The G*-number* $\kappa = \mathrm{aJ} + \mathrm{bO}$ *is thus divisible by* π *only when* a + b *is divisible by* 3.

If κ is not divisible by π, then one of the three following formula pairs is valid:

$$a = 3h, \quad b = 3k + e; \qquad a = 3h + e, \quad b = 3k;$$

$$a = 3h + e, \quad b = 3k + e,$$

with $e^2 = 1$, and thus, if $hJ + kO$ is set equal to λ,

$$\kappa = 3\lambda + eO \quad \text{or} \quad \kappa = 3\lambda + eJ \quad \text{or} \quad \kappa = 3\lambda + e,$$

so that in every case κ has the form

$$\kappa = 3\lambda + \varepsilon,$$

where ε is a *G*-unit.

Let us now consider the cube of κ. It becomes

$$\kappa^3 = 9(3\lambda^3 + 3\lambda^2\varepsilon + \lambda\varepsilon^2) + \varepsilon^3,$$

and, because $\varepsilon^3 = \pm 1$, it has the form

$$\kappa^3 = 9\mu \pm 1.$$

If κ *is not divisible by* π *we then have the congruences* $\kappa \equiv \varepsilon \bmod 3$, $\kappa^3 \equiv \pm 1 \bmod 9$.

22 The Quadratic Reciprocity Law

(*The Euler-Legendre-Gauss theorem.*) *The reciprocal Legendre symbols of the odd prime numbers* p *and* q *are governed by the formula*

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

This law, the so-called quadratic reciprocity law, was formulated but not proved by Euler (*Opuscula analytica*, Petersburg, 1783). In 1785 Legendre discovered the same law (*Histoire de l'Académie des Sciences*) independently of Euler and proved it partially.

The first complete proof was presented by Karl Friedrich Gauss (1777–1855) in his famous *Disquisitiones arithmeticae* (published in 1801), a book that laid the foundations of contemporary number theory; this work, its five hundred quarto pages swarming with profound

ideas, was written when Gauss was 20 years old. "It is really astonishing," says Kronecker, "to think that a single man of such young years was able to bring to light such a wealth of results, and above all to present such a profound and well organized treatment of an entirely new discipline."

Later Gauss discovered seven other proofs of the reciprocity theorem. (The Gauss proofs may be found in vol. 14 of Ostwald's *Klassiker der exakten Wissenschaften.*)

The quadratic reciprocity law is one of the most important theorems of number theory. Gauss called it the "*Theorema fundamentale.*" The American mathematician Dickson says in his *Theory of Numbers:* "The quadratic reciprocity law is doubtless the most important tool in the theory of numbers and occupies the central position in its history."

The importance of this law led other mathematicians like Jacobi, Cauchy, Liouville, Kronecker, Schering, and Frobenius to investigate it after Gauss and offer proofs of it. In his *Niedere Zahlentheorie,* P. Bachmann cites no fewer than 52 proofs and reports on the most important.

Probably the simplest of all the proofs is the following *arithmetic-geometric* proof, which arises from the combination of the so-called lemma of Gauss (Gauss' *Werke,* vol. II, p. 51) and a geometric idea of Cayley (Arthur Cayley [1821–1895], *Collected Mathematical Papers,* vol. II).

Before taking up the proof itself we will give the derivation of Gauss' lemma.

Let p be an odd prime number and D an integer that is not divisible by p. If x represents one of the numbers $1, 2, 3, \ldots, \mathfrak{p} = (p-1)/2$, R_x the common residue of the division Dx/p, g_x the corresponding integral quotient, then

$$Dx = R_x + g_x p. \tag{1}$$

Accordingly as R_x is smaller or greater than $\frac{1}{2}p$, we set $R_x = \rho_x$ or $R_x = \rho_x + p$, where in the second case ρ_x represents the negative minimum residue of the division Dx/p, and we obtain

$$Dx = \rho_x + g_x p \quad \text{or} \quad (1b) \qquad Dx = \rho_x + p + g_x p. \tag{1a}$$

If n is then the number of negative minimum residues occurring in the $\mathfrak{p}$ divisions Dx/p (for $x = 1, 2, 3, \ldots, \mathfrak{p}$), we have n equations of the form $(1b)$ and $m = \mathfrak{p} - n$ equations of the form $(1a)$.

We convert these equations into congruences mod p and obtain the $\mathfrak{p}$ congruences

$$Dx \equiv \rho_x \bmod p. \tag{2}$$

Now the $\mathfrak{p}$ residues ρ_x agree, except with respect to sign and sequence, with the $\mathfrak{p}$ numbers 1 to $\mathfrak{p}$.

[If, for example, ρ_r were equal to ρ_s or $\rho_r = -\rho_s$ for two different values r and s of x, then $Dr \equiv \rho_r$ and $Ds \equiv \rho_s$ would yield by subtraction or addition, respectively, $D(r \mp s) \equiv 0 \bmod p$. This congruence is, however, impossible, because neither D nor $r \mp s$ is divisible by p.]

Multiplication of the $\mathfrak{p}$ congruences (2) results in

$$D^{\mathfrak{p}}\mathfrak{p}! \equiv (-1)^n \mathfrak{p}! \bmod p,$$

and from this we obtain

$$D^{\mathfrak{p}} \equiv (-1)^n \bmod p.$$

However, since, according to Euler's theorem (No. 19),

$$D^{\mathfrak{p}} \equiv \left(\frac{D}{p}\right) \bmod p,$$

we obtain

$$\left(\frac{D}{p}\right) \equiv (-1)^n \bmod p,$$

whence, since both sides of this congruence have the absolute value 1,

$$\left(\frac{D}{p}\right) = (-1)^n. \tag{3}$$

This formula, in which n represents the number of negative minimum residues resulting from the $\mathfrak{p}$ divisions Dx/p $(x = 1, 2, 3, \ldots, \mathfrak{p})$, *is Gauss' lemma.*

Now let D be some odd prime number q that differs from p. We convert the $\mathfrak{p}$ equations (1*a*) and (1*b*) into congruences to the modulus 2, leave out all the excess multiples of 2, e.g., $(q-1)x$, and obtain

$$x \equiv \rho_x + g_x \bmod 2 \quad \text{and} \quad x \equiv 1 + \rho_x + g_x \bmod 2.$$

Addition of these $\mathfrak{p}$ congruences yields

$$\sum x \equiv n + \sum \rho_x + \sum g_x \bmod 2.$$

However, since the absolute values of ρ_x are in agreement with the numbers 1 through $\mathfrak{p}$ and each summand can be replaced by its opposite value in a congruence mod 2, we will write $\sum x$ in the obtained congruence instead of $\sum \rho_x$ and $-n$ instead of n, thereby obtaining

$$\sum x + n \equiv \sum x + \sum g_x \bmod 2$$

or

$$n \equiv \sum g_x \bmod 2. \tag{4}$$

In accordance with (4) we can now write (3) as

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

Now g_x is the greatest integer contained in the quotient qx/p. If we designate this as $[qx/p]$, we obtain at last

$$\left(\frac{q}{p}\right) = (-1)^{\Sigma[qx/p]}, \tag{I}$$

where x passes through all the integers from 1 to $\mathfrak{p} = (p-1)/2$.

Accordingly,

$$\left(\frac{p}{q}\right) = (-1)^{\Sigma[py/q]} \tag{II}$$

where y passes through all the integers from 1 to $\mathfrak{q} = (q-1)/2$.

Multiplication of (I) and (II) gives us

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\Sigma[(q/p)x]+\Sigma[(p/q)y]}. \tag{III}$$

The exponent of the right-hand side is, however, easily found.

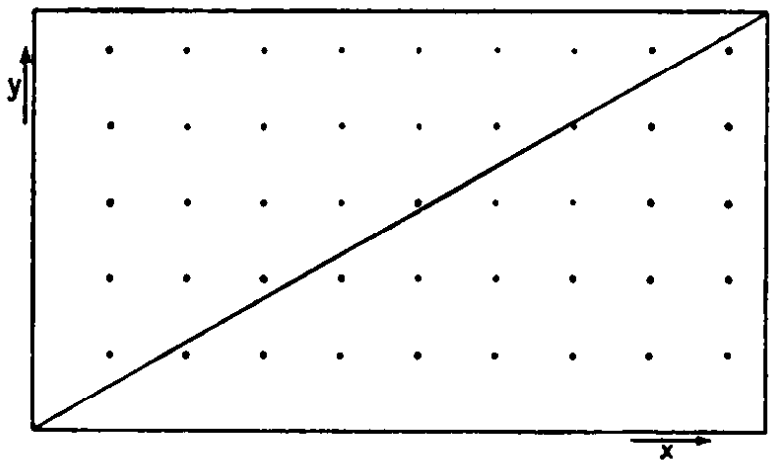

FIG. 4.

On a system of rectangular coordinates xy we draw the rectangle with the four angles

$$0|0, \quad \frac{p}{2}\Big|0, \quad \frac{p}{2}\Big|\frac{q}{2}, \quad 0\Big|\frac{q}{2}$$

and bisect it with a diagonal d from the origin, possessing the equation $y = (qx/p)$; we then mark off all the lattice points* within the rectangle. (Cf. the figure, in which $p = 19$, $q = 11$.)

To begin with, it is clear that no marked lattice point $x|y$ lies on d, since here x would necessarily be $< \frac{1}{2}p$ and $y < \frac{1}{2}q$, which contradicts the condition $y/x = q/p$.

For an integral abscissa x the corresponding ordinate of d is $y = (qx/p)$ and the number of marked lattice points lying on this ordinate is $[qx/p]$. Consequently, the number of the marked lattice points lying in the lower half of the rectangle is $\sum[qx/p]$, where x passes through all the integers from 1 to $\mathfrak{p}$.

Similarly, the number of all the marked lattice points lying in the upper half of our rectangle is $\sum[py/q]$, where y passes through all the integers from 1 to $\mathfrak{q}$.

The exponent appearing in (III) is then the number of all the marked lattice points in our rectangle. This is a total of $\mathfrak{p} \cdot \mathfrak{q}$ elements. Consequently,

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

or

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{[(p-1)/2]\cdot[(q-1)/2]}. \qquad \text{Q.E.D.}$$

23 Gauss' Fundamental Theorem of Algebra

Every equation of the n*th degree*

$$z^n + C_1 z^{n-1} + C_2 z^{n-2} + \cdots + C_n = 0$$

has n *roots.*

Expressed more precisely, this theorem reads:

The polynomial

$$f(z) = z^n + C_1 z^{n-1} + C_2 z^{n-2} + \cdots + C_n$$

can always be divided into n *linear factors of the form* $z - \alpha_\nu$.

* A lattice point is a point whose coordinates are integers.