Quadratic residues and quadratic reciprocity law

Exercise 1.

1. For which odd primes is 3 a quadratic residue ?
2. Let p be an odd prime such that $q = 2p+1$ is also prime. Show that 2 is a generator of $\mathbb{F}_q^\times$ if and only if $p \equiv 1 \bmod 4$.
3. Let $p_1, \ldots, p_n$ be primes which are congruent to 3 modulo 8. Show that $N = (p_1 \ldots p_n)^2+2$ admits a prime factor congruent to 3 modulo 8 which is not $p_1, \ldots, p_n$. Conclude.
4. What prime numbers can be written as $a^2 + ab + b^2$, with $a, b \in \mathbb{Z}$?

Exercise 2. [Jacobi symbol] Let $a \in \mathbb{Z}$ and $b = \prod_{i=1}^r p_i^{n_i}$ with the p_i's odd prime numbers not dividing a. We define the Jacobi symbol of a modulo b by

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{n_i}.$$

1. Show that $\left(\frac{a}{b}\right)$ only depends on $a \bmod b$, and is multiplicative in both a and b.
2. Find an example where $\left(\frac{a}{b}\right) = 1$ yet a is not a quadratic residue modulo b.
3. Determine $\left(\frac{-1}{b}\right)$ and $\left(\frac{2}{b}\right)$.
4. Show that, if a is also odd, $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ is a or b is 1 modulo 4, and $\left(\frac{a}{b}\right) = -\left(\frac{b}{a}\right)$ otherwise.
5. Deduce an algorithm to compute any Jacobi symbol.
6. Compute $\left(\frac{7}{15}\right)$, $\left(\frac{12}{43}\right)$, $\left(\frac{13}{53}\right)$ and $\left(\frac{10}{99}\right)$.

Exercise 3. Let n be an integer which is not a square. We will show that n is not a quadratic residue modulo an infinite number of primes. In particular, an integer n such $\left(\frac{n}{p}\right) = 1$ for every large prime p is a square.

1. Show that we can assume n is square-free.
2. First, assume that $n \neq 2$, so we write $n = 2^e p_1 \ldots p_r$ with $e \in \{0, 1\}$ and the p_i's pairwise distinct prime numbers. Let s be a non-quadratic residue modulo p_r and $\ell_1, \ldots, \ell_k$ odd prime numbers different from $p_1, \ldots, p_r$. Find an integer m such that

$$\begin{cases} m \equiv 1 \bmod \ell_i \text{ for } 1 \leq i \leq k \\ m \equiv 1 \bmod 8 \\ m \equiv 1 \bmod p_j \text{ for } 1 \leq j \leq r-1 \\ m \equiv s \bmod p_r. \end{cases}$$

3. Show that $\left(\frac{n}{m}\right) = -1$, and deduce that there exists a prime number p different from $p_1, \ldots, p_r, \ell_1, \ldots, \ell_k$ such that n is not a quadratic residue modulo p and conclude.

4. In the case $n=2$, we build inductively odd primes $\ell_1,\dots,\ell_k$ different from 3 such that $\left(\frac{2}{\ell_i}\right)=-1$ for $1\le i\le k$ (starting with $\ell_1=5$). Let $m=8\ell_1\dots\ell_k+3$. Show that $\left(\frac{2}{m}\right)=-1$ and deduce that there exists a prime number p different from $\ell_1,\dots,\ell_k$ such that n is not a quadratic residue modulo p and conclude.

Remark. One can show that if n is not a square, then actually

$$\lim_{x\to+\infty}\frac{\#\{p\le x\mid \left(\frac{n}{p}\right)=1\}}{\#\{p\le x\}}=\frac{1}{2},$$

in other words, n is a quadratic residue modulo primes "half of the time".

Exercise 4. [Gaussian sums] Let $p=2u-1$ be an odd prime number, $\zeta_p=e^{\frac{2i\pi}{p}}$ and $G_p=\sum_{a\in\mathbb{Z}/p\mathbb{Z}}\left(\frac{a}{p}\right)\zeta_p^a$. Recall we've shown in TD4, Exercise 5, that $G_p^2=p^*$, where

$$p^*=\begin{cases}p \text{ if } p\equiv 1 \bmod 4\\ -p \text{ if } p\equiv 3 \bmod 4.\end{cases}$$

Therefore,

$$G_p=\begin{cases}\pm\sqrt{p} \text{ if } p\equiv 1 \bmod 4\\ \pm i\sqrt{p} \text{ if } p\equiv 3 \bmod 4.\end{cases}$$

We now determine the sign.

1. Show that $\prod_{k=1}^{\frac{p-1}{2}}(\zeta_p^{ku}-\zeta_p^{-ku})^2=p^*$. (*Hint :* Recall that $\prod_{i=1}^{p-1}(1-\zeta_p)=p$)
2. Show that
$$\prod_{k=1}^{\frac{p-1}{2}}(\zeta_p^{2k-1}-\zeta_p^{-2k+1})=\begin{cases}\sqrt{p} \text{ if } p\equiv 1 \bmod 4\\ i\sqrt{p} \text{ if } p\equiv 3 \bmod 4.\end{cases}$$

   We now write $G_p=\varepsilon\prod_{k=1}^{\frac{p-1}{2}}(\zeta_p^{ku}-\zeta_p^{-ku})$, with $\varepsilon=\pm1$.
3. Let $P=\sum_{k=0}^{p-1}\left(\frac{k}{p}\right)X^k-\varepsilon\prod_{k=1}^{\frac{p-1}{2}}(X^{ku}-X^{p-ku})$. Show that $\Phi_p\mid P$ in $\mathbb{Z}[X]$.
4. Let $Y=X-1$. Show that $P\equiv 0 \bmod (p,Y^{p-1})$.
5. Show that
$$P\equiv\left(\frac{-1}{((p-1)/2)!}-\varepsilon\left(\frac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}}\right)Y^{\frac{p-1}{2}} \bmod (p,Y^{\frac{p+1}{2}}).$$

   (*Hint :* Expand both terms in P with respect to $X=1+Y$. For the product, treat each term separately modulo Y^2)
6. Conclude.