Math 533 Winter 2021, Lecture 15: Finite fields and quadratic residues

website: `https://www.cip.ifi.lmu.de/~grinberg/t/21w/`

1. Finite fields (cont'd)

1.1. One more lemma

The following lemma will be used twice in today's lecture:

Lemma 1.1.1. Let p be a prime. Then:
(a) We have $a^p = a$ for each $a \in \mathbb{Z}/p$.
(b) Let F be a field such that $\mathbb{Z}/p$ is a subring of F. Then,

$$\{a \in F \mid a^p = a\} = \mathbb{Z}/p.$$

This lemma gives a criterion for showing that an element of F lies in $\mathbb{Z}/p$: namely, just show that $a^p = a$.

Proof of Lemma 1.1.1. **(a)** Let $a \in \mathbb{Z}/p$. Write a as $a = \overline{u}$ for some integer u. Then, Fermat's Little Theorem yields $u^p \equiv u \bmod p$. But this means $\overline{u^p} = \overline{u}$. In other words, $a^p = a$ (since $a = \overline{u}$). This proves Lemma 1.1.1 **(a)**.

(b) From Lemma 1.1.1 **(a)**, we get $\mathbb{Z}/p \subseteq \{a \in F \mid a^p = a\}$.

Now, I claim that $|\{a \in F \mid a^p = a\}| \leq p$. Indeed, F is an integral domain. Thus, the easy half of the FTA (see Lecture 12) yields that if n is a nonnegative integer, then any nonzero polynomial of degree $\leq n$ over F has at most n roots in F. Applying this to the polynomial $x^p - x$ (which is nonzero and has degree p), we conclude that the polynomial $x^p - x$ has at most p roots in F. But the set of all roots of this polynomial $x^p - x$ in F is $\{a \in F \mid a^p = a\}$; hence, the preceding sentence says that $|\{a \in F \mid a^p = a\}| \leq p$. Thus, in particular, the set $\{a \in F \mid a^p = a\}$ is finite.

However, an easy and fundamental fact in combinatorics says that if X and Y are two finite sets with $X \subseteq Y$ and $|Y| \leq |X|$, then $X = Y$. Applying this to $X = \mathbb{Z}/p$ and $Y = \{a \in F \mid a^p = a\}$, we obtain $\mathbb{Z}/p = \{a \in F \mid a^p = a\}$ (since $\mathbb{Z}/p \subseteq \{a \in F \mid a^p = a\}$ and $|\{a \in F \mid a^p = a\}| \leq p = |\mathbb{Z}/p|$). This proves Lemma 1.1.1 **(b)**. □

Another useful lemma says (in terms of Lecture 14) that the Frobenius endomorphism of a field of characteristic p is always injective:

Lemma 1.1.2. Let p be a prime. Let F be a field of characteristic p. Let $a, b \in F$ satisfy $a \neq b$. Then, $a^p \neq b^p$.

Note that this would fail for $F = \mathbb{R}$ and $p = 2$ (because, for example, $1 \neq -1$ but $1^2 = (-1)^2$), and also fail for $F = \mathbb{C}$ and any $p > 1$. Thus, this marks one more of the situations where fields of prime characteristic p behave better than fields of characteristic 0.

Proof of Lemma 1.1.2. From $a \neq b$, we see that the element $a - b$ of F is nonzero. But F is a field, and thus an integral domain. Hence, it is easy to see (by induction on k) that any finite product $u_1 u_2 \cdots u_k$ of nonzero elements of F is nonzero. Thus, in particular, the product $\underbrace{(a-b)(a-b)\cdots(a-b)}_{p \text{ times}}$ is nonzero (since $a - b$ is nonzero). In other words, $(a-b)^p$ is nonzero.

However, part **(c)** of the Idiot's Binomial Formula (see Lecture 14) yields $(a-b)^p = a^p - b^p$, so that $a^p - b^p = (a-b)^p \neq 0$ (since $(a-b)^p$ is nonzero). In other words, $a^p \neq b^p$. This proves Lemma 1.1.2. □

1.2. An application of root adjunction

What are finite fields (particularly the ones that are not just $\mathbb{Z}/p$) good for? Known applications include error-correcting codes (BCH codes), group theory (many finite simple groups can be constructed as matrix groups over finite fields), block designs (roughly speaking, finite structures with symmetries that resemble geometries) and, of course, number theory (not unexpectedly; number theory uses everything). Let me show a more humble – but also more self-contained – application. Namely, by adjoining roots of polynomials to $\mathbb{Z}/p$, we will prove a curious fact about Fibonacci numbers:[1]

Theorem 1.2.1. Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence. This is the sequence of integers defined recursively by $f_0 = 0$ and $f_1 = 1$ and

$$f_n = f_{n-1} + f_{n-2} \qquad \text{for all } n \geq 2.$$

Let p be a prime. Then:

(a) If $p \equiv \pm 1 \bmod 5$ (meaning that p is congruent to one of 1 and -1 modulo 5), then $p \mid f_{p-1}$.

(b) If $p \equiv \pm 2 \bmod 5$ (meaning that p is congruent to one of 2 and -2 modulo 5), then $p \mid f_{p+1}$.

For example:

- For $p = 2$, Theorem 1.2.1 **(b)** says that $2 \mid f_3$ (since $2 \equiv 2 \bmod 5$), and indeed we have $f_3 = 2$.

[1] You have seen the Fibonacci sequence already (in Exercise 6 on homework set #1). Much more about it can be found (e.g.) in [Vorobi02] or [Grinbe21].

- For $p = 7$, Theorem 1.2.1 **(b)** says that $7 \mid f_8$ (since $7 \equiv 2 \bmod 5$), and indeed we have $f_8 = 21 = 3 \cdot 7$.
- For $p = 11$, Theorem 1.2.1 **(a)** says that $11 \mid f_{10}$ (since $11 \equiv 1 \bmod 5$), and indeed we have $f_{10} = 55 = 5 \cdot 11$.

Our proof of Theorem 1.2.1 will be inspired by the famous **Binet formula** for Fibonacci numbers:

Theorem 1.2.2 (Binet formula for Fibonacci numbers)**.** Let $\varphi = \dfrac{1+\sqrt{5}}{2} \approx 1.618$ and $\psi = \dfrac{1-\sqrt{5}}{2} \approx -0.618$ be the two roots of the quadratic polynomial $x^2 - x - 1$ in $\mathbb{R}$. Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence. Then,

$$f_n = \frac{1}{\sqrt{5}}\varphi^n - \frac{1}{\sqrt{5}}\psi^n \qquad \text{for each } n \in \mathbb{N}.$$

This is somewhat mysterious – why should irrational numbers like $\sqrt{5}$ appear in a formula for an integer sequence like $(f_0, f_1, f_2, \ldots)$? Proving Theorem 1.2.2 is an easy exercise in strong induction. Finding it is trickier – the matrix approach from Exercise 6 on homework set #1 can help here. Indeed, once you know that the matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{R}^{2\times 2}$ satisfies $A^n = f_n A + f_{n-1} I_2$ for each n (this was proven in Exercise 6 **(c)** on homework set #1), you can boil down the computation of f_n to the computation of A^n. But there is a famous trick for computing powers of a matrix: namely, you diagonalize the matrix and take the powers of its diagonal entries[2]. This trick only works if the matrix is diagonalizable; but fortunately, our matrix A is diagonalizable, so we can compute A^n using this trick, ultimately obtaining Theorem 1.2.2 stated above. This demystifies the formula: $x^2 - x - 1$ is just the characteristic polynomial of the matrix A, and φ and ψ are its eigenvalues.

Anyway, how does this help us proving Theorem 1.2.1? The Binet formula involves irrational numbers and division; we thus cannot directly draw any conclusions about divisibility from it.

We can, however, use it as an inspiration. To wit, we shall introduce analogues of φ and ψ in "characteristic p". These should be roots of the same polynomial $x^2 - x - 1$, but regarded as a polynomial over $\mathbb{Z}/p$ instead of $\mathbb{R}$. Depending on p, this polynomial may or may not have roots in $\mathbb{Z}/p$, but we can always construct a splitting field in which it will have roots (see Lecture 14). Let us use this to attempt a proof of Theorem 1.2.1:

[2]Namely: If $A = QDQ^{-1}$, then $A^n = QD^nQ^{-1}$ for any $n \in \mathbb{N}$. If the matrix D is diagonal, then D^n is easily computed by taking its diagonal entries to the n-th powers; thus, A^n can be obtained as well.

Proof of Theorem 1.2.1, part 1. First, we WLOG assume that $p \neq 5$ (since Theorem 1.2.1 makes no statement about $p = 5$). Hence, $p \nmid 5$ (since p is prime), so that $\overline{5} \neq \overline{0}$ in $\mathbb{Z}/p$. Furthermore, from $p \neq 5$, we obtain $5 \nmid p$ (since p is prime); thus, the remainder of p upon division by 5 must be 1, 2, 3 or 4. Therefore, p must satisfy one of the conditions $p \equiv \pm 1 \bmod 5$ and $p \equiv \pm 2 \bmod 5$.

Let F be the splitting field of the polynomial $x^2 - x - 1$ over $\mathbb{Z}/p$. (We know from Lecture 14 that such an F exists, since the polynomial is monic.) Thus,

$$x^2 - x - 1 = (x - \varphi)(x - \psi) \qquad \text{for some } \varphi, \psi \in F.$$

Consider these φ, ψ. Comparing coefficients in front of the monomials x^1 and x^0 in the polynomial identity

$$x^2 - x - 1 = (x - \varphi)(x - \psi) = x^2 - (\varphi + \psi)\, x + \varphi\psi$$

yields[3]

$$-1 = -(\varphi + \psi) \qquad \text{and} \qquad -1 = \varphi\psi.$$

(Of course, the "1" here stands for 1_F.) In other words,

$$\varphi + \psi = 1 \qquad \text{and} \qquad \varphi\psi = -1.$$

Define an element $\sqrt{5}$ of F by $\sqrt{5} = \varphi - \psi$. This is certainly a strange notation (this $\sqrt{5}$ is not the actual number $\sqrt{5}$ but just an analogue of it in our field F), but it is harmless (as we won't deal with the actual number $\sqrt{5}$ in this proof, but only with the element $\sqrt{5} = \varphi - \psi$ that we just introduced). Moreover, it is justified because

$$(\varphi - \psi)^2 = \varphi^2 - 2\varphi\psi + \psi^2 = \left(\underbrace{\varphi + \psi}_{=1}\right)^2 - 4\,\underbrace{\varphi\psi}_{=-1} = 1^2 - 4(-1) = \overline{5}.$$

As a consequence, $\left(\sqrt{5}\right)^2 = \overline{5} \neq \overline{0}$, so that $\sqrt{5} \neq \overline{0}$. Thus, $\sqrt{5}$ is a unit of F (since F is a field), so we can divide by $\sqrt{5}$.

Now, we claim that an analogue of the Binet formula holds in F: Namely, we have

$$\overline{f_n} = \frac{1}{\sqrt{5}}\varphi^n - \frac{1}{\sqrt{5}}\psi^n \qquad \text{for each } n \in \mathbb{N}. \tag{1}$$

[3] This is perhaps a good time to recall the warnings about evaluating polynomials over finite fields. Two polynomials f and g over a finite field F do not need to be identical just because their evaluations at all elements of F are identical (for example, the polynomials x^2 and x over $\mathbb{Z}/2$ are not identical, but their evaluations on both elements $\overline{0}$ and $\overline{1}$ of $\mathbb{Z}/2$ are identical). However, our two polynomials $x^2 - x - 1$ and $x^2 - (\varphi + \psi)\, x + \varphi\psi$ (whose coefficients we are comparing here) are known to be identical (not just their evaluations but the polynomials themselves); thus, we can compare their coefficients.

This can be proved by the same strong induction argument as the original Binet formula (Theorem 1.2.2).

Now, we want to show that $p \mid f_{p-1}$ for some primes p and that $p \mid f_{p+1}$ for other primes p (remember: we have already gotten rid of the $p = 5$ case). In other words, we want to show that $\overline{f_{p-1}} = 0$ for some primes p, and that $\overline{f_{p+1}} = 0$ for other primes p. For now, let us ignore the question of which primes p satisfy which of these.

Here comes a trick that will look magical, but is actually an instance of a general method. We have $\varphi^2 - \varphi - 1 = 0$ (since φ is a root of the polynomial $x^2 - x - 1$), so that $\varphi^2 = \varphi + 1$. Taking this equality to the p-th power, we obtain

$$\begin{aligned} \varphi^{2p} &= (\varphi+1)^p = \varphi^p + 1^p \qquad \text{(by the Idiot's Binomial Formula)} \\ &= \varphi^p + 1. \end{aligned}$$

In other words, $\varphi^{2p} - \varphi^p - 1 = 0$. Thus, φ^p is a root of the polynomial $x^2 - x - 1 = (x-\varphi)(x-\psi)$. In other words, $(\varphi^p - \varphi)(\varphi^p - \psi) = 0$. Since F is an integral domain, this entails $\varphi^p - \varphi = 0$ or $\varphi^p - \psi = 0$. In other words, $\varphi^p = \varphi$ or $\varphi^p = \psi$. In other words, $\varphi^p \in \{\varphi, \psi\}$. Similarly, $\psi^p \in \{\varphi, \psi\}$.

Moreover, $\varphi - \psi = \sqrt{5} \neq \overline{0}$, so that $\varphi \neq \psi$ and therefore $\varphi^p \neq \psi^p$ (by Lemma 1.1.2, since F has characteristic p). Combining this with $\varphi^p \in \{\varphi, \psi\}$ and $\psi^p \in \{\varphi, \psi\}$, we conclude that φ^p and ψ^p are two **distinct** elements of the set $\{\varphi, \psi\}$. Thus, $\{\varphi^p, \psi^p\} = \{\varphi, \psi\}$. So we are in one of the following two cases:

Case 1: We have $\varphi^p = \varphi$ and $\psi^p = \psi$.

Case 2: We have $\varphi^p = \psi$ and $\psi^p = \varphi$.

Let us consider Case 1. In this case, we have $\varphi^p = \varphi$ and $\psi^p = \psi$. Now, $\varphi \neq 0$ (since $\varphi^2 = \varphi + 1$ would turn into the absurd equality $0 = 1$ if φ was 0); thus, we can cancel φ from the equality $\varphi^p = \varphi$ (since F is a field). As a result, we obtain $\varphi^{p-1} = 1$. Similarly, $\psi^{p-1} = 1$. Now, (1) yields

$$\overline{f_{p-1}} = \frac{1}{\sqrt{5}} \underbrace{\varphi^{p-1}}_{=1} - \frac{1}{\sqrt{5}} \underbrace{\psi^{p-1}}_{=1} = \frac{1}{\sqrt{5}} \cdot 1 - \frac{1}{\sqrt{5}} \cdot 1 = 0.$$

Thus, we have shown that $\overline{f_{p-1}} = 0$ (that is, $p \mid f_{p-1}$) in Case 1.

Let us next consider Case 2. In this case, we have $\varphi^p = \psi$ and $\psi^p = \varphi$. Thus, $\varphi^{p+1} = \underbrace{\varphi^p}_{=\psi} \varphi = \psi\varphi = \varphi\psi = -1$ and similarly $\psi^{p+1} = -1$. Now, (1) yields

$$\overline{f_{p+1}} = \frac{1}{\sqrt{5}} \underbrace{\varphi^{p+1}}_{=-1} - \frac{1}{\sqrt{5}} \underbrace{\psi^{p+1}}_{=-1} = \frac{1}{\sqrt{5}} (-1) - \frac{1}{\sqrt{5}} (-1) = 0.$$

Thus, we have shown that $\overline{f_{p+1}} = 0$ (that is, $p \mid f_{p+1}$) in Case 2.

So we have shown that we always have $p \mid f_{p-1}$ or $p \mid f_{p+1}$. But why does the former hold for $p \equiv \pm 1 \bmod 5$ and the latter for $p \equiv \pm 2 \bmod 5$? In other

words, why does our Case 1 correspond to $p \equiv \pm 1 \bmod 5$ and our Case 2 to $p \equiv \pm 2 \bmod 5$?

This will take some more work. We have the following chain of equivalences:

$$\begin{aligned}
&(\text{we are in Case 1}) \\
&\iff (\varphi^p = \varphi \text{ and } \psi^p = \psi) \\
&\iff (\varphi^p = \varphi) \\
&\qquad \left(\begin{array}{c} \text{because if } \varphi^p = \varphi, \text{ then } \psi^p \text{ cannot be } \varphi \text{ (since } \varphi^p \neq \psi^p\text{)} \\ \text{and thus must be } \psi \text{ (since } \psi^p \in \{\varphi, \psi\}\text{)} \end{array} \right) \\
&\iff (\varphi \in \{a \in F \mid a^p = a\}) \\
&\iff (\varphi \in \mathbb{Z}/p) \qquad (\text{by Lemma 1.1.1 } \textbf{(b)}) \\
&\iff \left(\text{the polynomial } x^2 - x - 1 \text{ has a root in } \mathbb{Z}/p\right). \qquad (2)
\end{aligned}$$

(In the last equivalence sign, the "$\Longrightarrow$" part is obvious (since φ is a root of $x^2 - x - 1$). The "$\Longleftarrow$" part can be proved as follows: If the polynomial $x^2 - x - 1$ has a root in $\mathbb{Z}/p$, then this root must be either φ or ψ (because $x^2 - x - 1 = (x - \varphi)(x - \psi)$); however, in either of these cases, we obtain $\varphi \in \mathbb{Z}/p$ (because if $\psi \in \mathbb{Z}/p$, then $\varphi = \underbrace{(\varphi + \psi)}_{=1 \in \mathbb{Z}/p} - \underbrace{\psi}_{\in \mathbb{Z}/p} \in \mathbb{Z}/p$).)

Thus, our question is reduced to asking when the polynomial $x^2 - x - 1$ has a root in $\mathbb{Z}/p$. In other words, when can we find our φ and ψ in $\mathbb{Z}/p$, and when do we have to go into a larger field to find them?

We WLOG assume that $p \neq 2$ (since the case $p = 2$ is trivial to do by hand). Thus, $\overline{2} \in \mathbb{Z}/p$ is nonzero and thus has an inverse. This allows us to complete the square (just as in high school, but over the field $\mathbb{Z}/p$ now):

$$x^2 - x - 1 = \left(x - \frac{\overline{1}}{\overline{2}}\right)^2 - \frac{\overline{5}}{\overline{4}}. \qquad (3)$$

Thus, the polynomial $x^2 - x - 1$ has a root in $\mathbb{Z}/p$ if and only if $\dfrac{\overline{5}}{\overline{4}}$ is a square in $\mathbb{Z}/p$. Obviously, $\dfrac{\overline{5}}{\overline{4}}$ is a square in $\mathbb{Z}/p$ if and only if $\overline{5}$ is a square in $\mathbb{Z}/p$ (since $\overline{4} = \overline{2}^2$ is always a square in $\mathbb{Z}/p$). Thus, in order to prove Theorem 1.2.1, it remains to prove the following: □

Theorem 1.2.3. Let p be a prime such that $p \neq 2$. Then:

(a) If $p \equiv \pm 1 \bmod 5$ (meaning that p is congruent to one of 1 and -1 modulo 5), then $\overline{5}$ is a square in $\mathbb{Z}/p$.

(b) If $p \equiv \pm 2 \bmod 5$ (meaning that p is congruent to one of 2 and -2 modulo 5), then $\overline{5}$ is not a square in $\mathbb{Z}/p$.

For example, $\overline{5} \in \mathbb{Z}/p$ is not a square for $p = 7$, but is a square for $p = 11$ (namely, $\overline{5} = \overline{4}^2$).

I will now prove Theorem 1.2.3; then, I will explain how it helps complete the above proof of Theorem 1.2.1, and afterwards (perhaps most interestingly) discuss how to generalize it to other numbers instead of 5.

Proof of Theorem 1.2.3. The following proof (due to Gauss) will again use field extensions. We WLOG assume that $p \neq 5$ (since Theorem 1.2.3 makes no claim about the case $p = 5$).

An element z of a field F is said to be a **primitive 5-th root of unity** if it satisfies $z^5 = 1$ but $z \neq 1$. In other words, the element z is a primitive 5-th root of unity if it is nonzero and its order in the group $F^\times$ (this is the group of units of F) is 5.

For example, $\mathbb{R}$ has no primitive 5-th roots of unity (since a real number z satisfying $z^5 = 1$ must necessarily satisfy $z = 1$), but $\mathbb{C}$ has four of them: namely, $e^{2\pi ik/5}$ for $k \in \{1,2,3,4\}$. (See `https://upload.wikimedia.org/wikipedia/commons/4/40/One5Root.svg` for an illustration of the latter on the Argand diagram: The 5 blue points, which are the vertices of a regular points, all satisfy $z^5 = 1$, and all but one of them are primitive 5-th roots of unity.)

Does $\mathbb{Z}/p$ have any primitive 5-th roots of unity? Sometimes yes (e.g., for $p = 11$); sometimes no (e.g., for $p = 7$). We don't care – we shall just adjoin one.

To see how, we notice the following: If F is a field of characteristic p, then a primitive 5-th root of unity in F is just an element $z \in F$ that satisfies $z^4 + z^3 + z^2 + z + 1 = 0$. [4] Knowing this, we can easily adjoin a primitive 5-th root of unity to $\mathbb{Z}/p$: Namely, $x^4 + x^3 + x^2 + x + 1 \in (\mathbb{Z}/p)[x]$ is a monic polynomial of degree 4 over $\mathbb{Z}/p$. Thus, by Lecture 14, there exists a field that contains $\mathbb{Z}/p$ as a subring and that contains a root of this polynomial. Let S be such a field, and let z be this root. Thus, $z \in S$ satisfies $z^4 + z^3 + z^2 + z + 1 = 0$, and therefore is a primitive 5-th root of unity (by what we have just said). That is, we have $z^5 = 1$ and $z \neq 1$.

[4] *Proof.* If z is a primitive 5-th root of unity in F, then $z^5 = 1$ but $z \neq 1$, so that $\dfrac{z^5 - 1}{z - 1} = 0$ (since the numerator $z^5 - 1$ is 0 but the denominator $z - 1$ is nonzero), and therefore $z^4 + z^3 + z^2 + z + 1 = 0$ (since $z^4 + z^3 + z^2 + z + 1 = \dfrac{z^5 - 1}{z - 1}$).

Conversely, assume that $z^4 + z^3 + z^2 + z + 1 = 0$. Then, $z^5 - 1 = (z-1)\underbrace{\left(z^4 + z^3 + z^2 + z + 1\right)}_{=0} = 0$, so that $z^5 = 1$. However, if we had $z = 1$, then we would have $z^4 + z^3 + z^2 + z + 1 = 1^4 + 1^3 + 1^2 + 1 + 1 = \overline{5} \neq \overline{0}$, which would contradict $z^4 + z^3 + z^2 + z + 1 = 0 = \overline{0}$. Hence, we must have $z \neq 1$. Thus we have shown that $z^5 = 1$ and $z \neq 1$; in other words, z is a primitive 5-th root of unity.

Now comes the magic: Set $\tau = z - z^2 - z^3 + z^4 \in S$. Then,

$$\begin{aligned}
\tau^2 &= \left(z - z^2 - z^3 + z^4\right)^2 \\
&= z^2 + z^4 + z^6 + z^8 - 2zz^2 - 2zz^3 + 2zz^4 + 2z^2z^3 - 2z^2z^4 - 2z^3z^4 \\
&\qquad \text{(by expanding the square)} \\
&= z^2 + z^4 + z^6 + z^8 - 2z^3 - 2z^4 + 2z^5 + 2z^5 - 2z^6 - 2z^7 \\
&= z^2 + z^4 + z + z^3 - 2z^3 - 2z^4 + \overline{2} + \overline{2} - 2z - 2z^2 \\
&\qquad \left(\text{since } z^5 = 1 \text{ and thus } z^6 = z \text{ and } z^7 = z^2\right) \\
&= \overline{4} - \left(z + z^2 + z^3 + z^4\right) = \overline{5} - \underbrace{\left(z^4 + z^3 + z^2 + z + 1\right)}_{=0} = \overline{5}.
\end{aligned}$$

Thus, τ is a "square root" of $\overline{5}$ in S (meaning: an element of S whose square is $\overline{5}$). Hence, the only "square roots" of $\overline{5}$ in S are τ and $-\tau$ [5].

This suggests that studying τ should help understand whether $\overline{5}$ is a square in $\mathbb{Z}/p$. Indeed, if τ belongs to $\mathbb{Z}/p$, then $\overline{5}$ is a square in $\mathbb{Z}/p$ (since $\tau^2 = \overline{5}$). Conversely (but less obviously), if τ does **not** belong to $\mathbb{Z}/p$, then $\overline{5}$ is not a square in $\mathbb{Z}/p$ (because the only "square roots" of $\overline{5}$ in S are τ and $-\tau$, and neither of them belongs to $\mathbb{Z}/p$ [6]). Now, how can we tell whether τ belongs to $\mathbb{Z}/p$?

Inspired by Lemma 1.1.1 **(b)**, we compute τ^p. From $\tau = z - z^2 - z^3 + z^4$, we obtain

$$\tau^p = \left(z - z^2 - z^3 + z^4\right)^p = z^p - z^{2p} - z^{3p} + z^{4p}$$

(by the Idiot's Binomial Theorem from Lecture 14, applied several times). The right hand side of this can be greatly simplified if you know the remainder of p upon division by 5. Indeed, we have $z^5 = 1$, so that $z^6 = z$ and $z^7 = z^2$ and more generally $z^k = z^\ell$ for any two integers k and ℓ satisfying $k \equiv \ell \bmod 5$. Hence, in order to simplify the right hand side, we distinguish the following four cases:

Case 1: We have $p \equiv 1 \bmod 5$.
Case 2: We have $p \equiv 2 \bmod 5$.
Case 3: We have $p \equiv 3 \bmod 5$.
Case 4: We have $p \equiv 4 \bmod 5$.
(There is no Case 0, since $5 \nmid p$ entails $p \not\equiv 0 \bmod 5$.)

[5] This is a particular case of the following general fact: If R is an integral domain, and if $u, v \in R$ satisfy $u^2 = v$, then the only "square roots" of v in R are u and $-u$. (To check this, argue as follows: If w is a square root of v in R, then $(w-u)(w+u) = \underbrace{w^2}_{=v} - \underbrace{u^2}_{=v} = v - v = 0$, so that $w - u = 0$ or $w + u = 0$ (since R is an integral domain), so that $w = u$ or $w = -u$.)

[6] Indeed, from $\tau \notin \mathbb{Z}/p$, we obtain $-\tau \notin \mathbb{Z}/p$ (since otherwise, $\tau = -(-\tau)$ would yield $\tau \in \mathbb{Z}/p$).

In Case 2, we have

$$\begin{aligned}\tau^p &= \underbrace{z^p}_{\substack{=z^2 \\ (\text{since } p \equiv 2 \bmod 5)}} - \underbrace{z^{2p}}_{\substack{=z^4 \\ (\text{since } 2p \equiv 4 \bmod 5)}} - \underbrace{z^{3p}}_{\substack{=z^1 \\ (\text{since } 3p \equiv 1 \bmod 5)}} + \underbrace{z^{4p}}_{\substack{=z^3 \\ (\text{since } 4p \equiv 3 \bmod 5)}} \\ &= z^2 - z^4 - z^1 + z^3 = -\underbrace{\left(z - z^2 - z^3 + z^4\right)}_{=\tau} = -\tau.\end{aligned}$$

Similarly, we get $\tau^p = -\tau$ in Case 3, and we get $\tau^p = \tau$ in Cases 1 and 4.

Thus, in Cases 1 and 4, we have $\tau^p = \tau$ and therefore $\tau \in \{a \in F \mid a^p = a\} = \mathbb{Z}/p$ (by Lemma 1.1.1 **(b)**), and thus $\overline{5}$ is a square in $\mathbb{Z}/p$ (since $\tau^2 = \overline{5}$). On the other hand, in Cases 2 and 3, we have $\tau^p = -\tau \neq \tau$ (since $2\tau \neq 0$ [7]) and therefore $\tau \notin \{a \in F \mid a^p = a\} = \mathbb{Z}/p$ (by Lemma 1.1.1 **(b)**), and thus $\overline{5}$ is not a square in $\mathbb{Z}/p$ (as explained above). This proves Theorem 1.2.3. □

The "magical" use of z (a primitive 5-th root of unity) to construct a square root of $\sqrt{5}$ is connected to the ubiquity of $\sqrt{5}$ in the geometry of regular pentagons. But it is not specific to the number 5: Gauss has shown that $\sqrt{p}$ can be similarly constructed from a primitive p-th root of unity for any prime p. (Alas, we won't get to the details of this.)

Next, let us use Theorem 1.2.3 to complete our above proof of Theorem 1.2.1:

Proof of Theorem 1.2.1, part 2. Recall the two Cases 1 and 2 that appeared in part 1 of this proof. We extend the equivalence (2) as follows:

$$\begin{aligned}&(\text{we are in Case 1}) \\ &\iff \left(\text{the polynomial } x^2 - x - 1 \text{ has a root in } \mathbb{Z}/p\right) \\ &\iff \left(\text{the polynomial } \left(x - \frac{\overline{1}}{\overline{2}}\right)^2 - \frac{\overline{5}}{\overline{4}} \text{ has a root in } \mathbb{Z}/p\right) \\ &\qquad\qquad (\text{by (3)}) \\ &\iff \left(\frac{\overline{5}}{\overline{4}} \text{ is a square in } \mathbb{Z}/p\right) \\ &\iff \left(\overline{5} \text{ is a square in } \mathbb{Z}/p\right) \\ &\qquad\qquad \left(\text{since } \frac{\overline{5}}{\overline{4}} = a^2 \text{ is equivalent to } \overline{5} = (2a)^2\right) \\ &\iff (p \equiv \pm 1 \bmod 5) \qquad (4)\end{aligned}$$

(by Theorem 1.2.3, since p must satisfy one of the conditions $p \equiv \pm 1 \bmod 5$ and $p \equiv \pm 2 \bmod 5$). But we have shown that if we are in Case 1, then $p \mid f_{p-1}$. Thus,

[7] This can be shown as follows: From $\tau^2 = \overline{5} \neq 0$, we obtain $\tau \neq 0$. Moreover, $p \neq 2$ shows that $\overline{2} \neq 0$ in $\mathbb{Z}/p$. Now, F is an integral domain; hence, from $\overline{2} \neq 0$ and $\tau \neq 0$, we obtain $\overline{2}\tau \neq 0$. In other words, $2\tau \neq 0$.

we conclude using (4) that if $p \equiv \pm 1 \bmod 5$, then $p \mid f_{p-1}$. This proves Theorem 1.2.1 **(a)**. Likewise, if $p \equiv \pm 2 \bmod 5$, then we do **not** have $p \equiv \pm 1 \bmod 5$, so that we are **not** in Case 1 (by (4)), and thus we are in Case 2; hence, as we proved above, we must have $p \mid f_{p+1}$ in this case. Thus, Theorem 1.2.1 **(b)** is proved again. □

1.3. Quadratic residues: an introduction

We have touched upon an interesting subject, so let us delve deeper. Theorem 1.2.3 answers the question for which primes p the residue class $\overline{5} \in \mathbb{Z}/p$ is a square in $\mathbb{Z}/p$; but we can ask the same question about the residue class $\overline{a}$ of any $a \in \mathbb{Z}$.

Definition 1.3.1. Let p be a prime. Let a be an integer not divisible by p.

Then, a is said to be a **quadratic residue modulo** p (short: a **QR mod** p) if the residue class $\overline{a} \in \mathbb{Z}/p$ is a square (or, equivalently, if there is an integer b such that $a \equiv b^2 \bmod p$).

Otherwise, a is said to be a **quadratic nonresidue modulo** p (short: a **QNR mod** p).

Definition 1.3.2. Let p be a prime. Let a be an integer. The **Legendre symbol** $\left(\frac{a}{p}\right)$ (do not mistake this for a fraction! this is not a fraction!) is the integer defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a; \\ 1, & \text{if } a \text{ is a QR mod } p; \\ -1, & \text{if } a \text{ is a QNR mod } p. \end{cases}$$

Note that the Legendre symbol $\left(\frac{a}{p}\right)$ depends only on the prime p and the residue class $\overline{a} \in \mathbb{Z}/p$, not on the integer a itself. For example, $\left(\frac{-1}{p}\right) = \left(\frac{p-1}{p}\right)$ for any prime p.

Examples:

- 2 is a QR mod 7, since $2 \equiv 3^2 \bmod 7$. Thus, $\left(\frac{2}{7}\right) = 1$.
- 2 is a QNR mod 5, since the squares in $\mathbb{Z}/5$ are $\overline{0}, \overline{1}, \overline{4}$. Thus, $\left(\frac{2}{5}\right) = -1$.
- -1 is a QR mod 5, since $-1 \equiv 2^2 \bmod 5$. Thus, $\left(\frac{-1}{5}\right) = 1$.

- -1 is a QNR mod 3. Thus, $\left(\dfrac{-1}{3}\right) = -1$.
- Theorem 1.2.3 says that every prime $p \neq 2$ satisfies

$$\left(\frac{5}{p}\right) = \begin{cases} 0, & \text{if } p = 5; \\ 1, & \text{if } p \equiv \pm 1 \bmod 5; \\ -1, & \text{if } p \equiv \pm 2 \bmod 5. \end{cases}$$

This might whet an appetite: can we find similarly simple expressions for $\left(\dfrac{2}{p}\right)$ or $\left(\dfrac{3}{p}\right)$ or $\left(\dfrac{-1}{p}\right)$? What can we say about Legendre symbols in general? We begin with a simple yet surprising rule:

Theorem 1.3.3 (Euler's QR criterion)**.** Let $p \neq 2$ be a prime. Let a be an integer. Then,

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

Proof. Since p is prime and satisfies $p \neq 2$, we see that p is odd and ≥ 3. Hence, $(p-1)/2$ is a positive integer. Thus, $0^{(p-1)/2} = 0$.

We must prove that $\left(\dfrac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$. If $p \mid a$, then this boils down to $0 \equiv 0 \bmod p$ (since $0^{(p-1)/2} = 0$). Thus, we WLOG assume that $p \nmid a$.

Let $u = \overline{a} \in \mathbb{Z}/p$; thus, u is nonzero (since $p \nmid a$). Hence, the definition of $\left(\dfrac{a}{p}\right)$ yields

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a QR mod } p; \\ -1, & \text{if } a \text{ is a QNR mod } p \end{cases} = \begin{cases} 1, & \text{if } u \text{ is a square;} \\ -1, & \text{if } u \text{ is not a square} \end{cases}$$

(by the definition of QRs and QNRs) and thus

$$\overline{\left(\frac{a}{p}\right)} = \begin{cases} \overline{1}, & \text{if } u \text{ is a square;} \\ \overline{-1}, & \text{if } u \text{ is not a square.} \end{cases} \tag{5}$$

Also,

$$\overline{a^{(p-1)/2}} = \overline{a}^{(p-1)/2} = u^{(p-1)/2} \tag{6}$$

(since $\overline{a} = u$). Now, we have the following chain of equivalences.

$$\begin{aligned}
&\left(\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p\right) \qquad \text{(this is the claim we are proving)} \\
&\iff \left(\overline{\left(\frac{a}{p}\right)} = \overline{a^{(p-1)/2}}\right) \iff \left(\overline{a^{(p-1)/2}} = \overline{\left(\frac{a}{p}\right)}\right) \\
&\iff \left(u^{(p-1)/2} = \begin{cases} \overline{1}, & \text{if } u \text{ is a square;} \\ \overline{-1}, & \text{if } u \text{ is not a square} \end{cases}\right)
\end{aligned}$$

(by (5) and (6)). Hence, it remains to prove that

- $u^{(p-1)/2} = \overline{1}$ if u is a square;
- $u^{(p-1)/2} = \overline{-1}$ if u is not a square.

Equivalently, we shall prove the following three claims:

> *Claim 1:* Any nonzero element $v \in \mathbb{Z}/p$ satisfies $v^{(p-1)/2} = \overline{1}$ or $v^{(p-1)/2} = \overline{-1}$.
>
> *Claim 2:* Any nonzero square $v \in \mathbb{Z}/p$ satisfies $v^{(p-1)/2} = \overline{1}$.
>
> *Claim 3:* Any element $v \in \mathbb{Z}/p$ that is not a square satisfies $v^{(p-1)/2} \neq \overline{1}$.

This will prove the two bullet points we claimed above: The first bullet point will follow from Claim 2, while the second will follow from Claims 1 and 3. So it remains to prove the three Claims 1, 2 and 3.

Proof of Claim 1. Let $v \in \mathbb{Z}/p$ be a nonzero element. Then, Lemma 1.1.1 **(a)** yields $v^p = v$. We can cancel v from this equality (since v is nonzero and $\mathbb{Z}/p$ is a field), and thus obtain $v^{p-1} = 1$. Since $p-1$ is even, we have $\left(v^{(p-1)/2}\right)^2 = v^{p-1} = 1$, so that $\left(v^{(p-1)/2}\right)^2 - 1 = 0$. In view of $\left(v^{(p-1)/2}\right)^2 - 1 = \left(v^{(p-1)/2} - 1\right)\left(v^{(p-1)/2} + 1\right)$, this rewrites as $\left(v^{(p-1)/2} - 1\right)\left(v^{(p-1)/2} + 1\right) = 0$. Since $\mathbb{Z}/p$ is an integral domain, this entails $v^{(p-1)/2} - 1 = 0$ or $v^{(p-1)/2} + 1 = 0$. In other words, $v^{(p-1)/2} = \overline{1}$ or $v^{(p-1)/2} = \overline{-1}$. This proves Claim 1. □

Proof of Claim 2. Let $v \in \mathbb{Z}/p$ be a nonzero square. Thus, $v = w^2$ for some $w \in \mathbb{Z}/p$. Consider this w. Now, $w \neq 0$ (since $w^2 = v$ is nonzero). But Lemma 1.1.1 **(a)** yields $w^p = w$. We can cancel w from this equality (since $w \neq 0$ and $\mathbb{Z}/p$ is a field), and thus obtain $w^{p-1} = 1$. Now, from $v = w^2$, we obtain $v^{(p-1)/2} = \left(w^2\right)^{(p-1)/2} = w^{p-1} = 1 = \overline{1}$. This proves Claim 2. □

Proof of Claim 3. Here we take a bird's eye view (as in our above proof of Lemma 1.1.1 **(b)**), rather than treating a single element v. Indeed, $\mathbb{Z}/p$ is an integral domain. Thus, the easy half of the FTA (see Lecture 12) yields that if n is a nonnegative integer, then any nonzero polynomial of degree $\leq n$ over $\mathbb{Z}/p$ has at most n roots in $\mathbb{Z}/p$. Applying this to the polynomial $x^{(p-1)/2} - 1$ (which is nonzero and has degree $(p-1)/2$), we conclude that the polynomial $x^{(p-1)/2} - 1$ has at most $(p-1)/2$ roots in $\mathbb{Z}/p$. But the set of all roots of this polynomial $x^{(p-1)/2} - 1$ in $\mathbb{Z}/p$ is $\left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}$; hence, the preceding sentence says that $\left|\left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}\right| \leq (p-1)/2$.

On the other hand, $\{\text{nonzero squares } v \in \mathbb{Z}/p\} \subseteq \left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}$ (by Claim 2) and $|\{\text{nonzero squares } v \in \mathbb{Z}/p\}| = (p-1)/2$ (indeed, this is a particular case of something that was proved in the solution of Exercise 10 **(c)** on homework set #1; but the proof is not hard[8]).

However, an easy and fundamental fact in combinatorics says that if X and Y are two finite sets with $X \subseteq Y$ and $|Y| \leq |X|$, then $X = Y$. Applying this to $X = \{\text{nonzero squares } v \in \mathbb{Z}/p\}$ and $Y = \left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}$, we obtain $\{\text{nonzero squares } v \in \mathbb{Z}/p\} = \left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}$ (since $\{\text{nonzero squares } v \in \mathbb{Z}/p\} \subseteq \left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}$ and $\left|\left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}\right| \leq (p-1)/2 = |\{\text{nonzero squares } v \in \mathbb{Z}/p\}|$). Thus, every $v \in \mathbb{Z}/p$ satisfying $v^{(p-1)/2} = \overline{1}$ must be a nonzero square. By taking the contrapositive of this statement, we obtain Claim 3. □

Having proved Claims 1, 2 and 3, we thus have completed the proof of Theorem 1.3.3. □

Corollary 1.3.4 (Multiplicativity of the Legendre symbol)**.** Let $p \neq 2$ be a prime. Let $a, b \in \mathbb{Z}$. Then,

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

Proof. Note that $p > 2$ (since $p \neq 2$ and since p is a prime). Thus, the three integers $0, 1, -1$ are pairwise incongruent[9] modulo p. Yes, we will use this; just wait.

[8] *Proof idea:* Each nonzero square $v \in \mathbb{Z}/p$ has exactly two (distinct) "square roots", and each of the $p-1$ elements $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ appears as a "square root" of exactly one nonzero square. Hence, there is a 2-to-1 correspondence between the $p-1$ elements $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ and the nonzero squares $v \in \mathbb{Z}/p$. Therefore, the number of nonzero squares $v \in \mathbb{Z}/p$ is $(p-1)/2$. In other words, $|\{\text{nonzero squares } v \in \mathbb{Z}/p\}| = (p-1)/2$.

[9] "Incongruent" means "not congruent".

Theorem 1.3.3 yields

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \bmod p. \tag{7}$$

But Theorem 1.3.3 also yields $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$ and $\left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \bmod p$. Multiplying these two congruences, we obtain

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2} b^{(p-1)/2} \bmod p.$$

Comparing this congruence with (7), we find

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p. \tag{8}$$

We want an equality, not a congruence! But the congruence (8) turns out to entail the equality. Indeed, both sides of the congruence (8) equal 0 or 1 or -1 (since any Legendre symbol is either 0 or 1 or -1, and the same holds for a product of Legendre symbols). Hence, their congruence implies their equality (since $0, 1, -1$ are pairwise incongruent modulo p). This proves Corollary 1.3.4. □

Corollary 1.3.4 has two nice corollaries of its own:

Corollary 1.3.5. Let $p \neq 2$ be a prime. The map

$$\begin{aligned} (\mathbb{Z}/p)^\times &\to \{1, -1\}, \\ \overline{a} &\mapsto \left(\frac{a}{p}\right) \end{aligned}$$

is a group morphism (i.e., a homomorphism of groups).

Proof. The map is well-defined, since (as we have explained above) $\left(\frac{a}{p}\right)$ depends only on p and $\overline{a} \in \mathbb{Z}/p$ (not on a itself). Let us now show that this map is a group morphism.

In order to show that a map between two groups is a group morphism, it suffices to show that this map respects multiplication (this is well-known). Thus, it suffices to show that our map respects multiplication. In other words, it suffices to show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for any $a, b \in \mathbb{Z}$ that are not divisible by p (since any two elements of the group $(\mathbb{Z}/p)^\times$ can be written in the forms $\overline{a}$ and $\overline{b}$ for two such $a, b \in \mathbb{Z}$, and then their product will be $\overline{ab}$). But this follows from Corollary 1.3.4. □

Corollary 1.3.6. Let $p \neq 2$ be a prime. Let $u, v \in \mathbb{Z}/p$ be two nonzero residue classes. Then:

(a) If u and v are squares, then uv is a square.

(b) If only one of u and v is a square, then uv is not a square.

(c) If none of u and v is a square, then uv is a square.

Note that Corollary 1.3.6 **(c)** would fail if we replaced $\mathbb{Z}/p$ by $\mathbb{Q}$. For example, none of the rational numbers 2 and 3 is a square, but neither is $2 \cdot 3$. But it does hold in $\mathbb{Z}/p$ (as we shall now show), and (more generally) in finite fields, as well as in $\mathbb{R}$ (since the non-squares in $\mathbb{R}$ are precisely the negative reals, but a product of two negative reals is always positive).

Proof of Corollary 1.3.6. We shall only prove part **(c)**, for two reasons: First of all, parts **(a)** and **(b)** hold for any field (unlike part **(c)**, as we just discussed), and can easily be proved using nothing but the field axioms. Also, the proof we will give for part **(c)** can easily be adapted to the other two parts.

(c) Assume that none of u and v is a square. Write u and v in the form $u = \overline{a}$ and $v = \overline{b}$ for some integers a and b. Then, a is a QNR mod p (since $\overline{a} = u$ is not a square and thus nonzero), and thus $\left(\frac{a}{p}\right) = -1$ (by the definition of the Legendre symbol). Similarly, $\left(\frac{b}{p}\right) = -1$. Hence, Corollary 1.3.4 yields $\left(\frac{ab}{p}\right) = \underbrace{\left(\frac{a}{p}\right)}_{=-1}\underbrace{\left(\frac{b}{p}\right)}_{=-1} = (-1)(-1) = 1$. In other words, ab is a QR mod p (by the definition of the Legendre symbol). In other words, $\overline{ab}$ is nonzero and a square. In view of $\overline{ab} = \overline{a} \cdot \overline{b} = uv$ (since $\overline{a} = u$ and $\overline{b} = v$), this yields that uv is a square. Thus, Corollary 1.3.6 **(c)** is proven. $\square$

Let us now return to the computation of Legendre symbols. Thanks to Corollary 1.3.4, we have (for example) $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$ and $\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$ for any prime p. But how do we compute $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ and $\left(\frac{3}{p}\right)$?

We begin with $\left(\frac{-1}{p}\right)$, which is probably the easiest one:

Theorem 1.3.7. Let $p \neq 2$ be a prime. Then, -1 is a QR mod p (that is, $\overline{-1} \in \mathbb{Z}/p$ is a square) if and only if $p \equiv 1 \bmod 4$. In other words,

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

Proof. Since p is a prime satisfying $p \neq 2$, the number p is odd. Hence, $(p-1)/2 \in \mathbb{Z}$.

Theorem 1.3.3 yields the congruence

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

This congruence must actually be an equality, since both sides are 0 or 1 or -1 (just as in the proof of Corollary 1.3.4). In other words,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}. \tag{9}$$

Now, p must satisfy $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$ (since p is odd). In the former case, $(-1)^{(p-1)/2}$ is 1; in the latter, -1. Hence, (9) becomes

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

□

So we have simple formulas for $\left(\frac{-1}{p}\right)$ and $\left(\frac{5}{p}\right)$. What about $\left(\frac{a}{p}\right)$ for a general a ? We only need to know a formula for $\left(\frac{q}{p}\right)$ for each prime q (because, as per Corollary 1.3.4 above, we can then get a general formula for $\left(\frac{a}{p}\right)$ by decomposing a into a product of primes and possibly -1, and multiplying). Here is one:

Theorem 1.3.8 (Quadratic Reciprocity Law)**. (a)** Let $p \neq 2$ be a prime. Then,

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

(b) Let p and q be two distinct primes distinct from 2. Then,

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right).$$

For example, if p is a prime distinct from 2 and 5, then Theorem 1.3.8 **(b)**

(applied to $q = 5$) yields

$$\left(\frac{5}{p}\right) = \underbrace{(-1)^{(p-1)(5-1)/4}}_{\substack{=1 \\ \text{(since } 5-1=4 \text{ and thus} \\ (p-1)(5-1)/4=p-1 \text{ is even)}}} \quad \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

$$= \begin{cases} 1, & \text{if } \overline{p} \in \mathbb{Z}/5 \text{ is a square;} \\ -1, & \text{if } \overline{p} \in \mathbb{Z}/5 \text{ is not a square} \end{cases} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \bmod 5; \\ -1, & \text{if } p \equiv \pm 2 \bmod 5 \end{cases}$$

(the last equality follows from the fact that the nonzero squares in $\mathbb{Z}/5$ are $\overline{1}$ and $\overline{-1}$); this recovers the claim of Theorem 1.2.3. So Theorem 1.2.3 was merely the tip of an iceberg.

Theorem 1.3.8 is one of the most classical theorems in mathematics – discovered by Euler, proved by Gauss. By now, it has received over 250 proofs (see `https://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html` for a list), and new proofs keep getting published. You'll get to prove its part **(a)** on homework set #4, inspired by the $q = 5$ case we proved above. This will hopefully shed some more light on the strange definition of τ.

See [Burton11, Chapter 9] or [Stein09, Chapter 4] (or almost any text on elementary number theory) for more about quadratic residues. A collection of proofs of Theorem 1.3.8 has also been published as a book ([Baumga15]); one of the most elementary proofs is presented in [KeeGui20, §3.12]. See also [Schroe09, particularly Chapter 16] for an application of quadratic residues to the acoustics of concert halls.

References

[Baumga15] Oswald Baumgart, *The Quadratic Reciprocity Law: A Collection of Classical Proofs*, Springer 2015.

[Burton11] David M. Burton, *Elementary Number Theory*, 7th edition, McGraw-Hill 2011.

[KeeGui20] Patrick Keef, David Guichard, *An Introduction to Higher Mathematics*, 24 March 2020.

[Grinbe21] Darij Grinberg, *Notes on mathematical problem solving*, 10 February 2021.
`http://www.cip.ifi.lmu.de/~grinberg/t/20f/mps.pdf`

[Schroe09] Manfred Schroeder, *Number Theory in Science and Communication*, 5th edition 2009.

[Stein09] William Stein, *Elementary Number Theory: Primes, Congruences, and Secrets*, Springer 2009.

[Vorobi02] Nicolai N. Vorobiev, *Fibonacci Numbers*, Translated from the Russian by Mircea Martin, Springer 2002 (translation of the 6th Russian edition).