alpha(p) + \alpha(q)$ is odd if and only if $p \equiv q \equiv 3 \pmod 4$, which proves the Theorem. □

Exercise 1. Show that the congruence $x^2 \equiv 15 \pmod{89}$ has no solutions.

Proposition 2. *Let n be a positive integer, let p be an odd prime and let $a \in \mathbb{Z}$ be such that $(a, p) = 1$. Then, the congruence $x^2 \equiv a \pmod{p^n}$ has a solution if and only if $(\frac{a}{p}) = 1$.*

Proof. To prove the 'if' part, we assume that x is a solution of the congruence for some $n \geq 1$, that is, $x^2 - a = sp^n$. Let $\bar{x}$ be the inverse of x mod p; so, $x\bar{x} = 1 + tp$. With $y = x - s\bar{x}p^n(p+1)/2$ we have $y^2 - a = p^{n+1}(-s(1 + t(p+1)) + s^2\bar{x}^2p^{n-1}((p+1)/2)^2)$, i.e., a solution of $x^2 \equiv a \pmod{p^{n+1}}$. □

Exercise 2. Decide if the congruence $x^2 \equiv 12 \pmod{2989}$ has a solution.

Exercise 3. Find all primes p for which (i) $x^2 \equiv 13 \pmod p$, (ii) $x^2 \equiv 10 \pmod p$ has a solution.