Elementary Number Theory - Exercise 6b

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Use Gauss' Lemma to show that the quadratic congruence $x^2 \equiv 3 \pmod{31}$ has no solutions.

Solution 1. We want to compute $\left(\frac{3}{31}\right)$ using Gauss' Lemma, so we need to count the number of least residues of $3, 6, 9, \ldots, \frac{p-1}{2} \cdot 3 = 15 \cdot 3$ modulo $p = 31$ which are larger than $\frac{p-1}{2} = 15$. The least residues are given by

$$3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 2, 5, 8, 11, 14,$$

of which precisely 5 are larger than 15. Hence, by Gauss' Lemma, we have

$$\left(\frac{3}{31}\right) = (-1)^5 = -1,$$

so the congruence $x^2 \equiv 3 \pmod{31}$ has no solutions.

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

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

Hint: Gauss' Lemma.

Solution 2. Applying Gauss' Lemma, we consider the elements $2, 4, 6, \ldots, 2\frac{p-1}{2} = p - 1$ and count the number s of least residues that exceed $p/2$. In this case, the numbers are already the least residues, so we only have to count how many of the numbers $2, 4, 6, \ldots, p - 1$ are larger than $p/2$. A number of the form $2n$ is smaller than $p/2$ if and only if $n \leq \lfloor p/4 \rfloor$. Hence, the number of elements of the form $2n$ which are larger than $p/2$ is

$$s = (p - 1)/2 - \lfloor p/4 \rfloor.$$

If $p \equiv 1 \pmod 8$, that is, $p = 8k + 1$, then $s = 4k - \lfloor 2k + 1/4 \rfloor = 4k - 2k = 2k$ is even, so $(-1)^s = 1$. The other three cases for p modulo 8 are analogous.

Problem 3. Let $p > 7$ be a prime.

1. Determine $\left(\frac{5}{p}\right)$ in terms of the class of p modulo 5.
2. Determine $\left(\frac{7}{p}\right)$ in terms of the class of p modulo 28.

Hint: Use quadratic reciprocity.

Solution 3. 1. By quadratic reciprocity we have

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right).$$

The quadratic residues modulo 5 are 1 and 4, so we find

$$\left(\frac{5}{p}\right) = \begin{cases} 1, & p \equiv 1,4 \pmod 5, \\ -1, & p \equiv 2,3 \pmod 5. \end{cases}$$

2. Again, by quadratic reciprocity we have

$$\left(\frac{7}{p}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{7}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right).$$

The quadratic residues modulo 7 are $1,2,4$ and the nonresidues are $3,5,6$. The sign $(-1)^{\frac{p-1}{2}}$ is given by

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

Hence the Legendre symbol equals $\left(\frac{7}{p}\right)$ equals 1 if $p \equiv 1 \pmod 4$ and $p \equiv 1,2,4 \pmod 7$, or if $p \equiv 3 \pmod 4$ and $p \equiv 3,5,6 \pmod 7$. Otherwise, the Legendre symbol equals -1. Going through all values modulo 28, we find

$$\left(\frac{7}{p}\right) = \begin{cases} 1, & 1,3,9,19,25,27 \pmod{28} \\ -1, & 5,11,13,15,17,23 \pmod{28}. \end{cases}$$

Problem 4. Compute $\left(\frac{83}{137}\right)$ using the Jacobi symbol (without completely factoring the numerator).

Solution 4. We compute, using quadratic reciprocity and the rule for $\left(\frac{2}{m}\right)$,

$$\begin{aligned}
\left(\frac{83}{137}\right) &= (-1)^{\frac{83-1}{2}\cdot\frac{137-1}{2}}\left(\frac{137}{83}\right) \\
&= \left(\frac{54}{83}\right) \\
&= \left(\frac{2}{83}\right)\left(\frac{27}{83}\right) \\
&= (-1)\cdot(-1)^{\frac{27-1}{2}\cdot\frac{83-1}{2}}\left(\frac{83}{27}\right) \\
&= \left(\frac{2}{27}\right) \\
&= -1.
\end{aligned}$$

Problem 5. 1. Show that a prime $p > 3$ is either 1 or -1 modulo 6.

2. Let $p > 3$ be a prime. Prove that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 6, \\ -1, & p \equiv -1 \pmod 6. \end{cases}$$

3. Show that there are infinitely many primes $p \equiv 1 \pmod 6$.
Hint: Consider $m = 12(p_1 \cdots p_k)^2 + 1$, where $p_1, \ldots, p_k$ are the primes $\equiv 1 \pmod 6$.

Solution 5. 1. The least residues modulo 6 are $0, 1, 2, 3, 4, 5$. A prime $p > 3$ cannot be $0, 2, 3$, or 4 mod 6, since then it would be divisible by $6, 2, 3$, or 2, respectively. Hence, a prime $p > 3$ is congruent to 1 or $5 \equiv -1$ modulo 6.

2. Using quadratic reciprocity, we find

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Each prime $p > 3$ satisfies $p \equiv \pm 1 \pmod 6$. If $p \equiv 1 \pmod 6$ then $p \equiv 1 \pmod 3$ and hence $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. If $p \equiv -1 \pmod 6$, then $p \equiv -1 \pmod 3$, so $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$.

3. Assume that there are only finitely many primes $p_1, \ldots, p_k$ equivalent to $1 \pmod 6$. Consider $m = 12(p_1 \cdots p_k)^2 + 1$, and let p be a prime dividing m (which exists since $m > 1$). Then p cannot be $2, 3$, or one of the primes $p_1, \ldots, p_k$, so we must have $p \equiv -1 \pmod 6$. Since p divides m, we have

$$-1 \equiv 12(p_1 \cdots p_k)^2 \pmod p.$$

Mutliplying by 3, we find

$$-3 \equiv 36(p_1 \cdots p_k)^2 \equiv (6p_1 \cdots p_k)^2 \pmod p,$$

so -3 is a square modulo p, contradicting the first item.

Problem 6. Let $p \neq q$ be odd primes, and put $p^* = \left(\frac{-1}{p}\right)p$. Show that the quadratic reciprocity law can equivalently be written as

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

Solution 6. The quadratic reciprocity law states that

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

If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = 1$ and $p^* = p$, and $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1$, so the quadratic reciprocity law is equivalent to $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$ in this case.

If $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ and $p^* = -p$, and $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}}$. Then we have

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

We see that the quadratic reciprocity law is again equivalent to $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$.

Problem 7 (sage)**.** Write a program that computes the Jacobi symbol, using the method from the lecture (that is, without factoring the numerator).