2 Quadratic Reciprocity

2.1 Motivation

In G12ALN 5.3 you have leared how to solve linear equation modulo an integer. The next more complicated sort of equation will be quadratic equations. But this is really much more complicated. Even modulo integers m it seems difficult.
We will answer in this chapter how to solve equations like $x^2 \equiv a \pmod{p}$ for a prime p. In fact, that is an exageration: We will only learn how to detect whether or not this equation has a solution.
Note that the question is without interest when $p = 2$. We will therefore assume throughout this chapter that p is an *odd* prime.
For $p = 3$, we see that $x^2 \equiv 2$ has no solution, since $0^2 \equiv 0$ and $1^2 \equiv (-1)^2 \equiv 1$. For $p = 5$, we can compute all squares:

x	0	1	2	3	4
x^2	0	1	4	4	1

So only when $a \equiv 0, 1, 4 \pmod{5}$, we have a solution to $x^2 \equiv a \pmod{p}$. Similarly for $p = 7$, we have

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1

so only $a \equiv 0, 1, 2, 4$ admit a "square root", but not $a \equiv 3, 5, 6$.

Reduction to the prime case

[non-exminable] More generally, we could ask for a quadratic equation $x^2 + a\,x + b \equiv 0 \pmod{m}$. Suppose for simplicity that m is odd. Then we can complete the square $\bigl(x + \frac{a}{2}\bigr)^2 \equiv \frac{1}{4}(a^2 - 4\,b) \pmod{m}$. So we are reduced to find a solution to an equation of the form $x^2 \equiv a \pmod{m}$ discussed above.
We can use the Chinese remainder theorem to reduce to the case when $m = p^k$ is a prime power. Let $m = p_1^{a_1} \cdots p_r^{a_r}$ be the prime factorisation of m. If we can find a solution x_i to the equation $x^2 \equiv a \pmod{p_i^{a_i}}$ then the Chinese remainder theorem gives us a solution x modulo m. If there is a prime p_i such that we can not find a solution to $x^2 \equiv a \pmod{p_i^{a_i}}$, then we will never be able to find a solution modulo m either.
Note that there are several solutions modulo p_i in general and we will find plenty of solutions modulo m. E.g. $x^2 \equiv 4 \pmod{15}$ has four solutions modulo 15, namely $x \equiv 2, 7, 8, 13 \pmod{15}$.
Let p be an odd prime. Finally one would like to reduce the question modulo p^k to a question modulo p. This can be done indeed using Hensel's lemma (G12ALN 5.3.5). We review it in the last chapter.

2.2 The Legendre symbol

Definition. A **quadratic residue** modulo p is an integer $a \pmod{p}$ such that $p \nmid a$ and $x^2 \equiv a \pmod{p}$ does have solutions; a **quadratic non-residue**[1] modulo p is an integer a such that ($p \nmid a$ and) $x^2 \equiv a \pmod{p}$ has no solutions.

Lemma 2.1. *Let p be an odd prime. Let g be a primitive element modulo p. Then $a \equiv g^k \pmod{p}$ is a quadratic residue if and only if k is even, otherwise it is a quadratic non-residue. There are exactly $\frac{p-1}{2}$ quadratic residues modulo p and just as many quadratic non-residues.*

[1] A stupid name: It should be "non-quadratic residue".

Proof. If $k = 2n$ is even, then $x = g^n$ is a solution to $x^2 \equiv g^k \pmod p$ and hence g^k is a quadratic residue. Conversely, if $b = g^n$ is a solution to $x^2 \equiv g^k \pmod p$ then $2n \equiv k \pmod{p-1}$. Since $p-1$ is even, k must be even, too.
Now, $g^0, g^2, g^4, \dots, g^{p-3}$ are all quadratic residues modulo p and $g^1, g^3, g^5, \dots, g^{p-2}$ are all quadratic non-residues modulo p. There are $\frac{p-1}{2}$ of each. □

This would be false if p were not assumed to be prime. The only invertible residue classes that are square modulo 15 are 1 and 4.

Definition. The **Legendre Symbol** $\left(\frac{a}{p}\right)$ is defined for $a \in \mathbb{Z}$ and p an odd prime by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a; \\ +1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod p \text{ has solutions;} \\ -1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod p \text{ has no solutions.} \end{cases}$$

So $\left(\frac{a}{p}\right) = +1$ when a is a quadratic residue and $\left(\frac{a}{p}\right) = -1$ when a is a quadratic non-residue modulo p.

Remark. The number of solutions to $x^2 \equiv a \pmod p$ is always $1 + \left(\frac{a}{p}\right)$.

Proposition 2.2. *(i).* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *when* $a \equiv b \pmod p$*;*

(ii). ***Euler's Criterion:*** $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$*;*

(iii). $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & \textit{if } p \equiv 1 \pmod 4; \\ -1 & \textit{if } p \equiv 3 \pmod 4; \end{cases}$

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

Proof. (i). Clear.

(ii). If $p \mid a$, then both sides are zero modulo p.
Otherwise $a \equiv g^k$ for some k, where g is a fixed primitive element modulo p. Now $\left(\frac{a}{p}\right) = (-1)^k$.
Let $h = g^{(p-1)/2}$. Since $h^2 \equiv 1$, but $h \not\equiv 1 \pmod p$, we have $h \equiv -1 \pmod p$. Now $a^{(p-1)/2} \equiv h^k \equiv (-1)^k$ modulo p.

(iii). The previous part with $a = -1$.

(iv). Part ii) shows that $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, so they are equal as both are $-1, 0, 1$. □

Example. In principle, Euler's criterion give a way to compute $\left(\frac{a}{p}\right)$. But it is hardly faster than checking all residue classes x for a solution to $x^2 \equiv a \pmod p$. For $p = 11$, we get

a	0	1	2	3	4	5	6	7	8	9	10
a^5	0	1	32	243	1024	3125	7776	16807	32768	59049	100000
a^5 mod 11	0	1	-1	1	1	1	-1	-1	-1	1	-1
$\left(\frac{a}{11}\right)$	0	1	-1	1	1	1	-1	-1	-1	1	-1

Note that Euler's criterion is false when p is not a prime. For instance is $2^7 \not\equiv \pm 1$ modulo 15 so 15 can not be a prime. More convincingly, $3^{1996001} \equiv 2664001 \not\equiv \pm 1$ despite the fact that 3 is not a square modulo 3992003. So 3992003 is not prime.

An important consequence of the last item in the proposition is the following. If we want to know how to evaluate $(\frac{a}{p})$ for all a, it is enough to evaluate $(\frac{-1}{p})$, $(\frac{2}{p})$ and $(\frac{q}{p})$ for odd primes q, as we can first factor a. E.g.

$$\Bigl(\frac{-2143018}{p}\Bigr) = \Bigl(\frac{-1}{p}\Bigr)\cdot\Bigl(\frac{2}{p}\Bigr)\cdot\Bigl(\frac{101}{p}\Bigr)\cdot\Bigl(\frac{103^2}{p}\Bigr) = \Bigl(\frac{-1}{p}\Bigr)\cdot\Bigl(\frac{2}{p}\Bigr)\cdot\Bigl(\frac{101}{p}\Bigr).$$

We will now proceed to give a formula for exactly the other two Legendre symbols $(\frac{2}{p})$ and $(\frac{q}{p})$. But first we not an interesting consequence of the propostion:

Theorem 2.3. *There are infinitely many primes of the form $4n+1$.*

Proof. Suppose $\{p_1, \dots p_r\}$ is the complete list of primes of the form $4n+1$. Let p be a prime divisor of $n = (2p_1 \cdots p_r)^2 + 1$. Then -1 is a quadratic residue modulo p, so $p \equiv 1 \pmod 4$. But p can not be equal to p_i. Contradiction. □

2.3 The Computation of $(\frac{2}{p})$

We wish to find a closed formula for $(\frac{2}{p})$ only depending on the odd prime p. Here is what the first few values look like

p	3	5	7	11	13	17	19	23	27	31	37
$(\frac{2}{p})$	-1	-1	1	-1	-1	1	-1	1	-1	1	-1

Definition. Let n be an integer. The integer m such that $m \equiv n \pmod p$ and $|m| < \frac{p}{2}$ is called the **least residue** of n modulo p.

Proposition 2.4. $(\frac{2}{p}) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & \textit{if } p \equiv \pm 1 \pmod 8; \\ -1 & \textit{if } p \equiv \pm 3 \pmod 8. \end{cases}$

Proof. Consider the least residues of all even integers 2, 4, …, $p-1$.

$$\begin{aligned} p-1 &\equiv -1 \equiv (-1)^1 \cdot 1 \\ 2 &\equiv 2 \equiv (-1)^2 \cdot 2 \\ p-3 &\equiv -3 \equiv (-1)^3 \cdot 3 \dots \end{aligned}$$

There are $\frac{p-1}{2}$ elements in the list. Their product gives

$$2^{\frac{p-1}{2}} \cdot \Bigl(\frac{p-1}{2}\Bigr)! \equiv (-1)^{\frac{1}{2}\cdot\frac{p-1}{2}\cdot\frac{p+1}{2}} \cdot \Bigl(\frac{p-1}{2}\Bigr)! \pmod p\,.$$

Simplifying by the factorial on both sides and using Euler's criterion proves the proposition. □

2.4 Gauss's Lemma

The method used to compute $(\frac{2}{p})$ works for $(\frac{a}{p})$ in general:

Gauss's lemma 2.5. *Suppose $p \nmid a$. Let μ be the number of least residues of the elements in $\{a, 2a, 3a, \dots, \frac{p-1}{2}a\}$ that are negative. Then $(\frac{a}{p}) = (-1)^{\mu}$.*

Proof. The least residues of the $k \cdot a$ are, up to sign, all the numbers between 1 and $\frac{p-1}{2}$, since $k_1\, a \equiv \pm k_2\, a \pmod{p}$ is impossible unless $k_1 = k_2$. Taking the product gives

$$a^{(p-1)/2}((p-1)/2)! \equiv (-1)^{\mu}((p-1)/2)! \pmod{p}$$

and hence

$$a^{(p-1)/2} \equiv (-1)^{\mu} \pmod{p}$$

from which the result follows by Euler's criterion. □

Example. As an example we can take $a = 3$ and $p = 11$. So $\frac{p-1}{2} = 5$ and we are looking at the set $\{3, 6, 9, 12, 15\}$. The least residues are

$k \cdot a$	3	6	9	12	15
least residue	3	-5	-2	1	4

So $\mu = 2$ and $(\frac{3}{11}) = (-1)^2 = +1$. Indeed $5^2 \equiv 3 \pmod{11}$.

We could also use Gauss' lemma to compute $(\frac{a}{p})$, but it still requires to look at $\frac{p-1}{2}$ integers, which is very large when p is very large.

2.5 The Law of Quadratic Reciprocity

Quadratic Reciprocity Law 2.6. *Let p and q be distinct odd primes. Then*

(i). $$(\tfrac{-1}{p}) = (-1)^{(p-1)/2} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4}; \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

(ii). $$(\tfrac{2}{p}) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

(iii). $$(\tfrac{p}{q})(\tfrac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4} \textbf{ or } q \equiv 1 \pmod{4}; \\ -1 & \text{if } p \equiv 3 \pmod{4} \textbf{ and } q \equiv 3 \pmod{4}. \end{cases}$$

We have seen part i) and part ii) already. We will prove the most difficult part iii) later.

Computation of Legendre symbols

Here an example of how to compute Legendre symbols very fast.

$$\left(\frac{44}{47}\right) = \left(\frac{4}{47}\right) \cdot \left(\frac{11}{47}\right) = \left(\frac{11}{47}\right) = -\left(\frac{47}{11}\right) = -\left(\frac{3}{11}\right) = (-1) \cdot (-1) \cdot \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1$$

or faster

$$\left(\frac{44}{47}\right) = \left(\frac{-3}{47}\right) = \left(\frac{-1}{47}\right) \cdot \left(\frac{3}{47}\right) = (-1) \cdot (-1) \cdot \left(\frac{47}{3}\right) = \left(\frac{2}{3}\right) = -1$$

It is very quick to compute $(\frac{1000003}{3000017})$ this way, knowing that both entries are primes here. Otherwise we would have to factor and that may be very time consuming for large integers. Luckily there is a generalisation of Legendre symbols called Kronecker symbols (or Jacobi symbols) which satisfy a quadratic reciprocity even for composite numbers. But we do not go into details here.

So a computer can decide in mili-seconds if a given integer a is a quadratic residue modulo a huge prime p.

Primes for which a is a quadratic residue

The quadratic reciprocity law has an amazing consequence. Fix an a and look for all primes p for which $(\frac{a}{p}) = +1$. In fact this only depends on the residue class of p modulo $4 \cdot |a|$ (and sometimes on $|a|$ only).
For instance if $a = q$ is a prime which is congruent to $+1$ modulo 4. Then $(\frac{q}{p}) = (\frac{p}{q})$ by iii). The later only depends on the residue class of p modulo $q = a$. As an example, we can take $a = 5$. Then 5 is a quadratic residue modulo p if and only if $(\frac{p}{5}) = +1$, i.e. if and only if $p \equiv 1$ or 4 modulo 5.

p	3	5	7	11	13	17	19
$(\frac{5}{p})$	-1	0	-1	1	-1	-1	1
$p \bmod 5$	3	0	2	1	3	2	4

If instead $a = q$ is a prime which is congruent to 3 modulo 4. Then $(\frac{q}{p}) = \pm(\frac{p}{q})$ with the sign $+1$ if and only if $p \equiv +1 \pmod 4$. So we have that

$$\Big(\frac{q}{p}\Big) = +1 \Leftrightarrow \begin{cases} \big((\frac{p}{q}) = +1 \text{ and } p \equiv +1 \pmod 4\big) \text{ or} \\ \big((\frac{p}{q}) = -1 \text{ and } p \equiv -1 \pmod 4\big). \end{cases}$$

The first condition in both cases is a condition on p modulo q while the second is a condition on p modulo 4. So by the Chinese remainder theorem, we can formulate one condition modulo $4q$. As an example, we can take $a = 3$. The above shows that 3 is a quadratic residue modulo p if and only if either $\big(p \equiv +1 \pmod 3$ and $p \equiv 1 \pmod 4\big)$ or $\big(p \equiv -1 \pmod 3$ and $p \equiv -1 \pmod 4\big)$. That is equivalent to either $p \equiv 1 \pmod{12}$ or $p \equiv -1 \pmod{12}$ by the Chinese remainder theorem.

p	3	5	7	11	13	17	19
$(\frac{3}{p})$	0	-1	-1	1	1	-1	-1
$p \bmod 12$	0	5	7	-1	1	5	7

When a is composite, we can first factor it and then treat each case separately. For instance, we find for $a = -3$ that

$$\Big(\frac{-3}{p}\Big) = \begin{cases} +1 & \text{if } p \equiv 1 \pmod 3; \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

See the additional handout for more examples.

2.6 The proof of the Quadratic Reciprocity law

Proof of iii). [non-examinable] Let $R = \{(x, y) \in \mathbb{Z}^2 |\ 1 \leqslant x \leqslant (p-1)/2, \text{ and } 1 \leqslant y \leqslant (q-1)/2\}$. Clearly $\#R = \frac{p-1}{2} \cdot \frac{q-1}{2}$. We divide the set R into four disjoint parts according to the value of the function $z = 2(py - qx)$:

$$\begin{aligned} A &= \{(x, y) \in R| \quad p < z\}; \\ C &= \{(x, y) \in R| \quad 0 < z < p\}; \\ D &= \{(x, y) \in R| \ -q < z < 0\}; \\ B &= \{(x, y) \in R| \qquad z < -q\}. \end{aligned}$$

Note that z does not take the values $-q, 0, p$ for $(x, y) \in R$, since $p \mid z \Leftrightarrow p \mid x$ and $q \mid z \Leftrightarrow q \mid y$. Hence

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \#R = \#A + \#B + \#C + \#D.$$

Let μ_C be the number of elements in $\{q, 2q, 3q, \dots, \frac{p-1}{2}q\}$ whose least residue is negative. By Gauss' lemma, we have $(-1)^{\mu_C} = (\frac{q}{p})$. Let μ_D be the number of negative least residues among $\{p, 2p, \dots, \frac{q-1}{2}p\}$, hence $(-1)^{\mu_D} = (\frac{p}{q})$.

We will show that $\#A = \#B$, and then that $\#C = \mu_C$ and $\#D = \mu_D$. From these the theorem follows :

$$\frac{p-1}{2} \cdot \frac{q-1}{2} \equiv \mu_C + \mu_D \pmod{2}\,.$$

$\#A = \#B$: This is because R is symmetric about its centre point $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$. The map

$$(x, y) \mapsto (x', y') = \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$$

has the property that $(x, y) \in A \iff (x', y') \in B$, since $z + z' = p - q$ implies $z > p \Leftrightarrow z' < -q$, so gives a bijection between the points in A and those in B.
$\#C = \mu_C$: Fix $1 \leqslant x \leqslant \frac{p-1}{2}$. Then

$$(x, y) \in C \iff 0 < z < p \iff py - p/2 < qx < py.$$

For each x this inequality holds for at most one y, and is precisely the condition that the least residue of $q\,x$ modulo p is negative. So the total number of these (x, y) pairs is exactly the integer μ_C.
$\#D = \mu_D$: Similarly (interchanging p and q). □

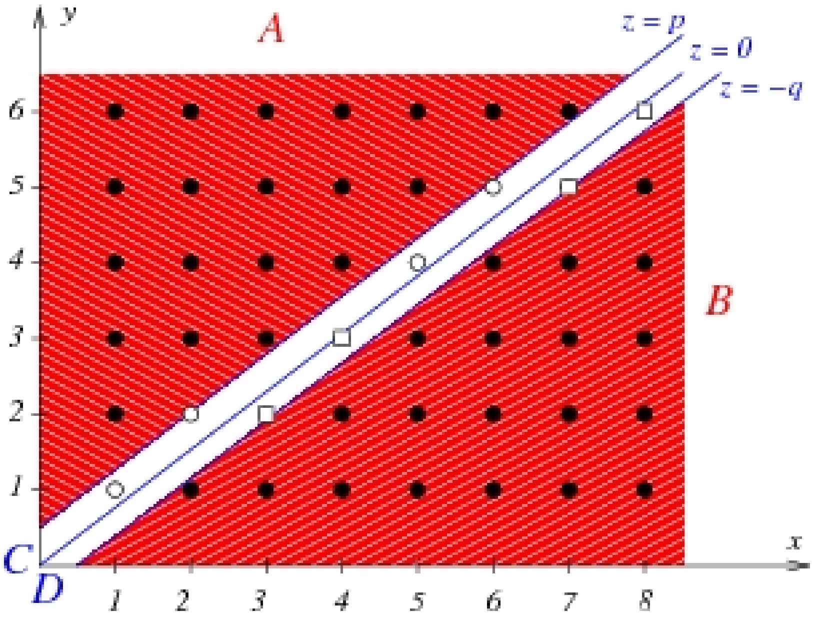

Figure 1: Illustration of the proof for $p = 17$ and $q = 13$.