Exercise 1)
Let $p$ be an odd prime number and denote by $q(p)$ the smallest positive quadratic non-residue modulo $p$. Show that $q(p) < 1 + \sqrt{p}$.
Hint: Consider $b > 0$ minimal with the property that $q(p)b > p$.

Exercise 2)
In the lecture we proved Linnik’s theorem which we can state as follows.

**Theorem 0.1.** Let $\varepsilon > 0$ and $N \in \mathbb{N}$. Then there is a constant $C(\varepsilon)$ (which is independent of $N$) such that there are at most $C(\varepsilon)$ prime numbers $p \leq N$ with the property that the smallest quadratic non-residue modulo $p$ is larger than $N^\varepsilon$.

Deduce from Linnik’s theorem the following corollary.

**Corollary 0.2.** Let $\varepsilon > 0$ and $x > 0$. Denote by $U(x)$ the number of primes $p \leq x$ such that the smallest quadratic non-residue is larger than $p^\varepsilon$. Then

$$U(x) \ll \varepsilon \log \log x.$$  

Exercise 3)
Fix integers $M$ and $N > 0$. Let $a_n \in \mathbb{C}$ for $n \in \mathbb{N}$ and assume that $a_n = 0$ if $n \notin (M, M + N]$. Let

$$S(\alpha) = \sum_{n \in \mathbb{Z}} a_n e(\alpha n).$$

For all primes $p$ set

$$\omega'(p) = \sharp \{ h \text{ mod } p : a_n = 0 \, \forall n \equiv h \text{ mod } p \}.$$ 

Assume that $\omega'(p) < p$ for all $p$ and define the multiplicative function

$$g'(q) = \mu^2(q) \prod_{p | q} \omega'(p)^{\omega'(p)/p}.$$  

In order to establish Montgomery’s sieve we used in the lecture the inequality

$$g'(q) \sum_{n \in \mathbb{Z}} |a_n|^2 \leq \sum_{q = 1}^Q \left| S \left( \frac{a}{q} \right) \right|^2,$$  

which holds for any integer $q \geq 1$. We proved this inequality in the lecture for the case that $q = p$ is a prime. The goal of this exercise is to show that one
can reduce the general case to the case that $q = p$ and hence finish the proof of this inequality for any $q$. For this discuss the following steps.

a) Show that the inequality (0.1) holds if and only if for all $\beta \in \mathbb{R}$ one has the inequality

$$|S(\beta)|^2 g'(q) \leq \sum_{\substack{a=1 \\ \gcd(a,q) = 1}}^q \left| S \left( \frac{a}{q} + \beta \right) \right|^2.$$

b) Discuss what happens to the inequality (0.1) in the case that $q$ is not square-free.

c) Let $q, q' \in \mathbb{N}$ with $\gcd(q, q') = 1$. Assume that the inequality (0.1) holds for both $q$ and $q'$. Deduce that (0.1) then also holds for the product $qq'$. Hint: If $\gcd(c, qq') = 1$ then there are numbers $a$ and $b$ with $\gcd(a, q) = 1$ and $\gcd(b, q') = 1$ such that

$$S \left( \frac{c}{qq'} \right) = S \left( \frac{a}{q} + \frac{b}{q'} \right).$$

Now make use of part a).