8. Quadratic Residues, Quadratic Reciprocity Law

8.1. Quadratic residues. Let m be an integer > 2. An integer a is called a *quadratic residue* modulo m iff there exists an integer x with

$$x^2 \equiv a \bmod m.$$

This means that the class of a in the ring $\mathbb{Z}/m$ is a square. Of particular importance is the case where $m = p$ is an odd prime. Since 0 is always a square, we consider the group $(\mathbb{Z}/p)^* = \mathbb{F}_p^*$ of non-zero elements. The squaring map

$$sq : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*, \quad x \mapsto sq(x) := x^2$$

is a group homomorphism. The kernel of sq consists of the solutions of the equation $x^2 = 1 \iff (x+1)(x-1) = 0$, hence $\mathrm{Ker}(sq) = \{\pm 1\}$. Therefore the image $sq(\mathbb{F}_p^*) = (\mathbb{F}_p^*)^2$, which is the subgroup of squares in $\mathbb{F}_p^*$, has $(\#F_p^*)/2 = (p-1)/2$ elements. Hence there are exactly as many squares as non-squares in $\mathbb{F}_p^*$. A further consequence is that the product of two non-squares is a square.

8.2. The Legendre symbol. For an odd prime p and an integer a which is coprime to p, the Legendre symbol $(\frac{a}{p})$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{if } a \text{ is a quadratic residue } \bmod p, \\ -1, & \text{if } a \text{ is not a quadratic residue } \bmod p. \end{cases}$$

This definition is extended to all integers a by setting

$$\left(\frac{a}{p}\right) = 0 \quad \text{for } p \mid a.$$

The Jacobi symbol has the following properties:

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right) \quad \text{if } a \equiv a' \bmod p,$$

and

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \text{for all } a, b \in \mathbb{Z}.$$

Therefore the map $x \mapsto (\frac{x}{p})$ can be seen as a group homomorphism $\mathbb{F}_p^* \to \{\pm 1\}$, which fits into an exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{F}_p^* \xrightarrow{sq} \mathbb{F}_p^* \xrightarrow{(\frac{\ }{p})} \{\pm 1\} \longrightarrow 1.$$

The following is an important criterion of Euler to decide whether an integer a is a quadratic residue mod p.

8.3. Theorem (Euler). *Let p be an odd prime. Then*

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p \quad \text{for all } a \in \mathbb{Z}.$$

Proof. If $p \mid a$, then both sides of the equation are congruent 0. We may therefore assume $p \nmid a$.

a) Suppose first that a is a square mod p, i.e. $a = b^2 \bmod p$ for some integer b. Then

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

by the theorem of Fermat.

b) Let g be a primitive root mod p. Since $g^{p-1} \equiv 1 \bmod p$ and $g^{(p-1)/2} \not\equiv 1 \bmod p$, we must have $g^{(p-1)/2} \equiv -1 \bmod p$. If a is a non-square mod p, then $a \equiv g^s \bmod p$ with an odd integer s. Now

$$s\,(p-1)/2 \equiv (p-1)/2 \bmod (p-1),$$

hence

$$a^{(p-1)/2} \equiv g^{s(p-1)/2} \equiv g^{(p-1)/2} \equiv -1 \bmod p, \quad \text{q.e.d.}$$

As an application of the criterion of Euler we can prove

8.4. Theorem (Supplements to the reciprocity law). *Let p be an odd prime. Then*

1) $$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1, & \text{if } p \equiv 1 \bmod 4, \\ -1, & \text{if } p \equiv 3 \bmod 4, \end{cases}$$

2) $$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1, & \text{if } p \equiv \pm 1 \bmod 8, \\ -1, & \text{if } p \equiv \pm 3 \bmod 8. \end{cases}$$

Proof. The first assertion is a direct consequence of theorem 8.3.

Ad 2). We have to calculate $2^{(p-1)/2} \bmod p$. We use a little trick and pass to the ring $\mathbb{Z}[i]$ of Gaussian integers. In $\mathbb{Z}[i]$ we have

$$2 = -i(1+i)^2,$$

therefore $2^{(p-1)/2} = (-i)^{(p-1)/2}(1+i)^{p-1}$, which implies

$$2^{(p-1)/2}(1+i) = (-i)^{(p-1)/2}(1+i)^p.$$

To calculate $(1+i)^p$, we use the binomial theorem. Since the binomial coefficients $\binom{p}{k}$ are divisible by p for all $k = 1, 2, \ldots, p-1$, it follows

$$(1+i)^p \equiv 1 + i^p \bmod p.$$

(Of course the congruence mod p is to be understood separately for the real and imaginary part.) Therefore $2^{(p-1)/2}$ is congruent mod p to the real part of

$$z_p := (-i)^{(p-1)/2}(1+i^p).$$

It is easily seen that z_p depends only on p mod 8 and

$$z_p = \begin{cases} 1+i & \text{if } p \equiv 1 \bmod 8, \\ -1-i & \text{if } p \equiv 3 \bmod 8, \\ -1-i & \text{if } p \equiv 5 \bmod 8, \\ 1+i & \text{if } p \equiv 7 \bmod 8. \end{cases}$$

This implies assertion 2) of the theorem, q.e.d.

8.5. Gauss sums. As we have seen in the proof of the preceeding theorem, it is sometimes helpful to use complex numbers. This will become even more apparent in the following developments. Let p be an odd prime and

$$\zeta_p := e^{2\pi i/p} \in \mathbb{C}.$$

ζ_p is a primitive p-th root of unity. We define the Gauss sum $S(p)$ as

$$S(p) := \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta_p^k.$$

This is an element of the ring $\mathbb{Z}[\zeta_p]$. Since ζ_p is a root of the so called cyclotomic polynomial

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1,$$

which is irreducible in the ring $\mathbb{Q}[X]$, every element $z \in \mathbb{Z}[\zeta_p]$ has a unique representation as

$$z = \sum_{k=0}^{p-2} a_k \zeta_p^k \quad \text{with } a_k \in \mathbb{Z}.$$

In particular

$$\zeta_p^{p-1} = -\sum_{k=0}^{p-2} \zeta_p^k.$$

Examples. i) Let $p = 3$. We have

$$\begin{aligned} \zeta_3 &= e^{2\pi i/3} = \tfrac{1}{2}(-1+i\sqrt{3}), \\ \zeta_3^2 &= e^{4\pi i/3} = e^{-2\pi i/3} = \tfrac{1}{2}(-1-i\sqrt{3}) \end{aligned}$$

and

$$S(3) = \left(\frac{1}{3}\right)\zeta_3 + \left(\frac{2}{3}\right)\zeta_3^2 = \tfrac{1}{2}(-1 + i\sqrt{3}) - \tfrac{1}{2}(-1 - i\sqrt{3}) = i\sqrt{3}.$$

ii) For $p = 5$ one has

$$\begin{aligned} \zeta_5 &= e^{2\pi i/5} = \cos(2\pi/5) + i\sin(2\pi/5), \\ \zeta_5^2 &= e^{4\pi i/5} = \cos(4\pi/5) + i\sin(4\pi/5), \\ \zeta_5^3 &= \overline{\zeta_5^2} = \cos(4\pi/5) - i\sin(4\pi/5), \\ \zeta_5^4 &= \overline{\zeta_5} = \cos(2\pi/5) - i\sin(2\pi/5), \end{aligned}$$

and $(\frac{1}{5}) = 1$, $(\frac{2}{5}) = -1$, $(\frac{3}{5}) = -1$, $(\frac{4}{5}) = 1$, therefore

$$\begin{aligned} S(5) &= \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = (\zeta_5 + \overline{\zeta_5}) - (\zeta_5^2 + \overline{\zeta_5^2}) \\ &= 2\cos(2\pi/5) - 2\cos(4\pi/5) = \sqrt{5}. \end{aligned}$$

This follows from the explicit formulas

$$\begin{aligned} \cos(2\pi/5) &= \tfrac{1}{2}(-1 + \sqrt{5}), \\ \cos(4\pi/5) &= \tfrac{1}{2}(-1 - \sqrt{5}), \end{aligned}$$

and can also be derived from part a) of the following theorem.

8.6. Theorem. *The Gauss sum for the odd prime p satisfies*

a) $\qquad S(p)^2 = \left(\frac{-1}{p}\right)p.$

b) *If $q \neq p$ is another odd prime, then*

$$S(p)^q \equiv \left(\frac{q}{p}\right)S(p) \bmod q.$$

Here the congruence mod q means that the difference of the right hand and left hand side is an element of $q\mathbb{Z}[\zeta_p]$.

Proof. a) To abbreviate the notation, we write ζ instead of ζ_p.

$$\begin{aligned} S(p)^2 &= \sum_{k\in\mathbb{F}_p^*}\left(\frac{k}{p}\right)\zeta^k \sum_{\ell\in\mathbb{F}_p^*}\left(\frac{\ell}{p}\right)\zeta^\ell = \sum_{k,\ell\in\mathbb{F}_p^*}\left(\frac{k\ell}{p}\right)\zeta^{k+\ell} \\ &= \sum_{k\in\mathbb{F}_p^*}\sum_{s\in\mathbb{F}_p^*}\left(\frac{kks}{p}\right)\zeta^{k+ks} = \sum_{s\in\mathbb{F}_p^*}\left(\frac{s}{p}\right)\sum_{k\in\mathbb{F}_p^*}(\zeta^{1+s})^k. \end{aligned}$$

Here we have substituted $\ell = ks$. When s runs through all elements of $\mathbb{F}_p^*$, also ks runs through all elements of $\mathbb{F}_p^*$. Now we have to distinguish the cases $s+1=0$ and $s+1 \neq 0$. In the latter case, ζ^{1+s} is a non-trivial p-th root of unity, hence

$$\sum_{k=0}^{p-1} (\zeta^{1+s})^k = 0 \quad \Longrightarrow \quad \sum_{k\in\mathbb{F}_p^*} (\zeta^{1+s})^k = -1$$

If $s+1=0$, then $(\zeta^{1+s})^k = 1$ for all k. It follows

$$S(p)^2 = \Big(\frac{-1}{p}\Big)(p-1) - \sum_{s=1}^{p-2}\Big(\frac{s}{p}\Big) = \Big(\frac{-1}{p}\Big)p - \sum_{s=1}^{p-1}\Big(\frac{s}{p}\Big).$$

Now $\sum\limits_{s=1}^{p-1}(\frac{s}{p}) = 0$ (since there are as many quadratic residues as non-residues), which implies

$$S(p)^2 = \Big(\frac{-1}{p}\Big)p, \qquad \text{q.e.d.}$$

b) We make use of the formula

$$(x_1 + x_2 + \ldots + x_r)^q \equiv x_1^q + x_2^q + \ldots + x_r^q \bmod q$$

This follows by induction on r from the binomial theorem and the fact that $q \mid \binom{q}{k}$ for $1 \le k \le q-1$. Applying this to the definition of $S(p)$ we get

$$\begin{aligned} S(p)^q &\equiv \sum_{k\in\mathbb{F}_p^*}\Big(\frac{k}{p}\Big)\zeta^{qk} \equiv \sum_{k\in\mathbb{F}_p^*}\Big(\frac{qqk}{p}\Big)\zeta^{qk} \equiv \qquad [\text{Subst. } s = qk] \\ &\equiv \sum_{s\in\mathbb{F}_p^*}\Big(\frac{q}{p}\Big)\Big(\frac{s}{p}\Big)\zeta^{s} \equiv \Big(\frac{q}{p}\Big)S(p) \bmod q, \quad \text{q.e.d.} \end{aligned}$$

8.7. Theorem (Quadratic reciprocity law of Gauss). *Let $p \neq q$ be odd primes. Then*

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

In other words,

$$\begin{aligned} \Big(\frac{p}{q}\Big) &= \Big(\frac{q}{p}\Big) && \text{if } p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4, \\ \Big(\frac{p}{q}\Big) &= -\Big(\frac{q}{p}\Big) && \text{if } p \equiv 3 \bmod 4 \text{ and } q \equiv 3 \bmod 4. \end{aligned}$$

Proof. We start with the formula of theorem 8.6.b) and multiply it by $S(p)$.

$$S(p)^{q+1} \equiv \Big(\frac{q}{p}\Big)S(p)^2 \bmod q.$$

Using 8.6.a) for $S(p)^2$ we get

$$\left(\frac{-1}{p}\right)^{(q+1)/2} p^{(q+1)/2} \equiv \left(\frac{q}{p}\right)\left(\frac{-1}{p}\right) p \mod q.$$

Since p is invertible mod q and $(\frac{-1}{p}) = \pm 1$, we can divide both sides by $(\frac{-1}{p})p$ and obtain

$$\left(\frac{-1}{p}\right)^{(q-1)/2} p^{(q-1)/2} \equiv \left(\frac{q}{p}\right) \mod q$$

Now we use theorem 8.4.1 and the Euler criterion 8.3, yielding

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) \mod q.$$

This congruence was derived as a congruence in $\mathbb{Z}[\zeta_p]$, i.e. the difference of the left hand and right hand side is an element of $q\mathbb{Z}[\zeta_p]$. Since $q\mathbb{Z}[\zeta_p] \cap \mathbb{Z} = q\mathbb{Z}$, this is already a congruence in $\mathbb{Z}$. Both sides of the congruence are ± 1 and $q \geq 3$, so we must actually have an equation

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

which is the assertion of the theorem.

8.8. Fermat primes. It is easy to see that if an integer of the form $2^k + 1$ is prime, then k must be a power of 2. Otherwise we could write $k = \ell m$ with $\ell \geq 3$ odd and $m > 1$, and $2^k + 1 = (2^m)^\ell + 1$ is divisible by $2^m + 1$. The numbers

$$F_n := 2^{2^n} + 1$$

were conjectured by Fermat to be primes. This is true for

$$\begin{aligned} F_0 &= 2^1 + 1 = 3, \\ F_1 &= 2^2 + 1 = 5, \\ F_2 &= 2^4 + 1 = 17, \\ F_3 &= 2^8 + 1 = 257, \\ F_4 &= 2^{16} + 1 = 65537, \end{aligned}$$

but already Euler showed that $F_5 = 2^{32} + 1 = 4\,294\,967\,297$ is divisible by 641. Until today, no Fermat prime F_n with index $n \geq 5$ was found. In order to derive a criterion for the primality of F_n, we first prove:

If F_n is prime, $(n \geq 1)$, then $\left(\frac{3}{F_k}\right) = -1.$

Since $F_n \equiv 1 \bmod 4$, the reciprocity law implies $(\frac{3}{F_n}) = (\frac{F_n}{3})$. We have the following congruence modulo 3

$$F_n = 2^{2^n} + 1 \equiv (-1)^{2^n} + 1 \equiv 2 \bmod 3.$$

Therefore $(\frac{3}{F_n}) = (\frac{2}{3}) = -1$, q.e.d.

8.9. Theorem (Pepin 1877). *The number $F_n = 2^{2^n} + 1$, $(n \geq 1)$, is prime iff*

$$3^{(F_n-1)/2} \equiv -1 \bmod F_n.$$

Proof. The necessity of this condition follows from the Euler criterion (theorem 8.3).

Suppose now that the condition is satisfied. Then $3^{F_n-1} \equiv 1 \bmod F_n$, hence the order of 3 in the multiplicative group $(\mathbb{Z}/F_n)^*$ is a divisor of $F_n - 1 = 2^{2^n}$. From $3^{(F_n-1)/2} \equiv -1$ it follows that $\mathrm{ord}_{(\mathbb{Z}/F_n)^*}(3) = 2^{2^n}$. Therefore $(\mathbb{Z}/F_n)^*$ must have at least $2^{2^n} = F_n - 1$ elements. This shows that F_n is prime.

Remark. Since $(F_n - 1)/2 = 2^{2^n-1}$, the calculation of $3^{(F_n-1)/2} \bmod F_n$ requires $2^n - 1$ squarings mod F_n. The number F_n has $2^n + 1$ binary digits.

8.10. Theorem. *Every possible prime divisor of F_n, $n \geq 5$, has the form*

$$p = h \cdot 2^{n+2} + 1$$

with an integer h.

Example. The prime divisor 641 of F_5, which was found by Euler, is in fact of this form:

$$641 = 5 \cdot 128 + 1 = 5 \cdot 2^{5+2} + 1.$$

Proof. If $p \mid F_n = 2^{2^n} + 1$, then

$$2^{2^n} \equiv -1 \bmod p \quad \Longrightarrow \quad 2^{2^{n+1}} \equiv 1 \bmod p.$$

This shows that the element 2 mod p in $\mathbb{F}_p^*$ has order 2^{n+1}; in particular we have $2^{n+1} \mid (p-1)$. It follows that $p \equiv 1 \bmod 8$, hence by theorem 8.4.2

$$\left(\frac{2}{p}\right) = 1.$$

Therefore there exists an element $x \in \mathbb{F}_p^*$ such that $x^2 \equiv 2 \bmod p$. This element has order 2^{n+2} in $\mathbb{F}_p^*$, hence $2^{n+2} \mid (p-1)$, which implies the assertion of the theorem.

8.11. Proposition. *Every pair of Fermat numbers F_n, F_m, $n \neq m$, is relatively prime, i.e.*

$$\gcd(F_n, F_m) = 1.$$

Proof. We may assume $n < m$. If F_n and F_m were not relatively prime, there would exist a common prime divisor p of F_n and F_m. Then

$$2^{2^n} \equiv -1 \bmod p \quad \text{and} \quad 2^{2^m} \equiv (2^{2^n})^{2^{m-n}} \equiv -1 \bmod p,$$

which is a contradiction.

8.12. The Jacobi symbol. If one wants to apply the reciprocity law to calculate the Legendre symbol $(\frac{a}{p})$, the argument a has to be decomposed into a product of primes. This may be difficult for large a. To overcome this difficulty, Jacobi has defined a generalization of the Jacobi symbol. Let m be an odd number ≥ 3 and

$$m = p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

a prime factorization of m. (The primes p_i are not necessarily distinct.) Then for $a \in \mathbb{Z}$ the Jacobi symbol is defined by

$$\Big(\frac{a}{m}\Big) := \prod_{i=1}^{r} \Big(\frac{a}{p_i}\Big).$$

The following properties follow immediately from the corresponding properties of the Legendre symbol:

$$\begin{aligned}
\Big(\frac{a}{m}\Big) &= \Big(\frac{b}{m}\Big) && \text{if } a \equiv b \bmod m,\\
\Big(\frac{ab}{m}\Big) &= \Big(\frac{a}{m}\Big)\Big(\frac{b}{m}\Big) && \text{for all } a, b \in \mathbb{Z},\\
\Big(\frac{a}{m}\Big) &= 0 \iff && \gcd(a, m) > 0.
\end{aligned}$$

Note however the following difference to the Legendre symbol: $(\frac{a}{m}) = 1$ is a necessary, but in general not sufficient condition for a to be a quadratic residue modulo m. For example,

$$\Big(\frac{2}{15}\Big) = \Big(\frac{2}{3}\Big)\Big(\frac{2}{5}\Big) = (-1)(-1) = 1,$$

but 2 is not a quadratic residue modulo 15.

8.13. Lemma. *For an odd integer $x \in \mathbb{Z}$ define $\varepsilon(x), \omega(x) \in \mathbb{Z}/2$ by*

$$\varepsilon(x) := \frac{x-1}{2} \bmod 2, \qquad \omega(x) := \frac{x^2-1}{8} \bmod 2.$$

Then ε and ω induce group homomorhisms

$$\varepsilon : (\mathbb{Z}/4)^* \longrightarrow \mathbb{Z}/2 \quad \text{and} \quad \omega : (\mathbb{Z}/8)^* \longrightarrow \mathbb{Z}/2$$

from the multiplicative groups $(\mathbb{Z}/4)^*$ *and* $(\mathbb{Z}/8)^*$ *to the additive group* $\mathbb{Z}/2$.

Proof. It is clear that $\varepsilon(x)$ depends only on x mod 4 and $\omega(x)$ depends only on x mod 8 and we have

x	1	3
$\varepsilon(x)$	0	1

x	1	3	5	7
$\omega(x)$	0	1	1	0

The formulas $\varepsilon(xy) = \varepsilon(x) + \varepsilon(y)$ and $\omega(xy) = \omega(x) + \omega(y)$ can be easily checked by a complete case distinction.

8.14. Theorem (Reciprocity law for the Jacobi symbol). *Let* $m \geq 3$ *be an odd integer. Then*

a) (1^{st} supplement)

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2} = \begin{cases} +1, & \text{if } m \equiv 1 \bmod 4, \\ -1, & \text{if } m \equiv 3 \bmod 4, \end{cases}$$

b) (2^{nd} supplement)

$$\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8} = \begin{cases} +1, & \text{if } m \equiv \pm 1 \bmod 8, \\ -1, & \text{if } m \equiv \pm 3 \bmod 8. \end{cases}$$

c) (reciprocity law) *If* $k \geq 3$ *is another odd integer which is coprime to* m, *then*

$$\left(\frac{k}{m}\right)\left(\frac{m}{k}\right) = (-1)^{\frac{k-1}{2}\cdot\frac{m-1}{2}}.$$

Proof. Let $m = p_1 \cdot \ldots \cdot p_r$ be a decomposition of m into a product of primes.

a) By definition we have

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^{r}\left(\frac{-1}{p_i}\right) = \prod_{i=1}^{r}(-1)^{(p_i-1)/2} = (-1)^{\sum \varepsilon(p_i)},$$

where ε was defined in the preceding lemma. By the same lemma,

$$\sum \varepsilon(p_i) \equiv \varepsilon\Big(\prod p_i\Big) \equiv \varepsilon(m) \bmod 2,$$

hence

$$\left(\frac{-1}{m}\right) = (-1)^{\varepsilon(m)} = (-1)^{(m-1)/2}.$$

b) Similarly,

$$\begin{aligned}\left(\frac{2}{m}\right) &= \prod_{i=1}^{r}\left(\frac{2}{p_i}\right) = \prod_{i=1}^{r}(-1)^{(p_i^2-1)/8} = (-1)^{\sum \omega(p_i)} \\ &= (-1)^{\omega(m)} = (-1)^{(m^2-1)/8}.\end{aligned}$$

c) Let $k = q_1 \cdot \ldots \cdot q_s$ be a prime decomposition of k. Then by definition and the reciprocity law for the Legendre symbol

$$\Big(\frac{k}{m}\Big)\Big(\frac{m}{k}\Big) = \prod_{i,j}\Big(\frac{q_j}{p_i}\Big)\Big(\frac{p_i}{q_j}\Big) = \prod_{i,j}(-1)^{\varepsilon(q_j)\varepsilon(p_i)} = (-1)^{\sum_{i,j}\varepsilon(q_j)\varepsilon(p_i)}$$

Now

$$\sum_{i,j}\varepsilon(q_j)\varepsilon(p_i) \equiv \Big(\sum_j \varepsilon(q_j)\Big)\Big(\sum_i \varepsilon(p_i)\Big) \equiv \varepsilon(k)\varepsilon(m) \equiv \frac{k-1}{2}\cdot\frac{m-1}{2} \bmod 2,$$

which proves the theorem.

8.15. Algorithm for the Jacobi symbol. The reciprocity law can be applied to get an efficient algorithm to calculate the Jacobi symbol. Suppose we want to calculate $(\frac{a}{m})$ with $m \geq 3$ odd and $a \in \mathbb{Z}$. In a similar way as for the Euclidean algorithm, set

$$x_0 := a, \quad x_1 := m$$

We now define inductively integers $x_2, x_3, \ldots x_k$ until we arrive at $x_k \in \{0,1\}$. To get x_i from x_{i-2}, x_{i-1} we divide x_{i-2} by x_{i-1} with rest

$$x_{i-2} = q_{i-1}x_{i-1} + y_i, \quad 0 \leq y_i < x_{i-1}.$$

If $y_i = 0$, we stop. Otherwise we write $y_i = 2^{t_i}x_i$ with x_i odd; if $x_i = 1$, we stop, otherwise we continue. In this way we get a chain of equations

$$\begin{aligned}
x_0 &= q_1x_1 + 2^{t_1}x_2,\\
x_1 &= q_2x_2 + 2^{t_2}x_3,\\
\vdots &\qquad \vdots\\
x_{i-1} &= q_ix_i + 2^{t_i}x_{i+1},\\
\vdots &\qquad \vdots\\
x_{k-1} &= q_kx_k + 2^{t_k}x_{k+1},
\end{aligned}$$

where $x_i \geq 3$ odd for all $1 \leq i \leq k$ and $x_{k+1} = 0$ or 1. We show now how one can reduce the calculation of $(\frac{x_{i-1}}{x_i})$ to the calculation of $(\frac{x_i}{x_{i+1}})$ for $i = 1, 2, \ldots$. We have for all $i \leq k$

$$\Big(\frac{x_{i-1}}{x_i}\Big) = \Big(\frac{2}{x_i}\Big)^{t_i}\Big(\frac{x_{i+1}}{x_i}\Big) = (-1)^{t_i\omega(x_i)}\Big(\frac{x_{i+1}}{x_i}\Big),$$

where $\omega(x)$ was defined in lemma 8.13. If $i = k$, we have $x_{i+1} = 0, 1$ and we can stop. Else we have $x_i \geq 3$ odd, so we can apply the quadratic reciprocity theorem to get

$$\Big(\frac{x_{i+1}}{x_i}\Big) = (-1)^{\varepsilon(x_i)+\varepsilon(x_{i+1})}\Big(\frac{x_i}{x_{i+1}}\Big),$$

yielding

$$\left(\frac{x_{i-1}}{x_i}\right) = (-1)^{t_i\omega(x_i)+\varepsilon(x_i)+\varepsilon(x_{i+1})}\left(\frac{x_i}{x_{i+1}}\right).$$

This is the desired recursion relation which allows to calculate the Jacobi symbol $(\frac{a}{m}) = (\frac{x_0}{x_1})$ in k steps. As in the case of the Euclidean algorithm the complexity is $O(\log m)$.