Elementary Number Theory - Exercise 6a

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Determine the quadratic residues modulo 11.

Solution 1. We know that half of the elements in $(\mathbb{Z}/11\mathbb{Z})^*$ are quadratic residues, i.e. there are precisely 5, and to find them we just need to compute the squares $1^2, 2^2, \dots \left(\frac{11-1}{2}\right)^2$ modulo 11. Hence the quadratic residues modulo 11 are given by $1, 4, 9, 5, 3$.

Problem 2. Let p be an odd prime. Show that

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

Solution 2. By Euler's criterion we have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p,$$

and since both sides are either 1 or -1, we obtain the stated identity.

Problem 3. Let p be an odd prime and $\gcd(p, ab) = 1$. Show that

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

Solution 3. By Euler's criterion we have

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p,$$

and since both sides are either 1 or -1, we obtain the claimed identity.

Problem 4. Compute the following Legendre symbols.

$$\left(\frac{14}{11}\right); \quad \left(\frac{2}{5}\right); \quad \left(\frac{256}{17}\right); \quad \left(\frac{18}{19}\right); \quad \left(\frac{10}{1009}\right).$$

Solution 4. Since the Legendre symbol depends on the numerator modulo p, we have $\left(\frac{14}{11}\right) = \left(\frac{3}{11}\right)$. We have seen above that 3 is a square mod 11 ($6^2 \equiv 3 \pmod{11}$), so $\left(\frac{14}{11}\right) = 1$.

We have $1^2 \equiv 1 \pmod 5$ and $2^2 \equiv 4 \pmod 5$, so the quadratic residues modulo 5 are 1 and 4 (which equals -1 modulo 5). Hence 2 is a non-residue, and $\left(\frac{2}{5}\right) = -1$.

Since the Legendre symbol is multiplicative and valued in $\{\pm 1\}$, we have

$$\left(\frac{256}{17}\right) = \left(\frac{2^8}{17}\right) = \left(\frac{2}{17}\right)^8 = 1.$$

Note that $18 \equiv -1 \pmod{19}$. By Euler's criterion we have

$$\left(\frac{18}{19}\right) \equiv \left(\frac{-1}{19}\right) \equiv (-1)^{\frac{19-1}{2}} \equiv -1 \pmod{19},$$

which implies $\left(\frac{18}{19}\right) = -1$.

We can multiply the numerator of the Legendre symbol by a square without changing its value (if the square is coprime to p). Hence,

$$\left(\frac{10}{1009}\right) = \left(\frac{10 \cdot 10^2}{1009}\right) = \left(\frac{1000}{1009}\right) = \left(\frac{-9}{1009}\right) = \left(\frac{-1}{1009}\right).$$

Using Euler's criterion, we have $\left(\frac{-1}{1009}\right) = (-1)^{\frac{1009-1}{2}} = 1$, so $\left(\frac{10}{1009}\right) = 1$.

Problem 5. Let p be an odd prime and $\gcd(a, p) = 1$. Show that

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

where a^{-1} denotes the inverse of a modulo p.

Solution 5. If x solves $x^2 \equiv a \pmod{p}$, then $y = x^{-1}$ solves $y^2 = a^{-1} \pmod{p}$, and vice versa. In particular, $x^2 \equiv a \pmod{p}$ is solvable if and only if $y^2 \equiv a^{-1} \pmod{p}$ is solvable, which means that $\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)$.

Another way to prove this is to use that the Legendre symbol is multiplicative, and only depends on the numerator modulo p, so

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

Since $\left(\frac{a^{-1}}{p}\right)$ and $\left(\frac{a}{p}\right)$ are both either $+1$ or -1, and their product is 1, they agree.

Problem 6. Let p be an odd prime. For $n \in \mathbb{Z}$ we define the *Gauss sum*

$$G_p(n) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right) e^{2\pi i a n/p},$$

where the sum runs over an arbitrary system of representatives for $(\mathbb{Z}/p\mathbb{Z})^*$.

1. Check that the sum is well-defined, that is, independent of the chosen system of representatives for $(\mathbb{Z}/p\mathbb{Z})^*$.

2. Show that
$$G_p(n) = \begin{cases} \left(\frac{n}{p}\right) G_p(1), & \text{if } p \nmid n, \\ 0, & \text{if } p \mid n. \end{cases}$$

3. Show that
$$G_p(1)^2 = \left(\frac{-1}{p}\right) p.$$
Deduce that $G_p(1) = \pm\sqrt{p}$ if $p \equiv 1 \pmod 4$ and $G_p(1) = \pm i\sqrt{p}$ if $p \equiv 3 \pmod 4$.
Hint: The sum $\sum_{a=0}^{p-1} e^{2\pi i n a/p}$ vanishes unless $p \mid n$.

Solution 6. 1. Changing the system of representatives means changing each a to $a + kp$ for some $k \in \mathbb{Z}$ (that may depend on a). But $\left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right)$ and $e^{2\pi i(a+kp)/p} = e^{2\pi i a/p}$, so the sum is well-defined.

2. If $p \mid n$, then
$$G_p(n) = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right) e^{2\pi i a n/p} = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right) = 0,$$
since precisely half of the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ are quadratic residues, and the other half are non-residues.

Let $p \nmid n$. If a runs through a system of representatives for $(\mathbb{Z}/p\mathbb{Z})^*$, then so does an. Hence, if we write $b = an$, then
$$G_p(n) = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right) e^{2\pi i a n/p} = \sum_{b\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{bn^{-1}}{p}\right) e^{2\pi i b/p} = \left(\frac{n^{-1}}{p}\right) G_1(p) = \left(\frac{n}{p}\right) G_1(p),$$
where we used that the Legendre symbol is multiplicative, and $\left(\frac{n^{-1}}{p}\right) = \left(\frac{n}{p}\right)$.

3. We compute
$$\begin{aligned}
G_p(1)^2 &= G_p(1)G_p(1) \\
&= \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right) e^{2\pi i a/p} \sum_{b\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{b}{p}\right) e^{2\pi i b/p} \\
&= \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \sum_{b\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{ab}{p}\right) e^{2\pi i(a+b)/p}.
\end{aligned}$$
As in the last item, we can replace a with ab, to write
$$\begin{aligned}
G_p(1)^2 &= \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \sum_{b\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{ab^2}{p}\right) e^{2\pi i(ab+b)/p} \\
&= \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right) \sum_{b\in(\mathbb{Z}/p\mathbb{Z})^*} e^{2\pi i b(a+1)/p}
\end{aligned}$$
The inner sum can be computed explicitly as
$$\sum_{b\in(\mathbb{Z}/p\mathbb{Z})^*} e^{2\pi i b(a+1)/p} = \sum_{b=0}^{p-1} e^{2\pi i b(a+1)/p} - 1 = \begin{cases} p-1, & a \equiv -1 \pmod p, \\ -1 & \text{else.} \end{cases}$$
Hence we find
$$G_p(1)^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{\substack{a\in(\mathbb{Z}/p\mathbb{Z})^* \\ a\not\equiv -1 \pmod p}} \left(\frac{a}{p}\right).$$

Recall that precisely half of the elemements in $(\mathbb{Z}/p\mathbb{Z})^*$ are quadratic residues, and the other half are quadratic non-residues, which implies $\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*}\left(\frac{a}{p}\right) = 0$. Hence

$$\sum_{\substack{a\in(\mathbb{Z}/p\mathbb{Z})^* \\ a\not\equiv -1 \pmod p}} \left(\frac{a}{p}\right) = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right) - \left(\frac{-1}{p}\right) = -\left(\frac{-1}{p}\right).$$

In total, we obtain

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

Problem 7 (sage)**.**

1. Write a program that computes the Legendre symbol $\left(\frac{a}{p}\right)$ by "brute force", that is, by checking if $x^2 \equiv a \pmod p$ has a solution. We will see a more efficient method in the next lecture.
2. We have seen above that $G_p(1) = \pm\sqrt{p}$ or $G_p(1) = \pm i\sqrt{p}$, depending on whether $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. Compute the Gauss sum $G_p(1)$ for several values of p and come up with a conjecture what the sign should be (the correct sign was determined by Gauss).