Selected topics of undergraduate mathematics leading to research: Artin's Conjecture, quadratic reciprocity, a primality test, and more general reciprocity laws

Gabor Wiese
gabor.wiese@uni.lu

16th July 2021

Abstract

These is a preliminary version of the beginning of notes for a lecture delivered remotely to undergraduate students at the Southeast University Nanjing, Jiangsu, in China on 14 and 16 July 2021.

The notes are still under construction and will still change. Any remarks are welcome!

1 Some aspects of elementary number theory

The purpose of this first section is to survey the most basic concepts from elementary number theory.

We start with *Euclidean division*, i.e. division with remainder:
For any $n, d \in \mathbb{Z}$ with $d \neq 0$ there are unique $q, r \in \mathbb{Z}$ such that

$$n = qd + r \text{ with } 0 \leq r \leq d-1.$$

We write

$$(d) = d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\}$$

for the *(principal) ideal of $\mathbb{Z}$ generated by d*, which is simply the set of all multiples of d. In view of the division with remainder, we have a partition of $\mathbb{Z}$ in cosets with respect to the possible remainders:

$$\mathbb{Z} = \bigsqcup_{r=0}^{d-1} r + (d) = \bigsqcup_{r=0}^{d-1} r + d\mathbb{Z} = \bigsqcup_{r=0}^{d-1} \{r + dn \mid n \in \mathbb{Z}\}.$$

Sometimes it is useful to write $\overline{r} = r + (d)$. We can add and multiply these cosets with the following simple formulas:

$$\big(r + (d)\big) + \big(s + (d)\big) = (r+s) + (d) \text{ or alternatively: } \overline{r} + \overline{s} = \overline{r+s}$$

$$\big(r+(d)\big)\cdot\big(s+(d)\big) = (r\cdot s)+(d) \text{ or alternatively: } \overline{r}\cdot\overline{s} = \overline{r\cdot s}$$

We write

$$\mathbb{Z}/(d) = \mathbb{Z}/d\mathbb{Z} = \{\overline{r} \mid 0 \le r \le d-1\} = \{r+d\mathbb{Z} \mid 0 \le r \le d-1\}$$

for the set of these cosets, which is in fact a commutative ring with respect to the addition and multiplication above. The neutral element for addition is $\overline{0}$ and the one for multiplication $\overline{1}$. If $r+(d) = s+(d)$ then we also write $r \equiv s \bmod d$ and say that r and s are congruent modulo d.
We have the following useful formulae for ideals:

$$(d,e) = (\gcd(d,e)) \text{ and } (d)\cap(e) = (\operatorname{lcm}(d,e))$$

for $d, e \in \mathbb{Z}$, where (d,e) is the ideal of $\mathbb{Z}$ generated by d, e, i.e. $(d,e) = \{dm+en \mid m,n \in \mathbb{Z}\}$.
In this lecture we make the convention that *ring* means *commutative ring*, unless explicitly stated otherwise.

Definition 1.1. *Let R be a ring. By $R^\times$ we denote the set of units of R, i.e. the elements $x \in R$ such that there is $y \in R$ with $1 = xy$. In that case, we write $y = x^{-1}$. The units form a group under multiplication: the* unit group *of R.*

The way we present elementary number theory here is that its most fundamental concept is that of Euclid's algorithm.

Theorem 1.2 (Euclid, Bézout)**.** *Let $a, b \in \mathbb{Z}$ not both zero. Then* Euclid's algorithm *computes the greatest common divisor d of a, b, notation $d = \gcd(a,b)$, that is:*

- $d \ge 1$,
- $d \mid a$, $d \mid b$,
- *for any $e \ge 1$ such that $e \mid a$ and $e \mid b$, one has $e \mid d$.*

Moreover, the extended Euclid's algorithm *gives $r, s \in \mathbb{Z}$ such that*

$$d = ar + bs.$$

The proof is completely algorithmic. We do not recall the algorithm here. One can/should use Euclid's algorithm to compute modular inverses.

Lemma 1.3. *Let $d \in \mathbb{Z}$ with $d \neq 0$. Let $r \in \mathbb{Z}$. Then*

$$\overline{r} \in (\mathbb{Z}/(d))^\times \Leftrightarrow \gcd(r,d) = 1.$$

Proof. '$\Rightarrow$': There is $s \in \mathbb{Z}$ such that $\overline{r}\cdot\overline{s} = \overline{rs} = \overline{1}$. This means $1 = rs + ad$ for some $a \in \mathbb{Z}$. Hence, any common divisor of r and d divides 1, whence $\gcd(r,d) = 1$.
'$\Leftarrow$': As $\gcd(r,d) = 1$, we have $(1) = \mathbb{Z} = (r,d)$. There are thus $a, s \in \mathbb{Z}$ such that $1 = rs + ad$. Consequently, $\overline{r}\cdot\overline{s} = \overline{rs} = \overline{1}$. □

We immediately obtain the following corollary.

Corollary 1.4. *Let $d \in \mathbb{Z}$ with $d > 0$. Then the following statement are equivalent.*

(i) $\mathbb{Z}/d\mathbb{Z}$ *is a field.*

(ii) $(\mathbb{Z}/d\mathbb{Z})^\times = \mathbb{Z}/d\mathbb{Z} \setminus \{\overline{0}\}$.

(iii) d *is a prime number.*

If p is a prime number, we shall also write

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/(p).$$

Moreover, when working with $\mathbb{Z}/(d)$, we shall often drop the bar from the notation and simply write, for example, 1 for $\overline{1}$.
Also the following famous theorem is based on the extended Euclid's algorithm.

Theorem 1.5 (Chinese Remainder Theorem)**.** *Let $n, m \in \mathbb{N}$ such that* $\gcd(n, m) = 1$. *Then the map*

$$\Phi : \mathbb{Z}/(nm) \to \mathbb{Z}/(n) \times \mathbb{Z}/(m), \quad a + (nm) \mapsto \big(a + (n), a + (m)\big)$$

is an isomorphism of rings.

Proof. The homomorphism property is easily checked.
Injectivity: Suppose $a \in \mathbb{Z}$ is in (n) and in (m). This means that $n \mid a$ and $m \mid a$. As $\gcd(n, m) = 1$, it follows $nm \mid a$, which means $a \in (nm)$, showing the injectivity.
Surjectivity: As $\gcd(n, m) = 1$, there are $x, y \in \mathbb{Z}$ such that $1 = nx + my$. We just have to interpret this equation in the right way. It means that $N := nx = 1 - my$ satisfies:

$$N \equiv 0 \mod (n) \text{ and } N \equiv 1 \mod (m).$$

In the same way we have that $M := my = 1 - nx$ satisfies:

$$M \equiv 0 \mod (m) \text{ and } M \equiv 1 \mod (n).$$

Let $b, c \in \mathbb{Z}$ and consider $\big(b + (n), c + (m)\big) \in \mathbb{Z}/(n) \times \mathbb{Z}/(m)$. Then $a := bM + cN$ is an element such that

$$a \equiv b \mod (n) \text{ and } a \equiv c \mod (m),$$

i.e. $\Phi(a + (nm)) = \big(b + (n), c + (m)\big)$, showing the surjectivity. □

By iterating the theorem, we obtain the following corollary.

Corollary 1.6. *Let $N = \prod_{i=1}^{k} p_i^{n_i}$ be the decomposition of $N \in \mathbb{N}$ into coprime powers of prime numbers. Then there is the isomorphism:*

$$\Psi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z},$$

sending $a + (N)$ to $\big(a + (p_1^{n_1}), \ldots, a + (p_k^{n_k})\big)$.

Definition 1.7. *Let $n \geq 1$ be an integer. Let*

$$\varphi(n) = |\big(\mathbb{Z}/(n)\big)^\times|,$$

the order of the unit group of the ring $\mathbb{Z}/(n)$, that is, the number of units of $\mathbb{Z}/(n)$. One calls φ Euler's totient function (or: Euler's φ-function).

Lemma 1.8. *Let $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$ be the factorisation of n into prime powers with pairwise distinct prime numbers $p_1, \ldots, p_r$.*
Then $\varphi(n) = (p_1 - 1)p_1^{e_1 - 1} \cdot (p_2 - 1)p_2^{e_2 - 1} \cdot (p_r - 1)p_r^{e_r - 1}$.

Proof. By the Chinese Remainder Theorem 1.5 it suffices to prove $\varphi(p^e) = (p-1)p^{e-1}$ for any prime number p.
In fact, it turns out to be easier to count non-units in $\mathbb{Z}/(p^e)$ instead of counting units. The non-units in $\mathbb{Z}/(p^e)$ are precisely the classes $a+(p^e)$ such that $p \mid a$, that is, $0, p, 2p, \ldots, (p^{e-1} - 1)p$. So, there are p^{e-1} non-units. Hence, $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$. □

Lemma 1.9. *(a) Let $m \in \mathbb{N}_{\geq 2}$. There is a group isomorphism*

$$(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}.$$

The factors are generated by the classes of -1 and 5 in $(\mathbb{Z}/2^m\mathbb{Z})^\times$, respectively.

(b) Let $p > 2$ be a prime number and $m \in \mathbb{N}_{\geq 1}$. There is a group isomorphism

$$(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{p-1}\mathbb{Z}.$$

Proof. Exercise. □

Now we need to recall some statements from group theory.

Theorem 1.10 (Lagrange)**.** *Let G be a finite group and $H \leq G$ a subgroup. Denote by $(G : H)$ the index of H in G and by $|G|$ (and $|H|$) the order of G (and H). Then*

$$|G| = |H| \cdot (G : H).$$

Proof. Let us denote by $\circ$ the group operation. As abbreviation write $r = (G : H)$. Then by definition there are r cosets, say, $g_1 \circ H, g_2 \circ H, \ldots, g_r \circ H$ such that

$$G = g_1 \circ H \sqcup g_2 \circ H \sqcup \cdots \sqcup g_r \circ H,$$

where the symbol $\sqcup$ means 'disjoint union'. Now note that

$$H \to g_i \circ H, \quad x \mapsto g_i \circ x$$

defines a bijection, so that the number of elements of H and $g_i \circ H$ are equal. Thus, $|G| = r|H|$. □

Corollary 1.11. *Let G be a finite group and $g \in G$ an element. The* order $\mathrm{ord}(g)$ *is the smallest positive $n \in \mathbb{Z}$ such that $e = g^n$ (that is, $\underbrace{g \circ g \circ \cdots \circ g}_{n\text{-times}}$), where e is the neutral element in G. Denote by $\langle g \rangle$ the smallest subgroup of G containing g.*
Then $\mathrm{ord}(g) = |\langle g \rangle|$ *divides* $|G|$ *and* $g^{|G|} = e$.

Proof. Let $H = \langle g \rangle$. We obviously have $|H| = \mathrm{ord}(g)$. Hence, Theorem 1.10 gives $\mathrm{ord}(g)$ divides $|G|$, say, $|G| = \mathrm{ord}(g) \cdot m$ for some $m \geq 1$. Then

$$g^{|G|} = g^{\mathrm{ord}(g) \cdot m} = \left(g^{\mathrm{ord}(g)}\right)^m = e^m = e,$$

finishing the proof. □

Corollary 1.12 ('Little Fermat'). *Let p be a prime number. Let $m \in \mathbb{Z}$ be an integer such that $m \equiv 1 \mod (p-1)$.*
Then for any $x \in \mathbb{F}_p$ one has: $x^m = x$ (equality in $\mathbb{F}_p$).

Proof. The group of units of $\mathbb{F}_p$ has order $p-1$ as the only non-unit is (the class of) 0. Let $0 \neq x \in \mathbb{F}_p$. By Corollary 1.11, $x^{p-1} = 1$. We have $m = 1 + (p-1)r$ for some $r \in \mathbb{Z}$. Thus:

$$x^m = x^{1+(p-1)r} = x \cdot x^{(p-1)r} = x \cdot \left(x^{p-1}\right)^r = x \cdot 1^r = x.$$

For $x = 0$ we obviously also have $x^m = 0^m = 0 = x$. □

Next we continue with some group theory that will be needed for understanding the multiplicative group of a finite field.

Lemma 1.13. *Let A be a finite abelian group. The* exponent $\exp(A)$ of A *is defined as the minimal positive integer e such that $a^e = 1$ for all elements $a \in A$. Then the following statements hold:*

(a) Let $a, b \in A$. Suppose that $1 = \gcd(\mathrm{ord}(a), \mathrm{ord}(b))$, then $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$.

(b) Let $a, b \in A$. Then there are $i, j \in \mathbb{N}$ such that $\mathrm{ord}(a^i b^j) = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$.

(c) There is $a \in A$ such that $\mathrm{ord}(a) = \exp(A)$.

(d) A is cyclic $\Leftrightarrow \exp(A) = \#A$.

Proof. (a) Let $e \geq 1$ such that $a^e b^e = 1$. Since $1 = \gcd(\mathrm{ord}(a^e), \mathrm{ord}(b^e))$, it follows from $a^e = b^{-e}$ that $a^e = 1 = b^e$. Thus, $\mathrm{ord}(a) \mid e$ and $\mathrm{ord}(b) \mid e$, hence, $\mathrm{ord}(a)\,\mathrm{ord}(b) = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b)) \mid e$. Of course, $(ab)^{\mathrm{ord}(a)\,\mathrm{ord}(b)} = 1$.
(b) Let

$$\mathrm{ord}(a) = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k} \text{ and } \mathrm{ord}(b) = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$$

be the prime factorisations (i.e. the $p_1, \ldots, p_k$ are pairwise distinct prime numbers), where we sort the primes in such a way that $m_1 \geq n_1, \ldots, m_s \geq n_s$ and $m_{s+1} < n_s, \ldots, m_k < n_k$. Let

$$a' := a^{p_{s+1}^{m_{s+1}} \cdot \ldots \cdot p_k^{m_k}} \text{ and } b' := b^{p_1^{n_1} \cdot \ldots \cdot p_s^{n_s}}.$$

It is clear that we have

$$\mathrm{ord}(a') = p_1^{m_1} \cdot \ldots \cdot p_s^{m_s} \text{ and } \mathrm{ord}(b') = p_{s+1}^{n_{s+1}} \cdot \ldots \cdot p_k^{n_k}.$$

Hence, (a) implies that the order of $a'b'$ is

$$p_1^{m_1} \cdot \ldots \cdot p_s^{m_s} \cdot p_{s+1}^{n_{s+1}} \cdot \ldots \cdot p_k^{n_k} = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b)).$$

Of course, $(ab)^{\mathrm{lcm}(\mathrm{ord}(a),\mathrm{ord}(b))} = 1$.
(c) Let e denote the lowest common multiple of the orders of all elements in A. It is an immediate consequence of (b) that there is an element $a \in A$ whose order is e. So, $e = \mathrm{ord}(a) \mid \exp(A)$. Clearly, $\exp(A)$ is less than or equal to e, showing the desired equality.
(d) is an immediate consequence of (c). □

Proposition 1.14. *Let K be a finite field. Then the group of units $K^\times = K \setminus \{0\}$ (group with respect to multiplication and neutral element 1) is a cyclic group of order $|K| - 1$.*

Proof. Let $e := \exp(K^\times)$. Due to Lemma 1.13 it suffices to show that $e = |K| - 1$. Suppose $e < |K| - 1$. Then every element $a \in K$ satisfies $a^{e+1} = a$, so that the $|K|$ elements are all zeros of the polynomial $X^{e+1} - X$, which has degree $e + 1$. This is, of course, impossible because a polynomial of degree $e + 1$ has at most $e + 1$ zeros (since the coefficients of the polynomial are in a field). □

2 Artin's Conjecture on Primitive Roots

This part contains material provided by Antonella Perucca.
Let p be a prime number. For $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$, i.e. such that $a \in \mathbb{F}_p^\times$, we refer to the order of a in the 'multiplicative' group $\mathbb{F}_p^\times$ as *the multiplicative order of a* mod p.
Here is a table of the multiplicative order of 2 mod p.

p odd prime											
order of (2 mod p)											
3	5	7	11	13	17	19	23	29	31	37	41
2	4	3	10	12	8	18	11	28	5	36	20

43	47	53	59	61	67	71	73	79	83	89	97	...
14	23	52	58	60	66	35	9	39	82	11	48	...

Remark 2.1. *(a) One value can be repeated at most finitely many times.*

For, if $\mathrm{ord}(2 \bmod p) = n$, *then* $p \mid (2^n - 1)$, *hence there are only finitely many such p.*

(b) Not all positive integers appear in the sequence:

For instance, $\mathrm{ord}(2 \bmod p) \neq 6$ *because* $2^6 - 1 = 3^2 \times 7$, *but for* $p = 3, 7$, *the order is not* 6.

Next we consider the index of $(2 \bmod p)$. That is, the quotient of $p-1$ divided by the multiplicative order.

p odd prime											
index of $(2 \bmod p)$											
3	5	7	11	13	17	19	23	29	31	37	41
1	1	2	1	1	2	1	2	1	6	1	2

43	47	53	59	61	67	71	73	79	83	89	97	...
3	2	1	1	1	1	2	8	2	1	8	2	...

We next include some results on the multiplicative order.

Theorem 2.2 (Bang, 1886). *Let $a \neq 0, \pm 1$. Then for every $n > 0$ there exists p such that $\operatorname{ord}(a \bmod p) = n$, with the following exceptions:*

$a = 2$	$n = 1, 6$
$a = 2^h - 1$	$n = 2$
$a = -2$	$n = 2, 3$
$a = -(2^h + 1)$	$n = 1$

Theorem 2.3 (Schinzel, 1975). *Let $a \neq 0$. Then a is determined by the family*

$$\left\{ \operatorname{ord}(a \bmod p) \right\}_{p \in S}$$

where S is any set containing all but finitely many primes p.

Conjecture 2.4 (Artin's primitive root conjecture (1927)). *Let $a \neq 0, \pm 1$ and not a square. There exist infinitely many primes p such that the multiplicative index of $(a \bmod p)$ is 1.*

Artin's Conjecture is still open. But, it has been proved under the assumption of the Generalised Riemann Hypothesis.

3 Legendre symbol

Let p be a prime number. This section is about the squares in $\mathbb{F}_p \setminus \{0\}$. We first show that for $p > 2$, exactly half the elements of $\mathbb{F}_p \setminus \{0\}$ are squares.

Lemma 3.1. *Let $p > 2$ be a prime number. There are $\frac{p-1}{2}$ squares in $\mathbb{F}_p^\times$ (a square in $\mathbb{F}_p^\times$ is an element a such that there is $b \in \mathbb{F}_p^\times$ such that $a = b^2$) and there are equally many nonsquares.*

Proof. We consider the group homomorphism

$$\varphi : \mathbb{F}_p^\times \xrightarrow{x \mapsto x^2} \mathbb{F}_p^\times.$$

Its kernel is clearly $\{-1, 1\}$ and its image is the set of squares $\mathbb{F}_p^{\times 2}$ in $\mathbb{F}_p^\times$. Thus the homomorphism theorem (1st isomorphism theorem) gives the isomorphism

$$\overline{\varphi} : \mathbb{F}_p^\times / \{1, -1\} \cong \mathbb{F}_p^{\times 2},$$

from which the claimed formula follows. □

Definition 3.2. *Let $N \in \mathbb{N}_{\geq 1}$. An integer $a \in \mathbb{Z}$ is called* quadratic residue modulo N *if there is $b \in \mathbb{Z}$ such that*

$$a \equiv b^2 \mod N.$$

Otherwise, we call it a quadratic nonresidue.

Lemma 3.3. *(a) Let $N \in \mathbb{N}_{\geq 1}$. Whether or not a is a quadratic residue modulo N only depends on the class of a in $\mathbb{Z}/N\mathbb{Z}$.*

(b) Suppose $N = \prod_{i=1}^{k} p_i^{n_i}$ in its factorisation into prime powers (that is, the p_i are distinct primes).

Then a is a quadratic residue modulo N if and only if it is a quadratic residue modulo $p_i^{n_i}$ for all $i \in \{1, \ldots, k\}$.

(c) Let $p > 2$ be a prime number, $n \in \mathbb{N}_{\geq 1}$ and $a \in \mathbb{Z}$ such that $p \nmid a$. Then the following statements are equivalent:

(i) a is a quadratic residue modulo p^n.

(ii) a is a quadratic residue modulo p.

(d) Let $a \in \mathbb{Z}$ be odd. Then the following statements are equivalent:

(i) a is a quadratic residue modulo 2^n.

(ii) $n = 1$ or ($n = 2$ and $a \equiv 1 \mod 4$) or ($n \geq 3$ and $a \equiv 1 \mod 8$).

Proof. (a) is clear since it is an assertion about the ring $\mathbb{Z}/N\mathbb{Z}$.
(b) We use Corollary 1.6 of the Chinese Remainder Theorem and its notation.
'$\Rightarrow$': If $a = b^2$, then $a_i = b_i^2$ for all $i \in \{1, \ldots, k\}$, showing that a_i is a square modulo $p_i^{n_i}$.
'$\Leftarrow$': Suppose now $a_i = b_i^2$ for all $i \in \{1, \ldots, k\}$. Then $\Psi(a) = (a_1, \ldots, a_k) = (b_1^2, \ldots, b_k^2) = \Psi(b^2)$.
(c) '(i) $\Leftarrow$ (ii)': If $a \equiv b^2 \mod p^n$, that is, $p^n \mid (b^2 - a)$, hence $p \mid (b^2 - a)$, thus $a \equiv b^2 \mod p$.
'(ii) $\Rightarrow$ (i)': Suppose $a \equiv b^2 \mod p$. As $p \nmid a$, it follows $p \nmid b$, thus b is a unit in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Hence, there is $c \in \mathbb{Z}$ such that $a \equiv b^2 c \mod p^n$ and $c \equiv 1 \mod p$.
Claim: For all $i \geq 0$ we have $c^{p^i} \equiv 1 \mod p^{i+1}$.
We show that claim by induction. The case $i = 0$ is true by assumption. Suppose the assertion is true for i, we want to prove it for $i + 1$. So, we know $c^{p^i} = 1 + p^{i+1}x$ for some $x \in \mathbb{Z}$. We take the p-th power and expand it

$$c^{p^{i+1}} = (c^{p^i})^p = (1 + p^{i+1}x)^p = \sum_{k=0}^{p} \binom{p}{k} p^{(i+1)k} x^k$$
$$= 1 + \binom{p}{1} p^{i+1}x + \sum_{k=2}^{p} \binom{p}{k} p^{(i+1)k} x^k \equiv 1 \mod p^{i+2}.$$

Thus, $c^{p^{n-1}} \equiv 1 \mod p^n$. We exploit this as follows. Set $d := c^{\frac{p^{n-1}+1}{2}}$. Then

$$d^2 = (c^{\frac{p^{n-1}+1}{2}})^2 = c^{p^{n-1}+1} = c^{p^{n-1}} \cdot c \equiv c \mod p^n.$$

Hence, $a \equiv b^2 c \equiv b^2 d^2 = (bd)^2 \mod p^n$.
(d) '(i) $\Rightarrow$ (ii)': Let $a = 2m+1$ be any odd number (with $m \in \mathbb{Z}$). Then its square is congruent to 1 modulo 8 (hence also 1 modulo 4 and 1 modulo 2):

$$a^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 4m(m+1) + 1 \equiv 1 \mod 8,$$

where we used that $m(m+1)$ is necessarily even as it is the product of two consecutive integers.
'(ii) $\Rightarrow$ (i)': The cases $n = 1$ and $n = 2$ are trivial as $1 = 1^2$ is a square. Let us hence assume $n \geq 3$ and $a \equiv 1 \mod 8$. From Lemma 1.9 it follows that $a \equiv 5^{2k} \mod 2^n$ for some $k \in \mathbb{N}$: in general we know $a \equiv (-1)^r 5^s \mod 2^n$ for some $r, s \in \mathbb{Z}$; thus $1 \equiv a \equiv (-1)^r 5^s \mod 8$, implying $2 \mid r$ and $2 \mid s$. □

This lemma reduces the calculation whether or not a is a quadratic residue modulo N to the calculation whether or not a is a quadratic residue modulo p for the primes p dividing N. This leads to the introduction of the Legendre symbol.

Definition 3.4. *Let $p > 2$ be a prime number and $a \in \mathbb{Z}$. The* Legendre symbol *is defined as*

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

Note that the definition only depends on the class of a modulo p.

Proposition 3.5 (Euler)**.** *Let $p > 2$ be a prime number and $a \in \mathbb{Z}$. Then the congruence*

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

holds.

Proof. If $p \mid a$, the result is straight forward:

$$\left(\frac{a}{p}\right) = 0 \text{ and } a^{\frac{p-1}{2}} \equiv 0^{\frac{p-1}{2}} = 0 \mod p.$$

We now assume $p \nmid a$, that is $a \in \mathbb{F}_p^\times$. We consider the group homomorphism

$$\varphi : \mathbb{F}_p^\times \xrightarrow{x \mapsto x^{\frac{p-1}{2}}} \mathbb{F}_p^\times.$$

Recall that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$ and note that $\varphi(x^2) = (\varphi(x))^2 = x^{p-1} = 1$ for all $x \in \mathbb{F}_p^\times$. This implies that the image is $\{1, -1\} \subseteq \mathbb{F}_p^\times$ and that the squares $\mathbb{F}_p^{\times 2}$ are in the kernel. The homomorphism theorem (1st isomorphism theorem) gives an isomorphism

$$\overline{\varphi} : \mathbb{F}_p^\times / \ker(\varphi) \cong \operatorname{im}(\varphi) = \{-1, 1\},$$

showing that the order of $\ker(\varphi)$ is $\frac{p-1}{2}$. By Lemma 3.1 there are $\frac{p-1}{2}$ squares in $\mathbb{F}_p^\times$, hence $\ker(\varphi) = \mathbb{F}_p^{\times 2}$. This proves the proposition. □

Corollary 3.6. *Let $p > 2$ be a prime number. The Legendre symbol defines a group homomorphism*

$$\mathbb{F}_p^\times \to \{-1, 1\}, \quad a \mapsto \left(\frac{a}{p}\right),$$

the kernel of which is $\mathbb{F}_p^{\times 2}$, the set of squares. In particular, for all $a, b \in \mathbb{Z}$ one has

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

Proof. This follows immediately from Proposition 3.5. □

4 Gauß' reciprocity law

We first state Gauß' reciprocity law. Its proof will be given later.

Theorem 4.1 (Gauß' reciprocity law)**.** *Let $p \neq q$ be two distinct odd prime numbers.*

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

(b) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \mod 8, \\ -1 & \text{if } p \equiv 3, 5 \mod 8. \end{cases}$

(c) $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. *In particular, if $p \equiv 1 \mod 4$ or $q \equiv 1 \mod 4$, then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.*

Let us remark that (a) is a direct consequence of Euler's result Proposition 3.5.

Example 4.2. *In the following examples we apply Gauß' reciprocity law and the fact that the Legendre symbol $\frac{n}{p}$ only depends on the residue class of n modulo p.*

- $\left(\frac{100}{101}\right) = \left(\frac{4 \cdot 25}{101}\right) = \left(\frac{4}{101}\right)\left(\frac{25}{101}\right) = 1 \cdot 1 = 1.$
- $\left(\frac{500}{101}\right) = \left(\frac{4 \cdot 125}{101}\right) = \left(\frac{4}{101}\right)\left(\frac{25}{101}\right)\left(\frac{5}{101}\right) = \left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1.$
- $\left(\frac{127}{31}\right) = \left(\frac{3}{31}\right) = -\left(\frac{31}{3}\right) = -\left(\frac{1}{3}\right) = -1.$

A generalisation of the Legendre Symbol is the Jacobi Symbol. We will use it for primality testing later this term.

Definition 4.3. *Let $m \geq 3$ be an odd natural number and write $m = p_1 \cdot \cdots \cdot p_k$ for its factorisation into (not necessarily distinct) prime numbers. For $a \in \mathbb{Z}$, the* Jacobi symbol *is defined as*

$$\left(\frac{a}{m}\right) := \prod_{i=1}^{k} \left(\frac{a}{p_i}\right),$$

where the Legendre symbol is used on the right hand side.

If m is a prime number, then the Jacobi symbol $\left(\frac{a}{m}\right)$ equals the Legendre symbol. However, if m is not a prime number, then one must not interpret the Jacobi symbol like the Legendre symbol. For instance,

$$\left(\frac{-1}{21}\right) = \left(\frac{-1}{3}\right)\left(\frac{-1}{7}\right) = (-1)\cdot(-1) = 1,$$

but -1 is not a square modulo 21 (see Lemma 3.3).

Lemma 4.4. *Let $m = \prod_{i=1}^{k} p_i \geq 3$ be an odd integer (and the p_i are primes) and let $a, b \in \mathbb{Z}$.*

(a) The Jacobi symbol $\left(\frac{a}{m}\right)$ only depends on the residue class of a modulo m.

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

Proof. (a) This follows immediately from the Chinese Remainder Theorem: If $a \equiv b \mod m$, then $a \equiv b \mod p_i$ for all $i \in \{1, \ldots, k\}$. But we already know for the Legendre symbol that $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$, which gives the assertion.
(b) $\left(\frac{ab}{m}\right) = \prod_{i=1}^{k}\left(\frac{ab}{p_i}\right) = (\prod_{i=1}^{k}\left(\frac{a}{p_i}\right))\cdot(\prod_{i=1}^{k}\left(\frac{a}{p_i}\right)) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$. □

We will now extend Gauß' reciprocity law from the Legendre to the Jacobi symbol. For this we first include a lemma.

Lemma 4.5. *(a) The map*

$$\epsilon : (\mathbb{Z}/4\mathbb{Z})^{\times} \to \{+1, -1\}, \quad m \mapsto (-1)^{\frac{m-1}{2}}$$

is a group homomorphism.

(b) The map

$$w : (\mathbb{Z}/8\mathbb{Z})^{\times} \to \{+1, -1\}, \quad m \mapsto (-1)^{\frac{m^2-1}{8}}$$

is a group homomorphism.

Proof. (a) We have $\frac{mk-1}{2} - \left(\frac{m-1}{2} + \frac{k-1}{2}\right) = 2 \cdot \frac{m-1}{2}\frac{k-1}{2} \equiv 0 \mod 2$. This shows $(-1)^{\frac{mk-1}{2}} = (-1)^{\frac{m-1}{2}}(-1)^{\frac{k-1}{2}}$.
(b) We have $\frac{m^2k^2-1}{8} - \left(\frac{m^2-1}{8} + \frac{k^2-1}{8}\right) = 8 \cdot \frac{m^2-1}{8}\frac{k^2-1}{8} \equiv 0 \mod 2$. This shows $(-1)^{\frac{m^2k^2-1}{8}} = (-1)^{\frac{m^2-1}{8}}(-1)^{\frac{k^2-1}{8}}$. □

Theorem 4.6 (Jacobi's reciprocity law)**.** *Let $m \neq k$ be two distinct odd integers at least 3.*

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

(b) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = w(m)$.

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

Proof. Let $m = \prod_{i=1}^r p_i$ and $k = \prod_{i=1}^s q_i$ be the factorisations of m and k into prime numbers (not necessarily distinct).
(a) $\left(\frac{-1}{m}\right) = \prod_{i=1}^r \left(\frac{-1}{p_i}\right) = \prod_{i=1}^r \epsilon(p_i) = \epsilon(\prod_{i=1}^r p_i) = \epsilon(m)$, where we used Gauß' reciprocity law Theorem 4.1 (a) and Lemma 4.5 (a).
(b) $\left(\frac{2}{m}\right) = \prod_{i=1}^r \left(\frac{2}{p_i}\right) = \prod_{i=1}^r w(p_i) = w(\prod_{i=1}^r p_i) = w(m)$, where we used Gauß' reciprocity law Theorem 4.1 (b) and Lemma 4.5 (b).
(c) We now use Gauß' reciprocity law Theorem 4.1 (c) and Lemma 4.5 (a):

$$\begin{aligned}\left(\frac{k}{m}\right)\left(\frac{m}{k}\right) &= \Big(\prod_{i=1}^r \left(\frac{k}{p_i}\right)\Big)\Big(\prod_{j=1}^s \left(\frac{m}{q_j}\right)\Big) = \Big(\prod_{i=1}^r \prod_{j=1}^s \left(\frac{q_j}{p_i}\right)\Big)\Big(\prod_{j=1}^s \prod_{i=1}^r \left(\frac{p_i}{q_j}\right)\Big) \\ &= \prod_{j=1}^s \prod_{i=1}^r \Big(\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)\Big) = \prod_{j=1}^s \prod_{i=1}^r (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = \prod_{j=1}^s \prod_{i=1}^r \epsilon(p_i)^{\frac{q_j-1}{2}} = \prod_{j=1}^s \epsilon(m)^{\frac{q_j-1}{2}} \\ &= \begin{cases} 1 & \text{if } \epsilon(m) = 1 \\ \prod_{j=1}^s (-1)^{\frac{q_j-1}{2}} = \prod_{j=1}^s \epsilon(q_j) = \epsilon(k) & \text{if } \epsilon(m) = -1 \end{cases}.\end{aligned}$$

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

Example 4.7. $\left(\frac{888}{1999}\right) = \left(\frac{2}{1999}\right)\left(\frac{4}{1999}\right)\left(\frac{111}{1999}\right) = \left(\frac{111}{1999}\right) = -\left(\frac{1999}{111}\right) = -\left(\frac{1}{111}\right) = -1$. *We used that* $1999 \equiv 7 \mod 8$ *(hence* $\left(\frac{2}{1999}\right) = 1$*) and* $111 \equiv 3 \mod 4$, $1999 \equiv 3 \mod 4$, $1999 = 111 \cdot 18 + 1$.
We have thus computed the Legendre symbol $\left(\frac{888}{1999}\right)$ *using the rules of the Jacobi symbol without factoring* 111*, just doing division with remainder. This is an important advantage because it is very hard to factor big numbers in practice!*

5 The Solovay-Strassen primality test

Cryptographic systems like RSA, Diffie-Hellman, El Gamal, etc. need 'big' prime numbers. How does one find 'big' prime numbers? How does one know whether a 'big' number is prime?
A *deterministic primality test* is an algorithm:

Input: $m \in \mathbb{N}_{\geq 2}$
Output: `true` $\Rightarrow$ m is a prime number.
`false` $\Rightarrow$ m is not a prime number.

A *probabilistic primality test* is an algorithm:

Input: $m \in \mathbb{N}_{\geq 2}$
Output: `true` $\Rightarrow$ m is a prime number with 'high probability'.
`false` $\Rightarrow$ m is not a prime number.

A prime number test does *not* compute a factorisation of m. The idea is to decide whether m is a prime number or not *without* factorising m. The reason for this is that factorisation of a big number is in practice often undoable (the security of RSA relies precisely on this). In practice, probabilistic primality tests are usually faster than deterministic ones, and for everyday cryptographic purposes probabilistic tests suffice: if the probability that my banking application is corrupted is less than 10^{-1000}, I shouldn't be worried.

In this section we present the so-called Solovay-Strassen primality test. It is a probabilistic one. Nowadays there are better ones, e.g. the Miller-Rabin test, but the Solovay-Strassen test nicely illustrate how such tests work, and it relies on the Legendre symbol.
Let us first recall that for an odd prime number p, for all $a \in \mathbb{Z}$ such that p does not divide a, we have $a^{\frac{p-1}{2}} \in \{1, -1\} \subseteq \mathbb{F}_p^\times$. This can be turned around to provide a deterministic primality test.

Proposition 5.1. *Let $N \in \mathbb{N}_{\geq 3}$ be odd. Suppose that for all $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ we have $a^{\frac{N-1}{2}} \equiv \pm 1 \mod N$. We suppose that one of the two following statements holds:*

(1) $N \equiv 3 \mod 4$.

(2) There is $b \in (\mathbb{Z}/N\mathbb{Z})^\times$: $b^{\frac{N-1}{2}} \equiv -1 \mod N$.

Then N is a prime number.

Proof. Exercise. □

For this exercise and also the next proof, it is useful to have some statements on so-called *Carmichael numbers*.

Proposition 5.2. *Let $N \in \mathbb{N}_{\geq 3}$ be odd. Suppose that for all $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ we have $a^{N-1} \equiv 1 \mod N$. Such a number is called a* Carmichael number.
Then N is squarefree and for every prime divisor p of N we have that $(p-1)$ divides $(N-1)$.

Proof. Let p^r be the highest power of p dividing N (with $r \geq 1$). Then $a^{N-1} \equiv 1 \mod p^r$, and this means that the order of a in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ divides $N-1$. By Lemma 1.9 we know that $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic, so there is $a \in \mathbb{Z}$ such that this order is $(p-1)p^{r-1}$. From the consequence that $(p-1)p^{r-1}$ divides $N-1$ we get both statements. □

The next result can be seen as a deterministic primality test. It is impractical as it would rely on testing too many cases, and testing primality by checking the divisors up to the square root is faster. However, it is the basis of the Solovay-Strassen test.

Corollary 5.3. *Let $N \in \mathbb{N}_{\geq 3}$ be odd. Then the following two statements are equivalent:*

(i) N is prime.

(ii) For all $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ we have (for the Jacobi symbol):

$$a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \mod N$$

Proof. '(i) ⇒ (ii)': This is just Euler's result: Proposition 3.5.
'(ii) ⇒ (i)': Squaring (ii) and applying Proposition 5.2 shows that N is squarefree. Let p be a prime divisor of N (necessarily odd) and let $g \in \mathbb{Z}$ be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Note that the Legendre symbol $\left(\frac{g}{p}\right)$ is -1. By the Chinese Remainder Theorem there exists $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $b \equiv g \mod p$ and $b \equiv 1 \mod q$ for any prime divisor $q \mid N$, $q \neq p$. Hence, the Jacobi symbol $\left(\frac{b}{N}\right)$ equals -1. Thus Proposition 5.1 shows that N is prime. □

We can now give the key ingredient in the Solovay-Strassen test.

Proposition 5.4. *Let $N \in \mathbb{N}_{\geq 3}$ be odd and suppose N is not a prime. Consider the set*

$$A := \{a \in (\mathbb{Z}/N\mathbb{Z})^\times \mid a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \mod N\}.$$

Then $\#A \leq \frac{1}{2}\varphi(N) = \frac{1}{2}\#(\mathbb{Z}/N\mathbb{Z})^\times$.

Proof. We consider the group homomorphism

$$\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/N\mathbb{Z})^\times, \quad a \mapsto a^{\frac{N-1}{2}} \cdot \left(\frac{a}{N}\right).$$

Note that A is equal to $\ker(\psi)$. By Corollary 5.3 and the assumption that N is not prime, there is $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $b^{\frac{N-1}{2}} \not\equiv \left(\frac{b}{N}\right) \mod N$, thus $\operatorname{im}(\psi) \supsetneq \{1\}$, so $\#\operatorname{im}(\psi) \geq 2$. The isomorphism theorem implies $\operatorname{im}(\psi) \cong (\mathbb{Z}/N\mathbb{Z})^\times/A$, thus by Lagrange's theorem $2 \leq \#\operatorname{im}(\psi) = \varphi(N)/\#A$, implying the assertion. □

We can now describe the Solovay-Strassen primality test.

Algorithm 5.5 (Solovay-Strassen primality test)**.**
Input: $N \in \mathbb{N}_{\geq 3}$ *odd,* $B \in \mathbb{N}$ *(the 'bound').*
Output: `true` *or* `false`.

(1) Set $i = 0$.

(2) Choose a 'random' $a \in (\mathbb{Z}/N\mathbb{Z})^\times$.

(3) Calculate the Jacobi symbol $g := \left(\frac{a}{N}\right)$ (via Jacobi's reciprocity law).

(4) Calculate $h := a^{\frac{N-1}{2}} \mod N$ by fast exponentiation modulo N.

(5) If $g \equiv h \mod N$,

- *then replace i by $i+1$.*
  If $i > B$, then return `true` *and stop. If $i \leq B$, then go back to step (2).*
- *otherwise, return* `false` *and stop.*

Remark 5.6. *Let $N \in \mathbb{N}_{\geq 3}$ be odd.*

(a) If the Solovay-Strassen algorithm for (N, B) returns `false`*, then N is not a prime number by Corollary 5.3.*

(b) If the Solovay-Strassen algorithm for (N, B) returns `true`*, then N is a prime number with 'probability' at least $1 - \frac{1}{2^B}$, in the following (slightly imprecise) sense: If N is not prime, then by Proposition 5.4 the 'probability' that the 'random' element a satisfies the congruence $a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \mod N$ is less than $\frac{1}{2}$. If the 'random' choice of a is really random (like tossing a coin) and independent of this congruence condition, then the probability of satisfying the congruence B consecutive times is at most $\frac{1}{2^B}$.*

6 Proof of Gauß' reciprocity law via Gauß' sums

In this section, which will not be treated in the course, we will prove Gauß' reciprocity law Theorem 4.1 by using Gauß sums, which allow to write down a closed formula for $\left(\frac{p}{q}\right)$ for distinct odd primes p, q.

Lemma 6.1. *Let p be a prime number and $n \in \mathbb{N}_{\geq 1}$ not divisible by p. There is a finite field extension $\mathbb{F}_p(n)$ of $\mathbb{F}_p$ such that $\mathbb{F}_p(n)^\times$ contains a cyclic subgroup of order n.*

Proof. Define $\mathbb{F}_p(n)$ as the splitting field over $\mathbb{F}_p$ of the polynomial $X^n - 1 \in \mathbb{F}_p[X]$, which is separable as $\gcd(X^n - 1, nX^{n-1}) = 1$. Thus it has n distinct roots, all of which are elements of order dividing n. We know that $\mathbb{F}_p(n)^\times$ is a cyclic group by Proposition 1.14, hence there are precisely n elements or order dividing n and these form a cyclic subgroup of order n, as required. □

For the rest of this section and the proof of Theorem 4.1 we fix two distinct odd prime numbers p, q.

Lemma 6.2. *For any $1 \neq \beta \in \mathbb{F}_p(q)$ of order q we have*

$$\sum_{k=0}^{q-1} \beta^k = 0 \in \mathbb{F}_p(q).$$

Proof. $(1-\beta)\sum_{k=0}^{q-1} \beta^k = \sum_{k=0}^{q-1} \beta^k - \sum_{k=1}^{q} \beta^k = \beta^0 - \beta^q = 1 - 1 = 0$. Divide by $1 - \beta$ to obtain the claim. □

We now fix an element α of $\mathbb{F}_p(q)^\times$ of order equal to q, which exists by Lemma 6.1.

Definition 6.3. *The* Gauß sum for q modulo p *(with respect to α) is defined as:*

$$S_p(q) := \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \alpha^k \in \mathbb{F}_p(q).$$

Proposition 6.4. $S_p(q)^2 = \left(\frac{-1}{q}\right) \cdot q \in \mathbb{F}_p(q)^\times$.

Proof. We first have by definition

$$S_p(q)^2 = \left(\sum_{n=1}^{q-1} \left(\frac{n}{q}\right) \alpha^n\right) \cdot \left(\sum_{m=1}^{q-1} \left(\frac{m}{q}\right) \alpha^m\right) = \sum_{n=1}^{q-1} \sum_{m=1}^{q-1} \left(\frac{nm}{q}\right) \alpha^{n+m}.$$

We rewrite this as

$$S_p(q)^2 = \sum_{n \in (\mathbb{Z}/q\mathbb{Z})^\times} \sum_{m \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{nm}{q}\right) \alpha^{n+m}.$$

Note now that multiplication by $n \in (\mathbb{Z}/q\mathbb{Z})^\times$ defines a group automorphism of $(\mathbb{Z}/q\mathbb{Z})^\times$; that is, every element $m \in (\mathbb{Z}/q\mathbb{Z})^\times$ can be written as $m = nr$ for a unique $r \in (\mathbb{Z}/q\mathbb{Z})^\times$. Thus we may make the variable substitution $m = nr$:

$$S_p(q)^2 = \sum_{n \in (\mathbb{Z}/q\mathbb{Z})^\times} \sum_{r \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{n(rn)}{q}\right) \alpha^{n+rn} = \sum_{r \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{r}{q}\right) \sum_{n \in (\mathbb{Z}/q\mathbb{Z})^\times} (\alpha^{1+r})^n.$$

We now use Lemma 6.2 to obtain

$$S_p(q)^2 = \sum_{r\in(\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{r}{q}\right) \cdot \begin{cases} -1 & \text{if } \alpha^{1+r} \neq 1, \\ q-1 & \text{if } \alpha^{1+r} = 1. \end{cases}$$

Thus we obtain

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

where we used $\left(\frac{-1}{q}\right) = \left(\frac{q-1}{q}\right)$ and the fact that in $(\mathbb{Z}/q\mathbb{Z})^\times$ contains as many squares as non-squares (Lemma 3.1), whence the finial sum cancels out. □

Proposition 6.5 (Closed formula for the Legendre symbol with Gauß sums)**.**

$$\left(\frac{p}{q}\right) = \frac{S_p(q)^p}{S_p(q)} \in \mathbb{F}_p(q).$$

Proof. We first have by definition

$$S_p(q)^p = \Big(\sum_{n=1}^{q-1}\left(\frac{n}{q}\right)\alpha^n\Big)^p = \sum_{n=1}^{q-1}\left(\frac{n}{q}\right)\alpha^{np} = \sum_{n=1}^{q-1}\left(\frac{np^2}{q}\right)\alpha^{np},$$

where we used 'little Fermat' Corollary 1.12 and the fact that $(-1)^p = -1$; the final equality is trivial.
Note now that multiplication by p defines a group automorphism of $(\mathbb{Z}/q\mathbb{Z})^\times$; that is, every element $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ can be written as $r = np$ for a unique $n \in (\mathbb{Z}/q\mathbb{Z})^\times$. Thus we may make the variable substitution $np = r$:

$$S_p(q)^p = \sum_{r\in(\mathbb{Z}/q\mathbb{Z})^\times}\left(\frac{rp}{q}\right)\alpha^r.$$

Next we exploit the multiplicativity of the Legendre symbol

$$S_p(q)^p = \left(\frac{p}{q}\right)\sum_{r\in(\mathbb{Z}/q\mathbb{Z})^\times}\left(\frac{r}{q}\right)\alpha^r = \left(\frac{p}{q}\right)S_p(q),$$

which is the claimed result, since $S_p(q)$ is invertible by Proposition 6.4. □

We can now do the main part of the proof of Gauß' reciprocity law.

Proof of Theorem 4.1 (c). We first combine Proposition 6.4 with Euler's result 3.5:

$$S_p(q)^2 = q\cdot\left(\frac{-1}{q}\right) = q\cdot(-1)^{\frac{q-1}{2}} \in \mathbb{F}_p(q)^\times.$$

We obtain from this equality the following equivalence:

$$\left(\frac{q\cdot(-1)^{\frac{q-1}{2}}}{p}\right) = 1 \Leftrightarrow S_p(q) \in \mathbb{F}_p$$

because on the one hand if $S_p(q) \in \mathbb{F}_p$, then $q \cdot (-1)^{\frac{q-1}{2}}$ is a square in $\mathbb{F}_p$; on the other hand, as square roots in fields are unique up to sign, if $q \cdot (-1)^{\frac{q-1}{2}}$ is a square in $\mathbb{F}_p$, then $S_p(q)$ must belong to $\mathbb{F}_p$.
Now recall that an element x in some finite extension of $\mathbb{F}_p$ lies in $\mathbb{F}_p$ if and only if $x^p = x$. Thus we have the equivalence

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

which by Proposition 6.5 gives the equivalence

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

As the only possible values for the Legendre symbols in question here are -1 or 1, we have shown the equality

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

It suffices to interpret this in the desired way:

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

by Theorem 4.1 (a), which we already proved above. □

We must still give the proof of part (b) of Gauß' reciprocity law. It is essentially the same arguments again with q replaced by 8.

Proof of Theorem 4.1 (b). Let us fix a generator γ of the group of elements of order dividing 8 in $\mathbb{F}_p(8)$, which exists by Lemma 6.1.
The *Gauß sum for* 2 *modulo* p is defined as

$$S_p(2) = \gamma + \gamma^{-1} \in \mathbb{F}_p(8).$$

Note that $\gamma^4 = -1$. We use this in the following calculation:

$$\gamma^2 + \gamma^{-2} = \gamma^2 + \gamma^6 = \gamma^2 + \gamma^4\gamma^2 = \gamma^2 - \gamma^2 = 0.$$

This implies

$$S_p(2)^2 = (\gamma + \gamma^{-1})^2 = \gamma^2 + 2 + \gamma^{-2} = 2 \in \mathbb{F}_p(8)^\times.$$

As in the proof of Theorem 4.1 (c) this gives the equivalences:

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow S_p(2) \in \mathbb{F}_p \Leftrightarrow S_p(2) = S_p(2)^p.$$

We hence also calculate the p-th power of $S_p(2)$. Assume first $p \equiv 1, -1 \mod 8$. Then (using again 'Little Fermat' Corollary 1.12)

$$S_p(2)^p = (\gamma + \gamma^{-1})^p = \gamma^p + \gamma^{-p} = \gamma + \gamma^{-1} = S_p(2).$$

Assume now $p \equiv 5, -5 \mod 8$. Then we have

$$S_p(2)^p = \gamma^p + \gamma^{-p} = \gamma^5 + \gamma^{-5} = \gamma^4\gamma + (\gamma^4)^{-1}\gamma^{-1} = -(\gamma + \gamma^{-1}) = -S_p(2).$$

Thus, we obtain $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1, -1 \mod 8$, which can be equivalently expressed as $(-1)^{\frac{p^2-1}{8}} = 1$. This consequently yields the claimed equality $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. □

7 Proof of Gauß' reciprocity law via the cyclotomic character

In this section, we give a proof of Theorem 4.1 (c) using cyclotomic fields, which is based on the cyclotomic character. This puts Gauß' reciprocity law in the context of a Galois representation. This will lead us below towards the Langlands program and more general reciprocity laws.

Definition 7.1. *An element $\zeta \in \mathbb{C}$ is called a* root of unity *if there is a positive integer $n \in \mathbb{Z}$ such that $\zeta^n = 1$.*
Concretely, for fixed n, the roots of unity are $\exp(\frac{2\pi i}{n})^j \in \mathbb{C}$, where $i^2 = -1$ and $0 \leq j \leq n-1$ (recall $\exp(2\pi i) = 1$).

Let $\zeta \in \mathbb{C}$ be a root of unity such that $\zeta^n = 1$. Then ζ is a root of the polynomial $X^n - 1 \in \mathbb{Q}[X]$. Note the factorisation:

$$X^n - 1 = (X - 1) \cdot (X^{n-1} + X^{n-2} + \cdots + X + 1).$$

Before going on, let us say that the order of ζ is the order as an element in the multiplicative group $\mathbb{C}^\times$. Concretely, the order of ζ is the smallest positive integer m such that $\zeta^m = 1$.

Lemma 7.2. *Let $n \in \mathbb{Z}$ be an integer. Put $\zeta_n := \exp(\frac{2\pi i}{n}) \in \mathbb{C}$.*

(a) The order of ζ_n equals n.

(b) For $j \in \mathbb{Z}$, the order of ζ_n^j equals n if and only if $j \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. (a) is clear. (b) Let $d = \gcd(n, j)$ and let m be the order of ζ_n^j, i.e. the minimum $m \geq 1$ such that $\zeta_n^{jm} = 1$, that is, the minimum $m \geq 1$ such that n divides jm. Note $m \leq n$.
If $d = 1$ (equivalently, $j \in (\mathbb{Z}/n\mathbb{Z})^\times$), then n divides m, and consequently the order is $n = m$.
If $d \neq 1$ (equivalently, $j \notin (\mathbb{Z}/n\mathbb{Z})^\times$), then write $n = dn'$. We then have that n divides jn', whence the order is at most $n' < n$. □

We now include a proposition, the proof of which is not difficult, but too long for these lectures. The polynomials defined in the proposition are called the *cyclotomic polynomials*.

Proposition 7.3. *(a) Let $n = p$ be a prime number. Then the polynomial $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$ is irreducible.*

(b) Let $n \in \mathbb{Z}$ be an integer at least 2. The polynomial

$$\Phi_n(X) = \prod_{j \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^j)$$

lies in $\mathbb{Q}[X]$ and is irreducible.

Definition 7.4. *Let $n \in \mathbb{Z}$ be a positive integer. The n-th* cyclotomic field *is defined as*

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}[X]/(\Phi_n(X)).$$

It is the smallest subfield of $\mathbb{C}$ containing ζ_n.

The following corollary follows immediately from Proposition 7.3.

Corollary 7.5. *The field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois of degree $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. A $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta_n)$ is given by ζ_n^j for $j \in (\mathbb{Z}/n\mathbb{Z})^\times$.*

We will now describe the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ via the cyclotomic character. Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ consists of all ring homomorphisms $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ and that its order equals the field degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$.
The following computation is crucial for the rest. Let $a = \sigma(\zeta_n)$. Then

$$a^m = \sigma(\zeta_n)^m = \sigma(\zeta_n^m).$$

Taking $m = n$ shows that $a = \sigma(\zeta_n)$ is also an n-th root of unity. Taking m to be the order of a, shows $\zeta_n^m = 1$. Hence the order of a equals n. Hence, $a = \zeta_n^j$ for some $j \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 7.6. *Let $n \in \mathbb{Z}$ be an integer at least 2.*
For $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ we define $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ by the formula

$$\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}.$$

This defines an isomorphism of groups

$$\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times,$$

sending χ to $\chi(\sigma)$. We call it the mod n cyclotomic character.

Proof. We first check that χ is a group homomorphism. For that, let $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. We compute

$$\zeta_n^{\chi(\sigma\tau)} = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{\chi(\tau)}) = \big(\sigma(\zeta_n)\big)^{\chi(\tau)} = \big(\zeta_n^{\chi(\sigma)}\big)^{\chi(\tau)} = \zeta_n^{\chi(\sigma)\cdot\chi(\tau)}$$

and consequently, $\chi(\sigma\tau) = \chi(\sigma) \cdot \chi(\tau)$.
It is injective because $\chi(\sigma) = 1$ implies $\sigma(\zeta_n) = \zeta_n$, whence $\sigma = \mathrm{id}$ (as σ is uniquely determined by the image of the generator ζ_n). Since the cardinalities of source and target are equal, χ is a bijection and, hence, an isomorphism. □

We now study the case for a prime $n = p > 2$. By Proposition 7.6, $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is isomorphic to $\mathbb{F}_p^\times$, which is cyclic of degree $p-1$. Recall from Corollary 3.6 that the Legendre symbol defines a surjective group homomorphism

$$\mathbb{F}_p^\times \to \{-1, 1\}, \quad a \mapsto \left(\frac{a}{p}\right),$$

the kernel of which is $\mathbb{F}_p^{\times 2}$, the set of squares.
Note that $\{-1, 1\}$ is the unique quotient of order 2 of $\mathbb{F}_p^\times$. Via the cyclotomic character, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ admits a unique quotient of order 2. By Galois theory, this quotient corresponds to the unique quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_n)$. We now describe this quadratic field explicitly.

Proposition 7.7. *Let $p > 2$ be a prime number. Put $p^* = (-1)^{\frac{p-1}{2}} p = \left(\frac{-1}{p}\right) p$. Then $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$.*

Proof. Let $\tau = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) \zeta_p^a \in \mathbb{Q}(\zeta_p)$. We show $\tau^2 = p^*$. This then implies that

$$\mathbb{Q}(\sqrt{p^*}) = \mathbb{Q}(\tau) \subseteq \mathbb{Q}(\zeta_p)$$

is the desired subfield.
We compute as follows (as in Neukirch: Algebraic Number Theory):

$$\left(\frac{-1}{p}\right) \tau^2 = \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{-ab}{p}\right) \zeta_p^{a+b} = \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{ab}{p}\right) \zeta_p^{a-b} = \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{ab^{-1}}{p}\right) \zeta_p^{a-b},$$

where we have used the multiplicativity of the Legendre symbol, replaced b by $-b$ and used $\left(\frac{b}{p}\right) = \left(\frac{b^{-1}}{p}\right)$. Next write $c = ab^{-1}$ to get

$$\left(\frac{-1}{p}\right) \tau^2 = \sum_{b,c \in \mathbb{F}_p^\times} \left(\frac{c}{p}\right) \zeta_p^{bc-b} = \sum_{c \in \mathbb{F}_p^\times \setminus \{1\}} \left(\frac{c}{p}\right) \sum_{b \in \mathbb{F}_p^\times} (\zeta_p^{c-1})^b + \sum_{b \in \mathbb{F}_p^\times} \left(\frac{1}{p}\right).$$

As ζ_p^{c-1} is a primitive p-th root of unity, we have $0 = \Phi_p(\zeta_p^{-1}) = \sum_{b=0}^{p-1} (\zeta_p^{c-1})^b$, showing $\sum_{b \in \mathbb{F}_p^\times} (\zeta_p^{c-1})^b = -1$. Furthermore, $\sum_{c \in \mathbb{F}_p^\times} \left(\frac{c}{p}\right) = 0$, as exactly half of the elements are squares and the others non-squares. Thus $\sum_{c \in \mathbb{F}_p^\times \setminus \{1\}} \left(\frac{c}{p}\right) = -1$. Consequently, we obtain

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

as claimed. □

We thus obtain the following commutative diagram, the horizontal arrows of which are isomorphisms.

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & \xrightarrow{\chi} & \mathbb{F}_p^\times \\ \downarrow & & \downarrow \left(\frac{\cdot}{p}\right) \\ \mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) & \longrightarrow & \{1, -1\}. \end{array} \tag{7.1}$$

In order to prove Gauß' reciprocity law, we now look more closely at the arithmetic of the cyclotomic character.
If we had the notions generally taught in a course on Algebraic Number Theory, we could finish in a couple of lines. Here, we take a down-to-earth approach based on polynomials and (have to) state some harder results as facts.
Let, for the time being, $K = \mathbb{Q}[X]/(f(X))$ be a Galois extension of $\mathbb{Q}$ given by a monic, irreducible integral polynomial $f \in \mathbb{Z}[X]$ of degree n. Let q be a prime number. We consider the reduction $\overline{f} \in \mathbb{F}_q[X]$ of $f(X)$ (in the sense of reducing all coefficients modulo q). In general, $\overline{f}$ will not be irreducible and so it factors

$$\overline{f}(X) = \overline{f}_1(X) \cdot \overline{f}_2(X) \cdots \overline{f}_r(X),$$

where we assume each $\overline{f}_i \in \mathbb{F}_q[X]$ to be irreducible.
We now make an important additional assumption: we assume the $\overline{f}_1(X), \overline{f}_2(X), \ldots, \overline{f}_r(X)$ to be pairwise distinct. (For those who know Algebraic Number Theory: this assumption is stronger than asking q to be unramified in K; that's the price we pay for working with polynomials rather than ideals.) This assumption implies that the roots (in $\overline{\mathbb{F}}_q$) of $\overline{f}(X)$ are all distinct, and they are partitioned into r subsets of cardinality n/r (here we use the assumption that the extension is Galois), with the i-th subset being the roots of $\overline{f}_i(X)$. This gives a corresponding partitioning of the n roots (in $\mathbb{C}$) of f; call $\mathcal{R}_i$ the subset of the roots of f that correspond to the roots of $\overline{f}_i(X)$ in $\overline{\mathbb{F}}_q$.
The Galois group $\mathrm{Gal}(\mathbb{F}_q[X]/(\overline{f}_1(X))/\mathbb{F}_q)$ is a cyclic group of order n/r generated by Frob_q, the Frobenius homomorphism sending x to x^q. It permutes the roots of $\overline{f}_1(X)$.

Fact 7.8. *The group* $\mathrm{Gal}(\mathbb{F}_q[X]/(\overline{f}_1(X))/\mathbb{F}_q)$ *is isomorphic to the subgroup of* $\mathrm{Gal}(K/\mathbb{Q})$ *consisting of those* σ *that permute* $\mathcal{R}_1$. *In particular, we can view* Frob_q *as an element of* $\mathrm{Gal}(K/\mathbb{Q})$.

Let us now see what this means for the quadratic extension $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$. We have to factor the polynomial $X^2 - p^*$ in $\mathbb{F}_q[X]$. For $q \neq p$, there are two possibilities:
If $\left(\frac{p^*}{q}\right) = 1$, the polynomial factors into two distinct polynomials of degree 1 in $\mathbb{F}_q[X]$.
If $\left(\frac{p^*}{q}\right) = -1$, the polynomial remains irreducible in $\mathbb{F}_q[X]$.

In the first case, $\mathrm{Frob}_q \in \mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$ will have order 1, and in the second case order 2. This means that the lower horizontal isomorphism in the diagram (7.1) sends Frob_q to the Legendre symbol $\left(\frac{p^*}{q}\right)$.

Fact 7.9. *In* $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, Frob_q *sends* ζ_p *to* ζ_p^q. *Thus* $\chi(\mathrm{Frob}_q) = q$. *This is 'believable' because* Frob_q *raises to the* q*-th power on the residue field, but we would need some more terminology to prove it correctly.*

Proof of Theorem 4.1 (c). Let q, p be distinct odd primes. The proof consists in following Frob_q through the commutative diagram (7.1).
First going right and then going down, sends Frob_q first to q and then down to $\left(\frac{q}{p}\right)$.

First going down and then going right, sends Frob_q first to Frob_q (in $\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$) and then right to $\left(\frac{p^*}{q}\right)$.
Since the diagram commutes, it does not matter which way we take, and so we conclude

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

This ends the proof. □

One can prove Theorem 4.1 (b) in a similar way, but then one has to change the generating polynomial of $\mathbb{Q}(\sqrt{p^*})$ so that its reduction modulo 2 is either irreducible or has two distinct factors. The point here is (for those knowing Algebraic Number Theory) that $\sqrt{p^*}$ does not generated the ring of integers of $\mathbb{Q}(\sqrt{p^*})$.

8 Some more general reciprocity laws

It is not so clear how to define the term 'general reciprocity law'. What I speak about here is my point of view.
The main point that I want to make is the following: We obtained Gauß' quadratic reciprocity law as a direct consequence of the cyclotomic character:

$$\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{F}_p^\times$$

and its property that it sends Frob_q to q for any prime $q \neq p$.
Let us now move on and speak about Galois representations. A d-dimensional Galois representations is simply a linear representation of a Galois group $\mathrm{Gal}(K/\mathbb{Q})$ of a Galois extension, such as a group homomorphism of the form

$$\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_d(F),$$

where F is a field. We know an example: the cyclotomic character!

$$\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathrm{GL}_1(\mathbb{F}_p).$$

It is of dimension 1.
Note that we can simply embed $\mathbb{F}_p^\times$ as a subgroup of $\mathbb{C}^\times$ by sending a generator of $\mathbb{F}_p^\times$ to ζ_{p-1}. Then the have a 1-dimensional Galois representation with complex coefficients

$$\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathrm{GL}_1(\mathbb{C}).$$

Galois representations with complex coefficients are called *Artin representations*.
Let us now consider a more general setting. Let K be a finite extension of $\mathbb{Q}$; such are called *number fields*. Let L/K be a finite Galois extension. Then all 1-dimensional Artin representations

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_1(\mathbb{C})$$

are classified by *(Global) Class Field Theory*. Indeed, more generally, all *abelian* extensions of K are described by the *Artin reciprocity law*. This uses GL_1 of the so-called adèles, which would need the introduction of much more terminology than what we can do here.
We rather go deeper into Galois representations. Suppose $f(z) = \sum_{n=1}^{\infty} a_n \exp(2\pi i z)^n$ is the Fourier expansion of a newform of weight 1, which is a holomorphic function on the upper half-plane satisfying certain transformation rules and $|a_q| \leq 2$ for all primes q. Then there is an attached Artin representation

$$\rho_f : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$$

such that for almost all primes q, the trace of $\rho_f(\mathrm{Frob}_q) = a_q$. Here K is a certain extension of $\mathbb{Q}$.
To f one can attach a so-called L-function. Explicitly, it is the function

$$L_f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

defined for $s \in \mathbb{C}$ such that $\mathrm{Re}(s) > 3/2$. One can show that it possesses an analytic continuation to all of $\mathbb{C}$.
On the other hand, given an Artin representation

$$\rho : \mathrm{Gal}(K/F) \to \mathrm{GL}_d(\mathbb{C})$$

one can also define an L-function by using the characteristic polynomials of $\rho(\mathrm{Frob}_q)$ for almost all q (and replacements for the q that are excluded).
The second Artin conjecture in these lectures is the following.

Conjecture 8.1 (Artin's conjecture on L-functions)**.** *The L-function of any Artin representation has an analytic continuation to the entire complex plane.*

This conjecture is also still open for $d \geq 3$. For $d = 1$ it follows from Class Field Theory. For $d = 2$, there are partial results. If F is 'totally real' and ρ is 'odd', then one knows that ρ comes from a ρ_f for a 'Hilbert modular form' and then the analytic continuation is known. This is a very recent result by Shu Sasaki (and others) published in 2019.
In summary, such Galois representations can be seen as generalisations of Gauß' quadratic reciprocity. Moreover, what we saw above is a glimpse of a correspondence between Galois representations and modular forms, or, more generally, automorphic forms. This correspondence is the heart of the *Langlands program*, and it is also referred to as 'Langlands reciprocity'. This is a very active area of research, in which many things remain to be discovered.

Exercises

Exercise 1. *(a) Let $n = 255$ and $e = 71$. Find $s \in \mathbb{N}$ such that $1 \leq s \leq 255$ and $es \equiv 1 \mod (n)$.*

(b) (Chinese Remainder Theorem) Compute $x \in \mathbb{Z}$ such that $x \equiv 2 \mod (15)$ and $x \equiv 3 \mod (17)$.

Exercise 2. *(a) Prove by induction: $5^{2^k} = (1+4)^{2^k} \equiv 1 + 2^{k+2} \mod 2^{k+3}$ for all $k \in \mathbb{N}_{\geq 0}$.*

(b) Conclude from (a) that the order of 5 in $(\mathbb{Z}/2^m\mathbb{Z})^\times$ equals 2^{m-2} for all $m \in \mathbb{N}_{\geq 2}$.

(c) Let $p > 2$ be a prime number. Prove by induction: $(1+p)^{p^k} \equiv 1 + p^{k+1} \mod p^{k+2}$ for all $k \in \mathbb{N}_{\geq 0}$.

(d) Conclude from (c) that the order of $1+p$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$ equals p^{m-1} for all $m \in \mathbb{N}_{\geq 1}$.

(e) Let $m \in \mathbb{N}_{\geq 2}$. Prove the existence of a group isomorphism

$$(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}.$$

The factors are generated by -1 and 5 in $(\mathbb{Z}/2^m\mathbb{Z})^\times$, respectively.

Hint. We know $\varphi(2^m) = (2-1)2^{m-1} = 2^{m-1}$. Prove that no power of 5 is equal to -1 in $(\mathbb{Z}/2^m\mathbb{Z})^\times$.

(f) Let $p > 2$ be a prime number and $m \in \mathbb{N}_{\geq 1}$. Prove the existence of a group isomorphism

$$(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{p-1}\mathbb{Z}.$$

Hint. We know that $\varphi(p^m) = (p-1)p^{m-1}$. Use the class of $1+p$, the fact that $\mathbb{F}_p^\times = \mathbb{Z}/p\mathbb{Z}^\times$ and the fact that p and $p-1$ are coprime.

Exercise 3. *(a) Compute the following Legendre symbols using Gauß reciprocity:*

$$\left(\frac{313}{367}\right), \qquad \left(\frac{367}{401}\right), \qquad \left(\frac{401}{313}\right), \qquad \left(\frac{3}{401}\right).$$

Hint. The numbers $3, 313, 367, 401$ are all prime.

(b) Let $p \geq 5$ be a prime number. Prove the following statements:

(1) $\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \mod 12, \\ -1, & \text{if } p \equiv \pm 5 \mod 12. \end{cases}$

(2) If $2^p - 1$ is prime, then $\left(\frac{3}{2^p-1}\right) = -1$.

Exercise 4. *Let $N \in \mathbb{N}_{\geq 3}$ be odd. Suppose that for all $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ we have $a^{\frac{N-1}{2}} \equiv \pm 1 \mod N$.*
By Proposition 5.2, we know that N is squarefree, i.e.

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

with distinct primes $p_1, \ldots, p_k$. We also know that $p_i - 1$ divides $N - 1$ for all $1 \leq i \leq k$.
By the Chinese Remainder Theorem, we further have the isomorphism

$$\Phi : (\mathbb{Z}/N\mathbb{Z})^\times \cong \prod_{i=1}^{k} (\mathbb{Z}/p_i)^\times.$$

(a) What is the image of the classes of 1 and -1 in $(\mathbb{Z}/N\mathbb{Z})^\times$ under Φ?

(b) Suppose that there is $j \in \{1, \ldots, k\}$ such that $\frac{N-1}{p_j - 1}$ is odd. Compute

$$(\overline{1}, \ldots, \overline{1}, g_j, \overline{1}, \ldots, \overline{1})^{\frac{N-1}{2}} \in \prod_{i=1}^{k} (\mathbb{Z}/p_i\mathbb{Z})^\times,$$

where g_j is a generator of $(\mathbb{Z}/p_i\mathbb{Z})^\times$.

(c) Suppose $N \equiv 3 \mod 4$. Deduce that N is prime.

(d) Suppose here that there is $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $b^{\frac{N-1}{2}} \equiv -1 \mod N$. Deduce that N is prime.

Hint: If for all $i \in \{1, \ldots, k\}$ we have that $\frac{N-1}{p_i - 1}$ is even, then compute

$$(\overline{a}, \ldots, \overline{a})^{\frac{N-1}{2}} \in \prod_{i=1}^{k} (\mathbb{Z}/p_i\mathbb{Z})^\times$$

for $a \in (\mathbb{Z}/N\mathbb{Z})^\times$.