CHAPTER 4

Quadratic Residues

4.1. Introduction

In this chapter, we are concerned with the quadratic congruences of the form

$$x^2 \equiv a \bmod p, \tag{4.1}$$

where $p \in \mathbb{N}$ is an odd prime and $a \in \mathbb{Z}$. We are interested in determining whether for given p and a, the congruence (4.1) has a solution $x \in \mathbb{Z}$.

If $a \equiv 0 \bmod p$, then clearly (4.1) is soluble, with $x \equiv 0 \bmod p$ being the only solution. We therefore make the assumption that $a \not\equiv 0 \bmod p$. If (4.1) is soluble, then we say that a is a quadratic residue modulo p. If (4.1) is not soluble, then we say that a is a quadratic non-residue modulo p.

THEOREM 4.1. *Suppose that $p \in \mathbb{N}$ is an odd prime. Then there are precisely $(p-1)/2$ quadratic residues modulo p, and these are represented by the numbers*

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{4.2}$$

PROOF. Suppose that $p \nmid a$. Then it follows from Lagrange's theorem that the congruence (4.1) has at most two solutions. On the other hand, if $x \equiv b \bmod p$ is a solution, then it is easy to check that $x \equiv p-b \bmod p$ represents another solution. It follows that the congruence (4.1) has either two solutions or no solutions. Note next that any solution of the congruence (4.1) must be of the form $x \equiv b \bmod p$, with $1 \leqslant b \leqslant p-1$. It follows that there can be at most $(p-1)/2$ quadratic residues modulo p. It remains to show that there are at least $(p-1)/2$ quadratic residues modulo p. To do so, note that the $(p-1)/2$ numbers in (4.2) are clearly quadratic residues modulo p. It therefore suffices to show that they are incongruent modulo p. Suppose on the contrary that $x^2 \equiv y^2 \bmod p$, with $1 \leqslant x < y \leqslant (p-1)/2$. Then $p \mid (y-x)(y+x)$, a contradiction since p is prime and $0 < y-x < y+x < p$. ◯

It is convenient to introduce the Legendre symbol, defined as follows. Suppose that $p \in \mathbb{N}$ is an odd prime. Then we write

$$\left(\frac{a}{p}\right)_L = \begin{cases} 1, & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{if } p \nmid a \text{ and } a \text{ is a quadratic non-residue modulo } p, \\ 0, & \text{if } p \mid a. \end{cases}$$

4.2. The Legendre Symbol

In this section, we analyze the Legendre symbol in a systematic way to provide some practical means of evaluating it. Our first step is not particularly useful in itself, but provides a path towards results of a more practical nature.

THEOREM 4.2 (Euler's criterion). *Suppose that $p \in \mathbb{N}$ is an odd prime. For every $a \in \mathbb{Z}$, we have*

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

PROOF. The result clearly holds if $p \mid a$, so we assume now that $p \nmid a$. If a is a quadratic residue modulo p, then there exists $x \in \mathbb{Z}$ such that $p \nmid x$ and $x^2 \equiv a \bmod p$. It follows from Fermat's little theorem that

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

Consider next the congruence

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \bmod p.$$

By Fermat's little theorem, this has $p-1$ solutions. However, it follows from Lagrange's theorem that neither

$$a^{\frac{p-1}{2}} - 1 \equiv 0 \bmod p \tag{4.3}$$

nor

$$a^{\frac{p-1}{2}} + 1 \equiv 0 \bmod p \tag{4.4}$$

has more than $(p-1)/2$ solutions. Hence each of (4.3) and (4.4) has exactly $(p-1)/2$ solutions. The $(p-1)/2$ quadratic residues a modulo p all satisfy (4.3). It follows that all the quadratic non-residues a must satisfy (4.4). ○

We have immediately the following two consequences.

THEOREM 4.3. *Suppose that $p \in \mathbb{N}$ is an odd prime. Then*

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

PROOF. Taking $a = 1$ in Theorem 4.2, we obtain

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

Note, however, that

$$\left(\frac{-1}{p}\right)_L - (-1)^{\frac{p-1}{2}} \in \{-2, 0, 2\}.$$

The result follows. ○

THEOREM 4.4. *Suppose that $p \in \mathbb{N}$ is an odd prime. Then for every $a, b \in \mathbb{Z}$, we have*

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

PROOF. The result is trivial if $p \mid a$ or $p \mid b$, so we assume now that $p \nmid a$ and $p \nmid b$. It follows from Theorem 4.2 that

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

Note, however, that

$$\left(\frac{ab}{p}\right)_L - \left(\frac{a}{p}\right)_L \left(\frac{b}{p}\right)_L \in \{-2, 0, 2\}.$$

The result follows. ○

In practice, Euler's criterion is not very useful when p is a rather large prime. The following represents a result of a more practical nature.

THEOREM 4.5 (Gauss's lemma). *Suppose that $p \in \mathbb{N}$ is an odd prime, and that the integer $a \in \mathbb{Z}$ satisfies $p \nmid a$. Let*

$$m = \#\left\{x \in \mathbb{N} : 1 \leqslant x < \frac{p}{2} \text{ and } \frac{p}{2} < ax - p\left[\frac{ax}{p}\right] < p\right\};$$

in other words, m is the number of integers x satisfying $1 \leqslant x < p/2$ for which the residue r_x of ax satisfies $p/2 < r_x < p$. Then

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

PROOF. By Euler's criterion, we have

$$\prod_{x=1}^{\frac{p-1}{2}} r_x \equiv \prod_{x=1}^{\frac{p-1}{2}} ax = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{a}{p}\right)_L \left(\frac{p-1}{2}\right)! \bmod p. \tag{4.5}$$

Let $\alpha_1, \ldots, \alpha_m$ denote the m values of r_x for which $p/2 < r_x < p$, and let $\beta_1, \ldots, \beta_\ell$ denote the ℓ values of r_x for which $0 < r_x < p/2$, with $\ell + m = (p-1)/2$. Then

$$\prod_{x=1}^{\frac{p-1}{2}} r_x = \left(\prod_{i=1}^{m} \alpha_i\right)\left(\prod_{j=1}^{\ell} \beta_j\right) \equiv (-1)^m \left(\prod_{i=1}^{m}(p-\alpha_i)\right)\left(\prod_{j=1}^{\ell} \beta_j\right) \bmod p. \tag{4.6}$$

For every $i = 1, \ldots, m$, we have $0 < p - \alpha_i < p/2$. Also, for every $j = 1, \ldots, \ell$, we have $0 < \beta_j < p/2$. Note also that the numbers $\alpha_1, \ldots, \alpha_m$ are distinct, and the numbers $\beta_1, \ldots, \beta_\ell$ are also distinct. Furthermore, for every $i = 1, \ldots, m$ and every $j = 1, \ldots, \ell$, the numbers $p - \alpha_i$ and β_j are different, for $p - \alpha_i = \beta_j$ would give $ax \equiv -ay \bmod p$, and hence $x + y \equiv 0 \bmod p$, for some $x, y \in \mathbb{Z}$ satisfying $1 \leqslant x < y \leqslant (p-1)/2$, clearly impossible. Hence

$$\left(\prod_{i=1}^{m}(p-\alpha_i)\right)\left(\prod_{j=1}^{\ell} \beta_j\right) = \left(\frac{p-1}{2}\right)!. \tag{4.7}$$

The result now follows on combining (4.5)–(4.7). ○

THEOREM 4.6. *Suppose that $p \in \mathbb{N}$ is an odd prime. Then*

$$\left(\frac{2}{p}\right)_L = (-1)^{[\frac{p}{2}]-[\frac{p}{4}]} = (-1)^{\frac{p^2-1}{8}}.$$

PROOF. The numbers $2, 4, 6, \ldots, p-1$ all lie between 0 and p, and so are their own residues modulo p. Moreover, $p/2 < 2x < p$ if and only if $p/4 < x < p/2$. Hence $m = [p/2] - [p/4]$. The second equality is obtained easily by checking. ○

4.3. Quadratic Reciprocity

Suppose that $p, q \in \mathbb{N}$ are distinct odd primes. There is a beautiful result which links the solubility of the two quadratic congruences

$$x^2 \equiv q \bmod p \quad \text{and} \quad x^2 \equiv p \bmod q,$$

in the sense that if we know whether one of these two congruences is soluble, then the determination of whether the other congruence is soluble involves only a simple calculation.

THEOREM 4.7 (Law of quadratic reciprocity). *Suppose that $p, q \in \mathbb{N}$ are distinct odd primes. Then*

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

Theorem 4.7 will follow from the following three results.

THEOREM 4.8. *Suppose that $p \in \mathbb{N}$ is an odd prime, and that the integer $a \in \mathbb{Z}$ satisfies $p \nmid a$. Then*

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

where

$$n=\sum_{y=1}^{\frac{p-1}{2}}\left[\frac{2ay}{p}\right].$$

PROOF. We use Gauss's lemma. In the notation of Theorem 4.5, we have

$$m=\#\left\{x\in\mathbb{N}:1\leqslant x\leqslant\frac{p-1}{2},\ 1<\frac{2ax}{p}-2\left[\frac{ax}{p}\right]<2\right\}.$$

Also, for any $x\in\mathbb{Z}$ satisfying $1\leqslant x\leqslant (p-1)/2$, we must have

$$0<\frac{2ax}{p}-2\left[\frac{ax}{p}\right]<2.$$

Hence

$$m=\sum_{x=1}^{\frac{p-1}{2}}\left[\frac{2ax}{p}-2\left[\frac{ax}{p}\right]\right]\equiv n \bmod 2,$$

and this completes the proof. ○

THEOREM 4.9. *Suppose that $p,q\in\mathbb{N}$ are distinct odd primes. Then*

$$\left(\frac{q}{p}\right)_L=(-1)^{\lambda(p,q)},$$

where

$$\lambda(p,q)=\sum_{x=1}^{\frac{p-1}{2}}\left[\frac{qx}{p}\right].$$

PROOF. Suppose that $a\in\mathbb{Z}$ is odd. Then $2\mid(a+p)$, and

$$\left(\frac{\frac{1}{2}(a+p)}{p}\right)_L=\left(\frac{4}{p}\right)_L\left(\frac{\frac{1}{2}(a+p)}{p}\right)_L=\left(\frac{2(a+p)}{p}\right)_L=\left(\frac{2a}{p}\right)_L=\left(\frac{2}{p}\right)_L\left(\frac{a}{p}\right)_L,$$

in view of Theorem 4.4. It follows from Theorem 4.8 that

$$\left(\frac{2}{p}\right)_L\left(\frac{a}{p}\right)_L=\left(\frac{\frac{1}{2}(a+p)}{p}\right)_L=(-1)^r,$$

where

$$r=\sum_{y=1}^{\frac{p-1}{2}}\left[\frac{(a+p)y}{p}\right].$$

Now

$$\sum_{y=1}^{\frac{p-1}{2}}\left[\frac{(a+p)y}{p}\right]=\sum_{y=1}^{\frac{p-1}{2}}\left(\left[\frac{ay}{p}\right]+y\right)=\sum_{y=1}^{\frac{p-1}{2}}\left[\frac{ay}{p}\right]+\frac{p^2-1}{8}.$$

Putting $a=1$, we deduce (again) that

$$\left(\frac{2}{p}\right)_L=(-1)^{\frac{p^2-1}{8}}.$$

It now follows that for odd prime q, we must have

$$\left(\frac{q}{p}\right)_L=(-1)^s,$$

where

$$s=\sum_{y=1}^{\frac{p-1}{2}}\left[\frac{qy}{p}\right],$$

and this completes the proof. ○

THEOREM 4.10. *Suppose that $p, q \in \mathbb{N}$ are distinct odd primes. In the notation of Theorem 4.9, we have*

$$\lambda(p,q) + \lambda(q,p) = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right).$$

PROOF. We have

$$\lambda(p,q) = \sum_{1 \leqslant x < \frac{p}{2}} \left[\frac{qx}{p}\right] = \sum_{1 \leqslant x < \frac{p}{2}} \sum_{1 \leqslant y < \frac{qx}{p}} 1 = \sum_{1 \leqslant y < \frac{q}{2}} \sum_{\frac{py}{q} < x < \frac{p}{2}} 1,$$

since $qx/p \notin \mathbb{Z}$ when $x < p$. Also,

$$\lambda(q,p) = \sum_{1 \leqslant y < \frac{q}{2}} \sum_{1 \leqslant x < \frac{py}{q}} 1.$$

It follows that

$$\lambda(p,q) + \lambda(q,p) = \sum_{1 \leqslant y < \frac{q}{2}} \sum_{1 \leqslant x < \frac{p}{2}} 1 = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right),$$

since both p and q are odd. ○

EXAMPLE. The numbers 8783 and 15671 are prime. We want to determine the number of solutions of the congruence $x^2 \equiv 8783 \bmod 15671$. We have

$$\left(\frac{8783}{15671}\right)_L = (-1)^{\left(\frac{8783-1}{2}\right)\left(\frac{15671-1}{2}\right)} \left(\frac{15671}{8783}\right)_L = -\left(\frac{15671}{8783}\right)_L = -\left(\frac{6888}{8783}\right)_L$$

$$= -\left(\frac{2}{8783}\right)_L^3 \left(\frac{3}{8783}\right)_L \left(\frac{7}{8783}\right)_L \left(\frac{41}{8783}\right)_L = -\left(\frac{2}{8783}\right)_L \left(\frac{3}{8783}\right)_L \left(\frac{7}{8783}\right)_L \left(\frac{41}{8783}\right)_L.$$

Next, note that

$$\left(\frac{2}{8783}\right)_L = -(-1)^{\left[\frac{8783}{2}\right]-\left[\frac{8783}{4}\right]},$$

$$\left(\frac{3}{8783}\right)_L = (-1)^{\left(\frac{3-1}{2}\right)\left(\frac{8783-1}{2}\right)} \left(\frac{8783}{3}\right)_L,$$

$$\left(\frac{7}{8783}\right)_L = (-1)^{\left(\frac{7-1}{2}\right)\left(\frac{8783-1}{2}\right)} \left(\frac{8783}{7}\right)_L,$$

$$\left(\frac{41}{8783}\right)_L = (-1)^{\left(\frac{41-1}{2}\right)\left(\frac{8783-1}{2}\right)} \left(\frac{8783}{41}\right)_L.$$

It follows that

$$\left(\frac{8783}{15671}\right)_L = -\left(\frac{8783}{3}\right)_L \left(\frac{8783}{7}\right)_L \left(\frac{8783}{41}\right)_L = -\left(\frac{2}{3}\right)_L \left(\frac{5}{7}\right)_L \left(\frac{9}{41}\right)_L = -(-1)^{\frac{9-1}{8}} \left(\frac{5}{7}\right)_L \left(\frac{3}{41}\right)_L^2$$

$$= \left(\frac{5}{7}\right)_L = (-1)^{\left(\frac{5-1}{2}\right)\left(\frac{7-1}{2}\right)} \left(\frac{7}{5}\right)_L = \left(\frac{7}{5}\right)_L = \left(\frac{2}{5}\right)_L = (-1)^{\frac{25-1}{8}} = -1.$$

Hence the congruence has no solutions.

4.4. The Jacobi Symbol

To shorten many calculations involving the Legendre symbol, we introduce the Jacobi symbol which can be considered in some way to be a generalization of the Legendre symbol. For every $n \in \mathbb{Z}$, we write

$$\left(\frac{n}{1}\right)_J = 1.$$

If m is a positive odd integer with canonical decomposition $m = p_1^{u_1} \ldots p_r^{u_r}$, where $p_1, \ldots, p_r$ are distinct odd primes, then we write

$$\left(\frac{n}{m}\right)_J = \prod_{i=1}^{r} \left(\frac{n}{p_i}\right)_L^{u_i}.$$

Remark. We emphasize immediately that the Jacobi symbol is for calculation only. In particular, note that

$$\left(\frac{n}{m}\right)_J = 1$$

does not necessarily imply that the congruence $x^2 \equiv n \bmod m$ is soluble. Consider, for example, the case when $n = 2$ and $m = 15$.

The following observations can be deduced from the properties of the Legendre symbol. We leave the proof as an exercise for the reader.

Theorem 4.11. *Suppose that m and m' are odd positive integers. Then for every $n, n' \in \mathbb{Z}$, we have*

(i) $\left(\frac{n}{m}\right)_J \left(\frac{n'}{m}\right)_J = \left(\frac{nn'}{m}\right)_J$;

(ii) $\left(\frac{n}{m}\right)_J \left(\frac{n}{m'}\right)_J = \left(\frac{n}{mm'}\right)_J$;

(iii) $\left(\frac{n}{m}\right)_J = \left(\frac{n'}{m}\right)_J$ *whenever* $n \equiv n' \bmod m$; *and*

(iv) $\left(\frac{a^2 n}{m}\right)_J = \left(\frac{n}{m}\right)_J$ *whenever* $(a, m) = 1$.

Theorem 4.12. *Suppose that m is an odd positive integer. Then*

$$\left(\frac{-1}{m}\right)_J = (-1)^{\frac{m-1}{2}} \quad \text{and} \quad \left(\frac{2}{m}\right)_L = (-1)^{\frac{m^2-1}{8}}.$$

Proof. It is convenient to write $m = p_1 \dots p_s$, where the prime factors are not necessarily distinct. Then

$$m = \prod_{j=1}^{s}(1 + p_j - 1) = 1 + \sum_{j=1}^{s}(p_j - 1) + \sum_{j=1}^{s}\sum_{\substack{k=1 \\ j\neq k}}^{s}(p_j - 1)(p_k - 1) + \ldots \equiv 1 + \sum_{j=1}^{s}(p_j - 1) \bmod 4,$$

and so

$$\frac{m-1}{2} \equiv \sum_{j=1}^{s} \frac{p_j - 1}{2} \bmod 2.$$

Thus

$$\left(\frac{-1}{m}\right)_J = \prod_{j=1}^{s} \left(\frac{-1}{p_j}\right)_L = \prod_{j=1}^{s}(-1)^{\frac{p_j-1}{2}} = (-1)^{\frac{m-1}{2}},$$

proving the first assertion. Similarly, we can write

$$m^2 = \prod_{j=1}^{s}(1 + p_j^2 - 1) = 1 + \sum_{j=1}^{s}(p_j^2 - 1) + \sum_{j=1}^{s}\sum_{\substack{k=1 \\ j\neq k}}^{s}(p_j^2 - 1)(p_k^2 - 1) + \ldots \equiv 1 + \sum_{j=1}^{s}(p_j^2 - 1) \bmod 16,$$

and so

$$\frac{m^2-1}{8} \equiv \sum_{j=1}^{s} \frac{p_j^2 - 1}{8} \bmod 2.$$

Thus

$$\left(\frac{2}{m}\right)_J = \prod_{j=1}^{s} \left(\frac{2}{p_j}\right)_L = \prod_{j=1}^{s}(-1)^{\frac{p_j^2-1}{8}} = (-1)^{\frac{m^2-1}{8}},$$

proving the second assertion. ○

We leave it as an exercise for the reader to prove the following reciprocity result.

Theorem 4.13. *Suppose that m and n are odd positive integers and $(m, n) = 1$. Then*

$$\left(\frac{m}{n}\right)_J \left(\frac{n}{m}\right)_J = (-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)}.$$

EXAMPLE. Let us consider our earlier example again. Recall that we want to determine the number of solutions of the congruence $x^2 \equiv 8783 \bmod 15671$, where the numbers 8783 and 15671 are prime. Omitting the details of a few steps from earlier, we have

$$\begin{aligned}\left(\frac{8783}{15671}\right)_L &= -\left(\frac{6888}{8783}\right)_L = -\left(\frac{2}{8783}\right)_L^3\left(\frac{861}{8783}\right)_L = -\left(\frac{861}{8783}\right)_L = -\left(\frac{861}{8783}\right)_J \\ &= -(-1)^{\left(\frac{861-1}{2}\right)\left(\frac{8783-1}{2}\right)}\left(\frac{8783}{861}\right)_L = -\left(\frac{8783}{861}\right)_L = -\left(\frac{173}{861}\right)_L \\ &= -(-1)^{\left(\frac{173-1}{2}\right)\left(\frac{861-1}{2}\right)}\left(\frac{861}{173}\right)_L = -\left(\frac{861}{173}\right)_L = -\left(\frac{-4}{173}\right)_L \\ &= -\left(\frac{-1}{173}\right)_L\left(\frac{2}{173}\right)_L^2 = -\left(\frac{-1}{173}\right)_L = -(-1)^{\frac{173-1}{2}} = -1.\end{aligned}$$

Alternatively, try to fill in the missing details in the argument below. We have

$$\begin{aligned}\left(\frac{8783}{15671}\right)_L &= -\left(\frac{15671}{8783}\right)_L = -\left(\frac{-1895}{8783}\right)_L = -\left(\frac{8783}{1895}\right)_J \\ &= -\left(\frac{8783}{5}\right)_J\left(\frac{8783}{379}\right)_J = -\left(\frac{379}{33}\right)_J = -\left(\frac{16}{33}\right)_J = -1.\end{aligned}$$

4.5. The Distribution of Quadratic Residues

Suppose that the prime $p \in \mathbb{N}$ satisfies $p \equiv 1 \bmod 8(k!)$, where $k \in \mathbb{N}$. Then it is not difficult to see that 2 is a quadratic residue modulo p. Furthermore, for any odd prime $q \in \mathbb{N}$ such that $q \leqslant k$ and $q \neq p$, we have

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

so that q is a quadratic residue modulo p. Suppose now that $n \in \mathbb{N}$ satisfies $n \leqslant k$. Then all the prime factors of n do not exceed k. It follows from Theorem 4.4 that n is a quadratic residue modulo p.

Now let n_p denote the least positive quadratic non-residue modulo p. For the prime p above, we have $n_p > k$. It follows that

$$\limsup_{p\to\infty} n_p = \infty.$$

In 1919, Vinogradov conjectured that for any $\epsilon > 0$, we have $n_p \ll_\epsilon p^\epsilon$ as $p \to \infty$. Here we prove the following weaker result.

THEOREM 4.14. *For every odd prime $p \in \mathbb{N}$, we have*

$$n_p \leqslant \frac{1}{2} + \left(p + \frac{1}{4}\right)^{\frac{1}{2}}. \tag{4.8}$$

PROOF. Let $h = [p/n_p] + 1$. Then $p < hn_p < p + n_p$, so that $(hn_p/p)_L = 1$. Since $(n_p/p)_L = -1$, it follows from Theorem 4.4 that $(h/p)_L = -1$. Note now that since $0 < h < p/2 + 1 < p$, we must have $1 \leqslant h < p$, so that $h \geqslant n_p$. We therefore conclude that

$$n_p \leqslant \left[\frac{p}{n_p}\right] + 1 \leqslant \frac{p}{n_p} + 1.$$

The inequality (4.8) follows. ◯