i.e. as the infinite continued fraction

$$x_0 = a_0 + \cfrac{|a_1|}{|b_1|} + \cfrac{|a_2|}{|b_2|} + \dots \tag{58}$$

This proves the following theorem:

*For any infinite sequence of natural numbers $b_1, b_2, \dots$ in which infinitely many terms are different from* 1, *any real number $x_0$ may be represented as an infinite continued fraction of form* (58), *where $a_0 = [x_0]$, $a_n$ $(n = 1, 2, \dots)$ are integers $0 \leqslant a_n < b_n$ for $n = 1, 2, \dots$*

As is easy to see, representation (57) coincides with the representation as a decimal with the varying base which was considered in Chapter VII, § 6.

CHAPTER IX

## LEGENDRE'S SYMBOL AND JACOBI'S SYMBOL

**§ 1. Legendre's symbol $\left(\frac{D}{p}\right)$ and its properties.** If $p$ is an odd prime and $D$ an integer not divisible by $p$, Legendre's symbol $\left(\frac{D}{p}\right)$ is said to be equal to 1 if $D$ is a quadratic residue to the modulus $p$, and it is said to be equal to $-1$ if $D$ is a quadratic non-residue to $p$.

In view of theorem 4 of Chapter V, we have

$$\left(\frac{D}{p}\right) \equiv D^{\frac{1}{2}(p-1)} (\mathrm{mod}\, p). \tag{1}$$

Consequently, the value of $\left(\frac{D}{p}\right)$ is 1 if and only if $D^{(p-1)/2}$ divided by $p$ leaves the remainder 1.

By theorem 15 of Chapter VI, we have

$$\left(\frac{D}{p}\right) = (-1)^{\mathrm{ind}\, D}, \tag{2}$$

where the indices are taken relative to a primitive root of the prime $p$.

If $D$ and $D'$ are integers not divisible by a prime $p$, then, by (1), the following property holds:

I. *If* $D \equiv D' (\mathrm{mod}\, p)$, *then* $\left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right)$.

From (2) it follows that if $D$ and $D'$ are integers not divisible by $p$, then

$$\left(\frac{DD'}{p}\right) = (-1)^{\mathrm{ind}\, DD'} \quad \text{and} \quad \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right) = (-1)^{\mathrm{ind}\, D + \mathrm{ind}\, D'}. \tag{3}$$

But, according to property II of indices (see Chapter VI, § 8), we have $\mathrm{ind}\, DD' \equiv \mathrm{ind}\, D + \mathrm{ind}\, D' (\mathrm{mod}\, p-1)$. Hence, since $p$ is an odd

prime, and *a fortiori*, we have $\operatorname{ind} DD' \equiv \operatorname{ind} D + \operatorname{ind} D' \pmod 2$, whence $(-1)^{\operatorname{ind} DD'} = (-1)^{\operatorname{ind} D + \operatorname{ind} D'}$. Consequently, by (3), $\left(\frac{DD'}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right)$. Thus we have proved

II. *If $D$ and $D'$ are integers not divisible by $p$, then*

$$\left(\frac{DD'}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right).$$

Now we prove (cf. Sierpiński [2]) that if $\left\{\frac{D}{p}\right\}$ is a real number defined for a fixed odd prime $p$ and any integer $D$ not divisible by $p$, which is different from zero for at least one value of $D$ and different from 1 for at least one $D$ and which, moreover, satisfies the conditions

1° if $D \equiv D' \pmod p$, then $\left\{\frac{D}{p}\right\} = \left\{\frac{D'}{p}\right\}$,

2° $\left\{\frac{DD'}{p}\right\} = \left\{\frac{D}{p}\right\}\left\{\frac{D'}{p}\right\}$ for any $D$ and $D'$ that are not divisible by $p$,

then for any integer $D$ not divisible by $p$ we have

$$\left\{\frac{D}{p}\right\} = \left(\frac{D}{p}\right). \tag{4}$$

Let $g$ be a primitive root of the prime $p$. For any integer $D$ that is not divisible by $p$ we have $D \equiv g^{\operatorname{ind} D} \pmod p$. Hence, in virtue of properties 1° and 2° of the symbol $\left\{\frac{D}{p}\right\}$, we have

$$\left\{\frac{D}{p}\right\} = \left\{\frac{g^{\operatorname{ind} D}}{p}\right\} = \left\{\frac{g}{p}\right\}^{\operatorname{ind} D}. \tag{5}$$

Let $\left\{\frac{g}{p}\right\} = a$. Since $g^{p-1} \equiv 1 \pmod p$, by 1° and 2°, the equalities $a^{p-1} = \left\{\frac{g}{p}\right\}^{p-1} = \left\{\frac{g^{p-1}}{p}\right\} = \left\{\frac{1}{p}\right\}$ hold, but, in view of 2°, $\left\{\frac{1}{p}\right\}^2 = \left\{\frac{1}{p}\right\}$, whence $\left\{\frac{1}{p}\right\} = 0$ or $\left\{\frac{1}{p}\right\} = 1$. We cannot have $\left\{\frac{1}{p}\right\} = 0$ because, if that were the case then, by 2° (for $D' = 1$), we would have $\left\{\frac{D}{p}\right\} = \left\{\frac{D}{p}\right\}\left\{\frac{1}{p}\right\} = 0$, contrary to the assumption that $\left\{\frac{D}{p}\right\}$ is not identically equal to zero (if $D$ is not divisible by $p$). Therefore $\left\{\frac{1}{p}\right\} = 1$, and so $a^{p-1} = 1$. But $a = \left\{\frac{g}{p}\right\}$ is a real number and the equation $x^{p-1} = 1$, $p$ being odd, has precisely two roots, 1 and $-1$. Consequently $a = 1$ or $a = -1$. If $a = 1$, then, by (5), for every integer $D$ not divisible by $p$ we have $\left\{\frac{D}{p}\right\} = 1$, contrary to the assumption that $\left\{\frac{D}{p}\right\}$ is not identically equal to 1 ($D$ not being divisible by $p$). Consequently,



we must have $a = -1$, whence, by (5), we obtain $\left\{\frac{D}{p}\right\} = (-1)^{\operatorname{ind} D}$. So, by (2), $\left\{\frac{D}{p}\right\} = \left(\frac{D}{p}\right)$. The theorem is thus proved. It follows that any property of Legendre's symbol can be deduced from properties I and II and the fact that $\left\{\frac{D}{p}\right\}$ is not identically equal to 1 or to 0 for any odd prime $p$.

Formula (1) implies that

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

In order to deduce some further properties of Legendre's symbol we prove the following

LEMMA OF GAUSS. $\left(\frac{D}{p}\right) = (-1)^{\lambda}$, *where $\lambda$ is the number of the residues* mod $p$ *that appear in the sequence*

$$D,\ 2D,\ 3D,\ \ldots,\ \tfrac{1}{2}(p-1)D \tag{6}$$

*and that are greater than $p/2$.*

Proof. For $k = 1, 2, \ldots, (p-1)/2$, let $r_k$ denote the remainder left by $kD$ divided by $p$; we set $\varrho_k = r_k$ if $r_k < p/2$ or $\varrho_k = p - r_k$ if $r_k > p/2$. (The equality $r_r = p/2$ is impossible since, by assumption, $p$ is an odd prime.)

Since $D$ is not divisible by $p$ and in sequence (6) the coefficients at $D$ are natural numbers $\leqslant (p-1)/2$, neither the sum nor the difference of any two terms of sequence (6) is divisible by $p$. Hence it easily follows that the sum and the difference of any two different terms of the sequence

$$\varrho_1, \varrho_2, \ldots, \varrho_{\frac{p-1}{2}}, \tag{7}$$

are indivisible by $p$. But, according to the definition of numbers $\varrho_k$, they are all greater than zero and less than $(p-1)/2$ (because either $\varrho_k = r_k < p/2$, whence $2\varrho_k < p$, i.e. $2\varrho_k \leqslant p-1$, or $\varrho_k = p - r_k$ and $r_k > p/2$, whence $\varrho_k < p/2$ again). Since, by the property of the numbers of sequence (7) proved above, terms at different places are different, we infer that the numbers of (7) are (in a certain order) equal to the numbers $1, 2, \ldots, (p-1)/2$. Hence

$$\varrho_1 \varrho_2 \ldots \varrho_{\frac{p-1}{2}} = \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! D^{p-1} \pmod p, \tag{8}$$

the congruence being valid since, in view of the theorem of Fermat, $D^{p-1} \equiv 1 \pmod p$.

Let $\lambda_k$ be equal to 0 or 1 depending on whether $r_k < p/2$ or $r_k > p/2$. By the definition of number $\varrho_k$ we have

$$\varrho_k \equiv (-1)^{\lambda_k} r_k \pmod{p}. \tag{9}$$

But, according to the definition of $r_k$, $r_k \equiv kD \pmod{p}$. Hence, in virtue of (9), we obtain

$$\varrho_1 \varrho_2 \cdots \varrho_{\frac{p-1}{2}} \equiv (-1)^{\lambda_1+\lambda_2+\ldots+\lambda_{\frac{p-1}{2}}} \left(\frac{p-1}{2}\right)! D^{\frac{p-1}{2}} \pmod{p}. \tag{10}$$

Formulae (8) and (9) together with the fact that the number $\left(\frac{p-1}{2}\right)! D^{(p-1)/2}$ is not divisible by $p$ give

$$D^{\frac{p-1}{2}} \equiv (-1)^{\lambda_1+\lambda_2+\ldots+\lambda_{\frac{p-1}{2}}} \pmod{p}. \tag{11}$$

But, according to the definition of $\lambda_k$, number $\lambda = \lambda_1+\lambda_2+\ldots+\lambda_{(p-1)/2}$ is exactly the number of the remainders obtained by dividing the numbers of (6) by $p$, successively. The number of the remainders is $> p/2$. On the other hand, the left-hand side of (11) is congruent to $\left(\frac{D}{p}\right) \pmod{p}$. Consequently, (11) turns into the congruence $\left(\frac{D}{p}\right) \equiv (-1)^{\lambda} \pmod{p}$. To see that this in fact implies the equality $\left(\frac{D}{p}\right) = (-1)^{\lambda}$, asserted by the lemma, it is sufficient to note that $\left(\frac{D}{p}\right)$ is equal either to 1 or to $-1$ and that $p$, being an odd prime, is $\geqslant 3$. The lemma is thus proved.

Numbers $\lambda_k$, defined in the course of the proof of the lemma of Gauss, are such that $(-1)^{\lambda_k} = (-1)^{[2kD/p]}$. In fact, if $r_k < p/2$, then $\lambda_k = 0$, and, on the other hand, the definition of $r_k$ shows that for an integer $t_k$ the equality $kD = pt_k + r_k$ is valid, whence $2kD/p = 2t_k + 2r_k/p$ and, since $0 < 2r_k < p$, $[2kD/p] = 2t_k$, we have $(-1)^{\lambda_k} = (-1)^{[2kD/p]}$. If $r_k > p/2$, then $1 < 2r_k/p < 2$ (because $r_k < p$), whence $[2r_k/p] = 1$ and $[2kD/p] = 2t_k + 1$. But, since for $r_k > p/2$ we have $\lambda_k = 1$, the formula $(-1)^{\lambda_k} = (-1)^{[2kD/p]}$ follows.

Since the formula proved above holds for any $k = 1, 2, \ldots, (p-1)/2$, we have

$$(-1)^{\lambda} = (-1)^{\lambda_1+\lambda_2+\ldots+\lambda_{(p-1)/2}} = (-1)^{\sum_{k=1}^{(p-1)/2} [2kD/p]}.$$

Thus the lemma of Gauss implies



COROLLARY. *We have*

$$\left(\frac{D}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} [2kD/p]}.$$

Consider the particular case of $D = 2$. By the corollary,

$$\left(\frac{2}{p}\right) = (-1)^{\lambda} \quad \text{holds for} \quad \lambda = \sum_{k=1}^{(p-1)/2} [4k/p]. \tag{12}$$

If $1 \leqslant k < p/4$, then $0 < 4k/p < 1$ and so $[4k/p] = 0$. The equality $k = p/4$ is impossible because $p$ is odd. For $[p/4] < k \leqslant (p-1)/2$ we have $1 < 4k/p \leqslant 2(p-1)/p < 2$; consequently, $[4k/p] = 1$. From this we infer that among the summands of the sum for $\lambda$ in (12) there are $(p-1)/2 - [p/4]$ summands equal to 1, the remaining ones being equal to zero. Consequently $\lambda = (p-1)/2 - [p/4]$. But, as is easy to verify, for odd $p$ we have

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] \equiv \frac{p^2-1}{8} \pmod{2}.$$

In fact, number $p$, being odd, is equal to one of the following four numbers: $8k+1$, $8k+3$, $8k+5$, $8k+7$, where $k$ is a natural number.

Write

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

Then, a simple calculation shows that

$$\begin{aligned} f(8k+1) &= 4k - 2k = 2k, & g(8k+1) &= k(8k+2), \\ f(8k+3) &= 4k+1-2k = 2k+1, & g(8k+3) &= (4k+1)(2k+1), \\ f(8k+5) &= 4k+2-(2k+1) = 2k+1, & g(8k+5) &= (2k+1)(4k+3), \\ f(8k+7) &= 4k+3-(2k+1) = 2k+2, & g(8k+7) &= (4k+3)(2k+2), \end{aligned}$$

whence, in any case, $f(p) \equiv g(p) \pmod{2}$. Consequently, $\lambda \equiv \frac{p^2-1}{8} \pmod{2}$, and thus, by (12), we obtain property IV of Legendre's symbol:

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

From this we infer that 2 is a quadratic residue to all primes $p$ of the form $8k \pm 1$ and is not a quadratic residue to any prime $p$ of the form $8k \pm 3$ (where $k$ is an integer). Now we apply property IV in the proof of the following theorem:

THEOREM 1. *There exist infinitely many primes of the form* $8k-1$, *where* $k = 1, 2, \ldots$

Proof. Let $n$ be a natural number $>1$. Number $N = 2(n!)^2-1$ is greater than 1 and has at least one odd prime divisor $p$ which is not of the form $8k+1$. The reason is that if all the odd prime divisors of number $N$ were of the form $8k+1$, then number $N$ itself would be of this form, which is clearly impossible since $N$ is of the form $8k-1$. We have $p \mid N$, i.e. $2(n!)^2 \equiv 1^2 (\mathrm{mod}\, p)$, which proves that $2(n!)^2$ is a quadratic residue to the modulus $p$. Therefore $\left(\frac{2(n!)^2}{p}\right) = 1$, which, in view of property II, gives $\left(\frac{2(n!)^2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{n!}{p}\right)^2 = \left(\frac{2}{p}\right)$. Consequently, $\left(\frac{2}{p}\right) = 1$ and, in view of property IV, $p$ must be of the form $8k \pm 1$. But the definition of $p$ shows that $p$ is not of the form $8k+1$, and so it must be of the form $8k-1$. But, since $p \mid N = 2(n!)^2-1$, we see that $p > n$. We have thus proved that for any natural number $n > 1$ there exists a prime $p$ greater than $n$ that is of the form $8k-1$. The proof is thus completed.

THEOREM 2. *There exist infinitely many primes of the form* $8k+3$, *where* $k = 0, 1, 2, \ldots$

Proof. Let $n$ be a natural number $>1$, and let $a = p_2 p_3 \ldots p_n$. Since $a$ is odd, its square $a^2$ is of the form $8t+1$, number $N = a^2+2$ being of the form $8t+3$. If any prime divisor of $N$ is of the form $8t \pm 1$, then number $N$ itself is of this form, which is impossible. Therefore the odd number $N$ has a (necessarily odd) prime divisor $p$ which is not of the form $8k \pm 1$; consequently $p$ is either of the form $8k+3$ or of the form $8k+5$. Suppose $p = 8k+5$. Since $p \mid N = a^2+2$, we have $a^2 \equiv -2 (\mathrm{mod}\, p)$ and so $\left(\frac{-2}{p}\right) = 1$. But, in virtue of properties II, III, IV,

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

Since $p = 8k+5$, number $\frac{1}{2}(p-1)$ is even and number $\frac{1}{8}(p^2-1)$ is odd, whence $\left(\frac{-2}{p}\right) = -1$, which is a contradiction. Therefore $p$ cannot be of the form $8k+5$, and so it is of the form $8k+3$. But, since $p \mid a^2+2$, $a = p_2 p_3 \ldots p_n$, we have $p > p_n$. Hence, since $n$ may be chosen arbitrarily large, theorem 2 is proved.

THEOREM 3. *There exist infinitely many primes of the form* $8k+5$, *where* $k = 0, 1, 2, \ldots$

Proof. Let $n$ be a natural number $>1$ and let $a = p_2 p_3 \ldots p_n$. Since $a$ is an odd number, number $N = a^2+4$ is of the form $8k+5$. If any of its prime divisors is of the form $8t \pm 1$, then number $N$ itself is of this form, but this is impossible. Consequently, $N$ must have an odd prime divisor $p$ which is either of the form $8k+3$ or of the form $8k+5$. The former case being impossible because, if $p = 8k+3$, the relation $p \mid N = a^2+4$ shows that $a^2 \equiv -4 (\mathrm{mod}\, p)$, and so $\left(\frac{-4}{p}\right) = 1$; hence, by properties II and III,

$$\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2 = (-1)^{(p-1)/2}$$

whence, in view of $p = 8k+3$, we have $\left(\frac{-4}{p}\right) = -1$, which is a contradiction. Consequently, $p$ is of the form $8k+5$. But, since $p \mid a^2+4$ and $a = p_2 p_3 \ldots p_n$, we have $p > p_n$, which, in view of the fact that $n$ is arbitrarily chosen, completes the proof of theorem 3.



**§ 2. The quadratic reciprocity law.** Let $p$ and $q$ be two different odd primes. Consider the pairs $(kq, lp)$, where $k = 1, 2, \ldots, (p-1)/2$, $l = 1, 2, \ldots, (q-1)/2$. The number of such pairs is clearly $\frac{p-1}{2} \cdot \frac{q-1}{2}$. For any of the pairs we have $kq \neq lp$ because, in the opposite case, i.e. if $kq = lp$, we have $p \mid kq$, whence, by $(p, q) = 1$, $p \mid k$, which is impossible because $k \leqslant (p-1)/2$. We divide all the pairs into two classes, one consisting of all the pairs for which $kq < lp$, the other comprising the pairs for which $kq > lp$. We calculate the number of pairs in each class as follows.

Given a number $l$ out of the sequence $1, 2, \ldots, (q-1)/2$. If the pair $(kq, lp)$ belongs to the first class, then $k < lp/q$. Since, as we know, $lp/q$ is not an integer and since

$$\frac{lp}{q} \leqslant \frac{(q-1)p}{2q} \leqslant \frac{p}{2}, \quad \text{whence} \quad \left[\frac{lp}{q}\right] < \frac{p}{2},$$

we have

$$2\left[\frac{lp}{q}\right] < p, \quad \text{i.e.} \quad 2\left[\frac{lp}{q}\right] \leqslant p-1, \quad \text{whence} \quad \left[\frac{lp}{q}\right] \leqslant \frac{p-1}{2}.$$

Consequently, for a given number $l$, $l \leqslant \frac{1}{2}(q-1)$, $k$ may take the values $1, 2, \ldots, \left[\frac{lp}{q}\right]$, which are $\left[\frac{lp}{q}\right]$ in number. From this we infer that the number of pairs which belong to the first class is $\sum_{l=1}^{(q-1)/2} \left[\frac{lp}{q}\right]$. Similarly, the number of the pairs that belong to the second class is $\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right]$. Since

the number of all the pairs in both classes is $\frac{p-1}{2}\cdot\frac{q-1}{2}$, we obtain the equality

$$\frac{p-1}{2}\cdot\frac{q-1}{2}=\sum_{l=1}^{(q-1)/2}\left[\frac{lp}{q}\right]+\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]. \tag{13}$$

In virtue of the corollary to the lemma of Gauss, by properties I and II we have

$$\left(\frac{2q}{p}\right)=\left(\frac{2(p+q)}{p}\right)=\left(\frac{2^2\frac{q+p}{2}}{p}\right)=\left(\frac{(q+p)/2}{p}\right)$$

$$=(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{k(p+q)}{p}\right]}=(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]+\sum_{k=1}^{(p-1)/2}k}=(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]+\frac{p^2-1}{8}}$$

(the last equality being valid since $\sum_{k=1}^{(p-1)/2}k=\frac{1}{8}(p^2-1)$). But (since $q$ is odd), in virtue of II and IV we have

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

which, combined with the formula proved above for $\left(\frac{2q}{p}\right)$, implies the equality

$$\left(\frac{q}{p}\right)=(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]}$$

valid for any odd $p$ and $q$. Hence

$$\left(\frac{p}{q}\right)=(-1)^{\sum_{l=1}^{(q-1)/2}\frac{lp}{q}}.$$

By (13), these two formulae show that the formula

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

is valid for any two different odd primes $p$ and $q$. This formula is known under the name of the *quadratic reciprocity law.*

Number $\frac{p-1}{2}\cdot\frac{q-1}{2}$ is odd if and only if each of the numbers $p$ and $q$ is of the form $4k+3$; hence equality V may be expressed by saying

*If two different odd primes $p$ and $q$ are of the form $4k+3$, then $\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$; if at least one of them is of the form $4k+1$, then $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$.*



There are as many as seven different proofs of the law of quadratic reciprocity given only by Gauss himself. A table of 45 proofs of this law, ordered according to the time of their discovery (from 1796 to 1897), is given by P. Bachmann [2], p. 203. The number of proofs has considerably increased since then.

Now we are going to apply property V to the proof of

THEOREM 4. *There are infinitely many primes of the form $5k-1$, where $k$ is a natural number.*

Proof. Let $n$ be an arbitrary natural number $>1$. Let $N=5(n!)^2-1$. Clearly, $N$ is an odd number $>1$ and, since it is not of the form $5t+1$, it has at least one prime divisor $p$ which is odd (different from 5) and not of the form $5t+1$. We have $p>n$. Since $p\mid N$, we have $5(n!)^2\equiv 1 \pmod p$, whence $\left(\frac{5}{p}\right)=1$. By V, we thus have $\left(\frac{p}{5}\right)=1$. The prime $p$, different from 5, must be of the form $5k\pm1$ or $5k\pm2$. If $p=5k\pm2$, then, by I and II, $\left(\frac{p}{5}\right)=\left(\frac{\pm2}{5}\right)=\left(\frac{\pm1}{5}\right)\left(\frac{2}{p}\right)$. But since, by III, $\left(\frac{\pm1}{5}\right)=1$ and, by IV, $\left(\frac{2}{p}\right)=-1$, we obtain $\left(\frac{p}{5}\right)=-1$, which is a contradiction. Therefore number $p$ must be of the form $5k\pm1$, and so, since it is proved not to be of the form $5k+1$, it is of the form $5k-1$. Thus we have shown that for any natural number $n$ there exists a prime $p>n$ that is of the form $5k-1$. This completes the proof of the theorem.

If $p=5k-1$ ($k$ being a natural number) is a prime, then $k$ must be even (since otherwise $p$ would be an even number $>2$, and thus composite). Therefore $k=2t$, where $t$ is a natural number and $p=10t-1$. From theorem 4 we infer that *there exist infinitely many primes of the form $10t-1$, where $t$ is a natural number.* In other words, there exist infinitely many primes whose last digits are 9.

It is easy to verify that there exist infinitely many primes of the form $5k\pm2$, where $k$ is a natural number. In fact, let $n$ be an arbitrary natural number $>2$. We put $N=p_2p_3\ldots p_n-2$. Then $N$ is an odd number $>1$ whose prime divisors are different from 5. If all its prime divisors were of the form $5k\pm1$, number $N$ itself would be of this form. Consequently, there exists at least one prime divisor $p$ of $N$ which is different from 5 and not of the form $5k\pm1$. So $p$ must be of the form $5k\pm2$. But, since $p>p_n$, the theorem follows. The theorem on arithmetical progressions implies that there are infinitely many primes of the forms $5k+2$ and $5k-2$. The proof, however, is far more difficult. Since $k$ must be an odd number, one easily sees that the former of the two theorems is equivalent to the theorem stating that there exist infinitely many primes whose last digits are 7; the latter theorem is equivalent to the theorem stating that there exist infinitely many primes whose last digits are 3.

THEOREM 5. *Every prime $p$ which is of the form $6k+1$ is of the form $p=3x^2+y^2$, where $x, y$ are natural numbers.*

Proof. Suppose that $p$ is a prime of the form $6k+1$. By property V of Legendre's symbol, $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)$. By property I, $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. Combining these two equalities, we obtain

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

which proves that $-3$ is a quadratic residue to the modulus $p$. Therefore there exists an integer $a$ such that $a^2+3 \equiv 0 \pmod{p}$. In view of Thue's theorem (see Chapter I, § 13), there exist natural numbers $x, y$, each $\leqslant \sqrt{p}$, such that for a suitable choice of the sign the number $ax \pm y$ is divisible by $p$. Hence it follows that $p \mid a^2x^2-y^2$. But, since $p \mid a^2+3$, whence $p \mid a^2x^2+3x^2$, we have $p \mid 3x^2+y^2$. But $x \leqslant \sqrt{p}$ and $y \leqslant \sqrt{p}$. Consequently, in view of the fact that $p$ is a prime, we have $x^2 < p$ and $y^2 < p$, whence $3x^2+y^2 < 4p$. In virtue of the relation $p \mid 3x^2+y^2$, we then have $3x^2+y^2 = pt$, where $t$ is a natural number $< 4$. If $t = 3$, then $3 \mid y$ and so $y = 3z$, where $z$ is a natural number, whence $p = x^2+3z^2$. If $t = 2$, then the numbers $x, y$ must both be even or both be odd. In either case number $2p = 3x^2+y^2$ is divisible by 4, whence $2 \mid p$, which is impossible. In the case where $t = 1$, we have $p = 3x^2+y^2$. Theorem 5 is thus proved.

It is easy to prove that if a prime $p$ is of the form $p = 3x^2+y^2$, where $x, y$ are natural numbers, then $p$ must be of the form $p = 6k+1$, where $k$ is a natural number. From theorem 10 of Chapter V it follows that any prime of the form $6k+1$ has exactly one representation in the form $3x^2+y^2$, where $x$ and $y$ are natural numbers. B. van der Pol and P. Speziali [1] have tabulated the representations in the form $3x^2+y^2$ of primes of the form $6k+1$ which are less than 10000. In particular, we have $7 = 3\cdot1^2+2^2$, $13 = 3\cdot2^2+1^2$, $19 = 3\cdot1^2+4^2$, $31 = 3\cdot3^2+2^2$, $37 = 3\cdot2^2+5^2$, $43 = 3\cdot3^2+4^2$, $61 = 3\cdot2^2+7^2$, $67 = 3\cdot1^2+8^2$, $73 = 3\cdot4^2+5^2$, $79 = 3\cdot5^2+2^2$, $97 = 3\cdot4^2+7^2$.

As has been noticed by A. Mąkowski, theorem 5 implies the following corollary: *for any prime $p$ of the form $6k+1$ number $2p^4$ is the sum of three biquadrates.*

This is obtained immediately from theorem 5 by a simple application of the identity

$$2(3x^2+y^2)^4 = (3x^2+2xy-y^2)^4+(3x^2-2xy-y^2)^4+(4xy)^4$$

and by the remark that for $p = 3x^2+y^2$ we have the equality $3x^2 \pm 2xy-y^2 = p-2y^2 \pm 2xy$ the right-hand side of which is different from zero since $p = 6k+1$ is odd.



We note that also the following identity holds:

$$2(3x^2+y^2)^2 = (3x^2+2xy-y^2)^2+(3x^2-2xy-y^2)^2+(4xy)^2.$$

Hence, in particular, for $x = 1$, $y = 2$ we obtain

$$2\cdot7^4 = 3^4+5^4+8^4, \quad 2\cdot7^2 = 3^2+5^2+8^2,$$

and, for $x = 2$, $y = 1$, we find

$$2\cdot13^4 = 15^4+7^4+8^4, \quad 2\cdot13^2 = 15^2+7^2+8^2.$$

In this connection, we present the following two identities:

$$2(3x^2+y^2)^2 = (x+y)^4+(x-y)^4+(2x)^4,$$

$$2(3x^2+y^2) = (x+y)^2+(x-y)^2+(2x)^2.$$

From them we derive the following corollary: *for any prime $p$ of the form $6k+1$ number $2p^2$ is a sum of three biquadrates of natural numbers.*

For example, for $x = 1$, $y = 2$, we have

$$2\cdot7^2 = 3^4+1^4+2^4, \quad 2\cdot7 = 3^2+1^2+2^2;$$

for $x = 2$, $y = 1$ we have

$$2\cdot13^2 = 3^4+1^4+4^4, \quad 2\cdot13 = 3^2+1^2+4^2.$$

**§ 3. Calculation of Legendre's symbol by its properties.** The five properties of Legendre's symbol deduced from its definition combined with the fact that the value of the symbol is either 1 or $-1$ enable us to calculate its value.

Let $p$ be a given odd prime and $D$ an integer not divisible by $p$. Let $r$ be the remainder left by $D$ divided by $p$. Consequently, we have $0 < r < p$, and, by property I, $\left(\frac{D}{p}\right) = \left(\frac{r}{p}\right)$. Let $a^2$ denote the greatest square that divides $r$. We have $r = ka^2$, where either $k = 1$ or $k$ is the product of different primes, i.e. $k = q_1q_2\ldots q_s$, with $q_1 < q_2 \ldots < q_s$; moreover, since $r < p$, we have $q_s < p$. In virtue of property II we have

$$\left(\frac{D}{p}\right) = \left(\frac{ka^2}{p}\right) = \left(\frac{k}{p}\right)\left(\frac{a^2}{p}\right) = \left(\frac{k}{p}\right)\left(\frac{a}{p}\right)^2 = \left(\frac{k}{p}\right),$$

this being equal to $\left(\frac{1}{p}\right) = 1$ or to $\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\ldots\left(\frac{q_s}{p}\right)$. If $q_1 = 2$, then $\left(\frac{q_1}{p}\right)$ is calculated by the use of property IV. If $q_1 > 2$, then the values of the

symbols $\left(\frac{q}{p}\right)$, where $q$ and $p$ are odd primes and $q < p$, are still to be calculated. By property V, we have

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

Thus the calculation of Legendre's symbol $\left(\frac{D}{p}\right)$ reduces to the calculation of the symbols $\left(\frac{D'}{q}\right)$, where $q$ is an odd prime less than $p$.

Therefore, after a finite number of reductions, we obtain the value of the symbol $\left(\frac{D}{p}\right)$. This procedure has the disadvantage that it involves expansions into prime factors. In order to avoid that, Jacobi introduced a more general symbol; it will be investigated in the next section.

**§ 4. Jacobi's symbol and its properties.** Jacobi defined the symbol $\left(\frac{D}{P}\right)$ for odd numbers $P > 1$ and integers $D$ relatively prime to $P$ as follows:

If $P = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$ is the factorization of $P$ into prime factors (each factor being odd), then

$$\left(\frac{D}{P}\right) = \left(\frac{D}{q_1}\right)^{\alpha_1}\left(\frac{D}{q_2}\right)^{\alpha_2}\dots\left(\frac{D}{q_s}\right)^{\alpha_s}, \tag{14}$$

where on the right-hand side we have Legendre's symbols.

It follows immediately from the definition that if $P$ is a prime, then Jacobi's symbol is equal to Legendre's symbol. However, for investigating the quadratic residuacity Jacobi's symbol does not correspond exactly to Legendre's symbol. The reason is that though the equality $\left(\frac{D}{P}\right) = -1$ implies that $D$ is not a quadratic residue to $P$ because then at least one of the factors $\left(\frac{D}{q_i}\right)$, one on the right-hand side of (14), must be equal to $-1$, whence the congruence $x^2 \equiv D \pmod{q_i}$ is insolvable, and so, *a fortiori* (since $q_i \mid D$) the congruence $x^2 \equiv D$ is insovable, the relation $\left(\frac{D}{P}\right) = +1$ does not necessarily imply that $D$ is a quadratic residue to $P$, for example $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$ and the congruence $x^2 \equiv 2 \pmod{15}$ is insolvable because the congruence $x^2 \equiv 2 \pmod 3$ is insolvable.



Jacobi's symbol possesses five properties similar to those of Legendre's symbol. In order to prove them we note that (14) may be rewritten in the form

$$\left(\frac{D}{P}\right) = \left(\frac{D}{q_1}\right)\left(\frac{D}{q_2}\right)\dots\left(\frac{D}{q_s}\right), \tag{15}$$

where $P = q_1 q_2 \dots q_s$ and the primes $q_1, q_2, \dots, q_s$ are not necessarily different.

PROPERTY I. *If* $D \equiv D' \pmod P$, *then* $\left(\frac{D}{P}\right) = \left(\frac{D'}{P}\right)$.

Proof. In virtue of (15) we have

$$\left(\frac{D}{P}\right) = \left(\frac{D}{q_1}\right)\left(\frac{D}{q_2}\right)\dots\left(\frac{D}{q_s}\right); \quad \left(\frac{D'}{P}\right) = \left(\frac{D'}{q_1}\right)\dots\left(\frac{D'}{q_s}\right). \tag{16}$$

If $D \equiv D' \pmod P$, then, *a fortiori*, $D \equiv D' \pmod{q_i}$ for any $i = 1, 2, \dots, s$. Consequently, by property I of Legendre's symbol, $\left(\frac{D}{q_i}\right) = \left(\frac{D'}{q_i}\right)$ for $i = 1, 2, \dots, s$, whence, by (16), $\left(\frac{D}{P}\right) = \left(\frac{D'}{P}\right)$.

PROPERTY II. $\left(\frac{DD'}{P}\right) = \left(\frac{D}{P}\right)\left(\frac{D'}{P}\right)$ *for any integers* $D$ *and* $D'$ *not divisible by* $P$.

The proof follows easily from property II of Legendre's symbol, formula (16) and the fact that

$$\left(\frac{DD'}{P}\right) = \left(\frac{DD'}{q_1}\right)\left(\frac{DD'}{q_2}\right)\dots\left(\frac{DD'}{q_s}\right).$$

As an immediate consequence of property II we obtain $\left(\frac{1}{P}\right) = 1$.

PROPERTY III. $\left(\frac{-1}{P}\right) = (-1)^{(P-1)/2}$.

Proof. In view of (15), by property III of Legendre's symbol, we have

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{q_1}\right)\left(\frac{-1}{q_2}\right)\dots\left(\frac{-1}{q_s}\right) = (-1)^{\frac{q_1-1}{2}+\frac{q_2-1}{2}+\dots+\frac{q_s-1}{2}}. \tag{17}$$

Consider the identity

$$P = q_1 q_2 \dots q_s = \big((q_1-1)+1\big)\big((q_2-1)+1\big)\dots\big((q_s-1)+1\big).$$

All the numbers $q_1-1, q_2-1, \ldots, q_s-1$ are even; consequently the product of any two of them is divisible by 4. Hence

$$P = 4k+1+(q_1-1)+(q_2-1)+\ldots+(q_s-1),$$

and so

$$\frac{P-1}{2} = 2k+\frac{q_1-1}{2}+\frac{q_2-1}{2}+\ldots+\frac{q_s-1}{2}.$$

Therefore

$$(-1)^{\frac{P-1}{2}} = (-1)^{\frac{q_1-1}{2}+\frac{q_2-1}{2}+\ldots+\frac{q_s-1}{2}}.$$

Hence, by (17), property III follows.

PROPERTY IV. $\left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8}$.

Proof. In virtue of (15), by property IV of Legendre's symbol, we have

$$\left(\frac{2}{P}\right) = \left(\frac{2}{q_1}\right)\left(\frac{2}{q_2}\right)\ldots\left(\frac{2}{q_s}\right) = (-1)^{\frac{q_1^2-1}{8}+\frac{q_2^2-1}{8}+\ldots+\frac{q_s^2-1}{8}}. \tag{18}$$

Since the square of any odd natural number is of the form $8k+1$, the identity

$$P^2 = \left((q_1^2-1)+1\right)\left((q_2^2-1)+1\right)\ldots\left((q_s^2-1)+1\right)$$

shows that any of the differences $q_1^2-1, q_2^2-1, \ldots, q_s^2-1$ is divisible by 8. Consequently, the product of any two of them is divisible by 64. Hence

$$P^2 = 64k+1+(q_1^2-1)+(q_2^2-1)+\ldots+(q_s^2-1),$$

and so

$$\frac{P^2-1}{8} = 8k+\frac{q_1^2-1}{8}+\frac{q_2^2-1}{8}+\ldots+\frac{q_s^2-1}{8},$$

whence

$$(-1)^{\frac{P^2-1}{8}} = (-1)^{\frac{q_1^2-1}{8}+\frac{q_2^2-1}{8}+\ldots+\frac{q_s^2-1}{8}},$$

which, by (18), completes the proof of property IV.

PROPERTY V. $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$ *for any relatively prime odd numbers* $P, Q > 1$.

Proof. Let $Q = r_1 r_2 \ldots r_t$, where $r_1, r_2, \ldots, r_t$ are not necessarily different odd primes.



In virtue of (15), property II, and property V of Legendre's symbol, we have

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i=1}^{s}\prod_{j=1}^{t}\left(\frac{q_i}{r_j}\right)\left(\frac{r_j}{q_i}\right) = (-1)^{\sum_{i=1}^{s}\sum_{j=1}^{t}\frac{q_i-1}{2}\cdot\frac{r_j-1}{2}}. \tag{19}$$

But

$$\sum_{i=1}^{s}\sum_{j=1}^{t}\frac{q_i-1}{2}\cdot\frac{r_j-1}{2} = \sum_{i=1}^{s}\frac{q_i-1}{2}\cdot\sum_{j=1}^{t}\frac{r_j-1}{2}. \tag{20}$$

As is easily noticed, in the proof of property III

$$\sum_{i=1}^{s}\frac{q_i-1}{2} = \frac{P-1}{2}-2k \quad \text{and similarly} \quad \sum_{j=1}^{t}\frac{r_j-1}{2} = \frac{Q-1}{2}-2l,$$

whence, $P$ and $Q$ being odd, we have

$$\sum_{i=1}^{s}\frac{q_i-1}{2}\cdot\sum_{j=1}^{t}\frac{r_j-1}{2} = \frac{P-1}{2}\cdot\frac{Q-1}{2}+2h.$$

This by (19) and (20) completes the proof of property V.

**§ 5. Eisenstein's rule.** The properties of Jacobi's symbol introduced in the preceding section will serve to obtain the Eisenstein rule, by means of which the value of Jacobi's symbol (and thus also of Legendre's symbol) may be calculated without using the factorization of a number into primes.

First of all we note that the task of calculating the value of $\left(\frac{D}{P}\right)$, where $P$ is an odd number $>1$ and $D$ an integer relatively prime to $P$, may be reduced to that of calculating the value of $\left(\frac{Q}{P}\right)$, where $Q$ is an odd natural number. In fact, if $2^\beta$ (where $\beta$ is an integer $\geqslant 0$) is the greatest power of 2 that divides $D$, then $D = (-1)^\alpha 2^\beta Q$, where $\alpha = 0$ or 1, $Q$ being a natural odd number. Clearly, in order to find the number $Q$ we do not need to know the factorization of $D$ into primes; it is sufficient to divide $D$ by consecutive powers of 2.

By the properties of Jacobi's symbol, in virtue of the formula for $D$, we obtain

$$\left(\frac{D}{P}\right) = (-1)^{\frac{P-1}{2}\alpha+\frac{P^2-1}{8}\beta}\left(\frac{Q}{P}\right).$$

Thus it remains to find the value of $\left(\frac{Q}{P}\right)$, where $Q, P$ are odd relatively prime natural numbers.

Let $R$ be the remainder left by $Q$ divided by $P$. Consequently, $R$ is one of the numbers of the sequence $1, 2, \ldots, P-1$. Number $P-R$ also belongs to this sequence. Hence, for an integer $t$ we have

$$Q = Pt+R \quad \text{and} \quad Q = P(t+1)-(P-R).$$

Since the sum of the numbers $R$ and $P-R$ is odd, one of them must be odd, the other being even. Let $P_1$ denote the odd number. If $P_1 = R$, then $Q = Pt+P_1$; if $P_1 = P-R$, then $Q = P(t+1)-P_1$. In any case $Q = Pk+\varepsilon_1 P_1$, where $k$ is an integer and $\varepsilon_1$ is 1 or $-1$. We note that $k$ must be an even number, since otherwise the number $Q \pm P_1$ would be odd, which is clearly impossible because the numbers $Q$ and $P_1$ are odd. Consequently, $k = 2k_1$, where $k_1$ is an integer. We have $Q = 2k_1 P+\varepsilon_1 P_1$.

If $P_1 \neq 1$, then we may repeat the above reasoning with $P$ and $P_1$ in place of $Q$ and $P$. Then we obtain the equality $P = 2k_2 P_1+\varepsilon_2 P_2$, where $k_2$ is an integer and $\varepsilon_2 = \pm 1$, $P_2$ is an odd natural number.

If $P_2 \neq 0$, then, as in the previous case, $P_1 = 2k_3 P_2+\varepsilon_3 P_3$ and so on. Numbers $P, P_1, P_2, \ldots$ are strictly decreasing because $P_1 \leqslant P-1$, $P_2 \leqslant P_1-1, \ldots$ Therefore the sequence of the equalities that link together numbers $P, P_1, P_2, \ldots$ cannot be infinite because the number of odd natural numbers $< P$ is finite. Therefore we ultimately obtain the last equality, $P_{n-2} = 2k_n P_{n-1}+\varepsilon_n P_n$, where $P_n$ must be equal to 1, since otherwise a next equality could be obtained. Thus we obtain the sequence of equalities:

$$\begin{aligned} &Q = 2k_1 P+\varepsilon_1 P_1, \quad P = 2k_2 P_1+\varepsilon_2 P_2, \quad P_1 = 2k_3 P_2+\varepsilon_3 P_3, \quad \ldots, \\ &P_{n-3} = 2k_{n-1} P_{n-2}+\varepsilon_{n-1} P_{n-1}, \quad P_{n-2} = 2k_n P_{n-1}+\varepsilon_n P_n, \end{aligned} \tag{21}$$

where $P_n = 1$. The first equality of (21), by properties I and II of Jacobi's symbol, gives

$$\left(\frac{Q}{P}\right) = \left(\frac{\varepsilon_1}{P}\right)\left(\frac{P_1}{P}\right). \tag{22}$$

If $\varepsilon_1 = 1$, then

$$\left(\frac{\varepsilon_1}{P}\right) = 1 = (-1)^{\frac{P-1}{2}\cdot\frac{1-1}{2}} = (-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}};$$

if $\varepsilon_1 = -1$, then

$$\left(\frac{\varepsilon_1}{P}\right) = (-1)^{\frac{P-1}{2}} = (-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}}.$$



In any case we then have

$$\left(\frac{\varepsilon_1}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}}.$$

In virtue of property V of Jacobi's symbol and by the fact that the square of Jacobi's symbol is always equal to 1, we have

$$\left(\frac{P_1}{P}\right) = \left(\frac{P}{P_1}\right)\cdot(-1)^{\frac{P-1}{2}\cdot\frac{P_1-1}{2}},$$

whence, by (22),

$$\left(\frac{Q}{P}\right) = \left(\frac{P}{P_1}\right)\cdot(-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}+\frac{P-1}{1}\cdot\frac{P_1-1}{2}}.$$

But (since $\varepsilon_1^2 = 1$) we have

$$\begin{aligned} \frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}+\frac{P-1}{2}\cdot\frac{P_1-1}{2} &= \frac{P-1}{2}\cdot\frac{P_1-\varepsilon_1}{2} = \frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-\varepsilon_1^2}{2\varepsilon_1} \\ &= \frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-1}{2\varepsilon_1}. \end{aligned}$$

Moreover, trivially, $(-1)^{a/\varepsilon_1} = (-1)^a$ for $\varepsilon_1 = \pm 1$, and so

$$(-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}+\frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-1}{2}} = (-1)^{\frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-1}{2}};$$

consequently

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-1}{2}}\left(\frac{P}{P_1}\right).$$

Similarly, from the second equality of (20) we find

$$\left(\frac{P}{P_1}\right) = (-1)^{\frac{P_1-1}{2}\cdot\frac{\varepsilon_2 P_2-1}{2}}\left(\frac{P_1}{P_2}\right)$$

and so on. Finally, the last but one equality gives

$$\left(\frac{P_{n-3}}{P_{n-2}}\right) = (-1)^{\frac{P_{n-2}-1}{2}\cdot\frac{\varepsilon_{n-1}P_{n-1}-1}{2}}\left(\frac{P_{n-1}}{P_{n-1}}\right)$$

and from the last equality, taking into account that $P_n = 1$, we find

$$\left(\frac{P_{n-2}}{P_{n-1}}\right) = \left(\frac{\varepsilon_n}{P_{n-1}}\right).$$

But hence, for $\varepsilon_n = \pm 1$, we easily obtain

$$\left(\frac{\varepsilon_n}{P_{n-1}}\right) = (-1)^{\frac{P_{n-1}-1}{2}\cdot\frac{\varepsilon_n-1}{2}},$$

whence, in view of $P_n = 1$, we obtain

$$\left(\frac{P_{n-2}}{P_{n-1}}\right) = (-1)^{\frac{P_{n-1}-1}{2}\cdot\frac{\varepsilon_n P_{n-1}}{2}}.$$

Now if we put together the formulae obtained for $\left(\frac{Q}{P}\right)$, $\left(\frac{P}{P_1}\right)$, ..., $\left(\frac{P_{n-2}}{P_{n-1}}\right)$ we get the final formula

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-1}{2}+\frac{P_1-1}{2}\cdot\frac{\varepsilon_2 P_2-1}{2}+\ldots+\frac{P_{n-1}-1}{2}\cdot\frac{\varepsilon_n P_n-1}{2}}.$$

The value of the right-hand side of this equality depends on the number of odd summands in the exponent. The product $\frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-1}{2}$ is odd if and only if each of the numbers $P$ and $\varepsilon_1 P_1$ is of the form $4t+3$. Therefore we may write

$$\left(\frac{Q}{P}\right) = (-1)^m, \tag{23}$$

where number $m$ is equal to the number of those of the pairs $P_{i-1}$, $\varepsilon_1 P$ ($i = 1, 2, \ldots, n$, and $P_0 = P$) in which both $P_{i-1}$ and $\varepsilon_i P_i$ are of the form $4t+3$. This gives

EISENSTEIN'S RULE. *To calculate* $\left(\frac{Q}{P}\right)$ *we look at equalities* (21) *and find the number* $m$ *of the pairs* $P_{i-1}$ *and* $\varepsilon_i P_i$ *in which both* $P_{i-1}$ *and* $\varepsilon_i P_i$ *are of the form* $4t+3$. *Then we substitute* $m$ *in* (23).

As is easy to see, the rule makes it possible to calculate the value of Jacobi's symbol without developing a number into prime factors.

EXAMPLES. **1.** We apply Eisenstein's rule in order to find the value of $\left(\frac{641}{257}\right)$. Here equalities (21) are the following:

$$641 = 2\cdot 257+127, \quad 257 = 2\cdot 127+3, \quad 127 = 42\cdot 3+1.$$

Among the pairs 257, 127; 127, 3; 3, 1, only the second is such that each of its terms is of the form $4t+3$. Therefore $m = 1$, and, consequently, $\left(\frac{641}{257}\right) = -1$, which shows that number 641 is not a quadratic residue for the modulus 257.



**2.** We calculate the value of the symbol $\left(\frac{65537}{274177}\right)$. We have $65537 = 0\cdot 274177+65537$, $274177 = 4\cdot 65537+12029$, $65537 = 6\cdot 12029-6637$, $12029 = 2\cdot 6637-1245$, $6637 = 6\cdot 1245-833$, $1245 = 2\cdot 833-421$, $833 = 2\cdot 421-9$, $421 = 46\cdot 9+7$, $9 = 2\cdot 7-5$, $7 = 2\cdot 5-3$, $5 = 2\cdot 3-1$.

Among the pairs $P_{i-1}$, $\varepsilon_i P_i$ only in the pairs $7, -5$ and $3, -1$ both of the terms are of the form $4t+3$. Therefore $m = 2$, whence $\left(\frac{65537}{274177}\right) = 1$.

**3.** In order to calculate the value of $\left(\frac{-104}{997}\right)$ we find that $-104 = (-1)\cdot 2^3\cdot 13$. So $\left(\frac{-104}{997}\right) = \left(\frac{-1}{997}\right)\left(\frac{2}{997}\right)\left(\frac{13}{997}\right)$. Number 997 is of the form $4t+1$, so $\left(\frac{-1}{997}\right) = 1$. Number 997 is of the form $8t+5$, so $\left(\frac{2}{997}\right) = -1$. Therefore $\left(\frac{-104}{997}\right) = -\left(\frac{13}{997}\right)$. In order to calculate the value of $\left(\frac{13}{997}\right)$ we write equalities like (20), i.e.

$$13 = 0\cdot 997+13, \quad 997 = 76\cdot 13+9, \quad 13 = 2\cdot 9-5, \quad 9 = 2\cdot 5-1.$$

We see that there is no pair $P_{i-1}$, $\varepsilon_i P_i$ in which both terms are of the form $4t+3$. Consequently, $m = 0$, whence $\left(\frac{13}{997}\right) = 1$ and so $\left(\frac{-104}{997}\right) = -1$.