

**GEOMETRISCHER BEWEIS DES FUNDAMENTALTHEOREMS  
FÜR DIE QUADRATISCHEN RESTE,**

GOTTHOLD EISENSTEIN

*Crelle's Journal für die Reine und Angewandte Mathematik* **28** (1844) 246-248  
Math. Werke I, 164-166;  
Engl. Transl.: *Quart. J. Math.* **1** (1857), 186-191, A. Cayley: *Coll. Math. Papers* III, 39-43

Skanningskopii artykułu z *Crelle's*, po edycji

## 20.

## Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste.

(Von Herrn Stud. *Gotth. Eisenstein* zu Berlin.)

**E**s sei  $p$  eine positive ungerade Primzahl,  $a$  der Complexus aller *geraden* Zahlen  $< p$  und  $> 0$ , also  $a = 2, 4, \dots, p-1$ ;  $q$  sei irgend eine durch den Modul  $p$  nicht theilbare ganze Zahl. Bezeichnet man durch  $r$  das allgemeine Glied der Reste der Vielfachen  $qa$  nach dem mod.  $p$ , so werden offenbar die Zahlen der Reihe, deren allgemeines Glied  $(-1)^r \cdot r$  ist, mit den Zahlen der Reihe  $a$  bis auf Vielfache von  $p$  übereinstimmen; also wird man die beiden Congruenzen haben:

$$q^{1(p-1)} \Pi a \equiv \Pi r \pmod{p}, \quad \text{und} \quad \Pi a \equiv (-1)^{\Sigma r} \Pi r \pmod{p},$$

woraus folgt

$$q^{1(p-1)} \equiv (-1)^{\Sigma r} \pmod{p}, \quad \text{also} \quad \left(\frac{q}{p}\right) = (-1)^{\Sigma r}.$$

Bedeutet  $E\left(\frac{qa}{p}\right)$  die größte in dem Bruche  $\frac{qa}{p}$  steckende ganze Zahl, so ist offenbar  $\Sigma qa = p \Sigma E\left(\frac{qa}{p}\right) + \Sigma r$ ; und da alle  $a$  gerade sind, und  $p \equiv 1 \pmod{2}$  ist, so folgt hieraus  $\Sigma r \equiv \Sigma E\left(\frac{qa}{p}\right) \pmod{2}$ ; also ist auch

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

Wenn  $q = 2$  ist, so giebt diese Formel sogleich den Werth von  $\left(\frac{2}{p}\right)$ : ist dagegen  $q$  ungerade, also  $q-1$  gerade, so findet man durch eine leichte Transformation

$$\begin{aligned} \Sigma E\left(\frac{qa}{p}\right) &\equiv -E\left(\frac{a}{p}\right) + E\left(\frac{2a}{p}\right) - E\left(\frac{3a}{p}\right) + \dots \pm E\left(\frac{\frac{1}{2}(q-1)a}{p}\right) \\ &\equiv E\left(\frac{a}{p}\right) + E\left(\frac{2a}{p}\right) + E\left(\frac{3a}{p}\right) + \dots + E\left(\frac{\frac{1}{2}(q-1)a}{p}\right) \pmod{2}. \end{aligned}$$

Wird letztere Summe durch  $u$  bezeichnet, so hat man auch  $\left(\frac{q}{p}\right) = (-1)^u$ .

Man stelle sich jetzt in der Ebene ein rechtwinkliges Coordinatensystem  $(x, y)$  und die ganze Ebene durch Parallelen mit den Axen in den Abständen  $= 1$  von einander in lauter Quadrate von den Dimensionen  $= 1$  getheilt vor.

**Gitterpunkte** sollen alle Eckpunkte von Quadraten heißen, welche nicht in den beiden Coordinaten-Axen liegen (Taf. II. Fig. 1. 2.).

Nimmt man auf irgend einer senkrechten Parallele einen Punct an, dem die Ordinate  $y$  entspricht, so wird  $E(y)$  die Anzahl der Gitterpunkte ausdrücken, welche zwischen diesem Puncte und der wagerechten Axe liegen; und nimmt man auf irgend einer wagerechten Parallele einen Punct an, dem die Abscisse  $x$  entspricht, so wird  $E(x)$  die Anzahl der Gitterpunkte ausdrücken, welche zwischen diesem Puncte und der senkrechten Axe liegen. Zeichnet man daher in der Ebene irgend eine Curve, deren Gleichung  $y = \varphi(x)$  ist (Fig. 1.), so wird die Summe

$$E\varphi(1) + E\varphi(2) + E\varphi(3) + E\varphi(4) + \text{etc.}$$

die Anzahl der Gitterpunkte geben, welche zwischen dieser Curve und der Axe der  $x$  liegen, diejenigen Gitterpunkte mitgerechnet, welche etwa zufällig auf der Curve selbst liegen sollten.

Es sei nun, um wieder auf unsern Gegenstand zu kommen,  $AB$  (Fig. 2.) diejenige gerade Linie, deren Gleichung  $y = \frac{q}{p}x$  ist, wo  $p$  und  $q$  jetzt beide als positive ungerade **Primzahlen** vorausgesetzt werden.  $AD = FB$  sei  $= p$ ,  $AF = DB = q$ ,  $AC = EG = \frac{1}{2}(p-1)$ ,  $AE = CG = \frac{1}{2}(q-1)$ . Bezeichnet man durch  $\mu$  die Anzahl der Gitterpunkte zwischen  $AB$  und  $AD$ , bis zur Ordinate  $CG$  incl. (welche in der Figur durch Sternchen (\*) ausgezeichnet sind), so wird man nach dem oben Bewiesenen  $\left(\frac{q}{p}\right) = (-1)^\mu$  haben. Da die Gleichung unserer Geraden auch so geschrieben werden kann:  $x = \frac{p}{q}y$ , so wird man auf dieselbe Weise, wenn  $\nu$  die Anzahl der Gitterpunkte bezeichnet, welche zwischen  $AB$  und  $AF$  bis zur Abscisse  $EG$  incl. liegen (welche durch kleine Nullen (°) ausgezeichnet sind),  $\left(\frac{p}{q}\right) = (-1)^\nu$  haben. Offenbar erschöpfen aber alle mit \* und alle mit ° bezeichneten Gitterpunkte zusammengenommen, d. h. alle Gitterpunkte *rechts* und alle Gitterpunkte *links* von  $AB$ , **sämmtliche** Gitterpunkte des Rechtecks  $AEGC$ , deren Anzahl  $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$  ist; also ergibt sich  $\mu + \nu = \frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$ , und

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\mu+\nu} = (-1)^{\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)};$$

was zu beweisen war.

Übrigens läßt sich die obige Transformation  $\sum E\left(\frac{qa}{p}\right) \equiv \mu \pmod{2}$  ebenfalls durch eine sehr einfache geometrische Betrachtung nachweisen, wenn man bedenkt, daß  $\sum E\left(\frac{qa}{p}\right)$  nichts anders ist, als die Anzahl der Gitterpunkte, welche auf den *geraden* Ordinaten (denen die Abscissen  $x = 2, 4, 6, \dots, p-1$  entsprechen) zwischen *AB* und *AD* bis zu *BD* liegen, und daß jede Ordinate, von der Axe *AD* bis zu *FB* excl. hin,  $q-1$ , also eine gerade Anzahl Gitterpunkte enthält; so wie, daß die beiden Dreiecke *BAD* und *ABF* congruent sind und daß dieses in Bezug auf *BF* und *BD* genau ebenso liegt, wie jenes in Bezug auf *AD* und *AF*; wovon die Ausführung dem Leser überlassen bleiben mag.

*Anmerkung.* Es gibt Figuren, für welche man durch einfache Formeln die Anzahl der innerhalb derselben liegenden Gitterpunkte bestimmen kann. Stellt man sich z. B. einen Kreis vor, dessen Mittelpunkt im Anfangspunkte der Coordinaten liegt und dessen Radius  $= \sqrt{m}$  ist, so wird die Anzahl der Gitterpunkte *S*, welche dieser Kreis umschließt, die auf den Axen liegenden mitgerechnet, durch folgende Formel gegeben:

$$S = 1 + 4(E(m) - E(\frac{1}{3}m) + E(\frac{1}{5}m) - E(\frac{1}{7}m) + \dots),$$

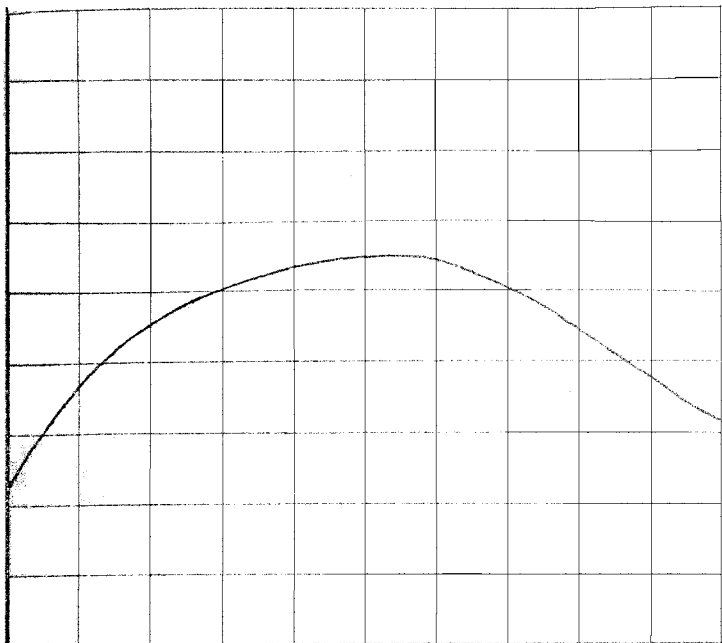
bis die Reihe von selbst abbricht. Wie leicht zu sehen, drückt diese Gleichung eine Relation zwischen der Anzahl der Gitterpunkte eines *Kreises* und der Anzahl der Gitterpunkte eines zwischen zwei *Hyperbeln* eingeschlossenen Segments aus. Setzt man in der Formel

$$\frac{1}{m} S = \frac{1}{m} + 4\left(\frac{1}{m} E(m) - \frac{1}{m} E(\frac{1}{3}m) + \frac{1}{m} E(\frac{1}{5}m) - \text{etc.}\right),$$

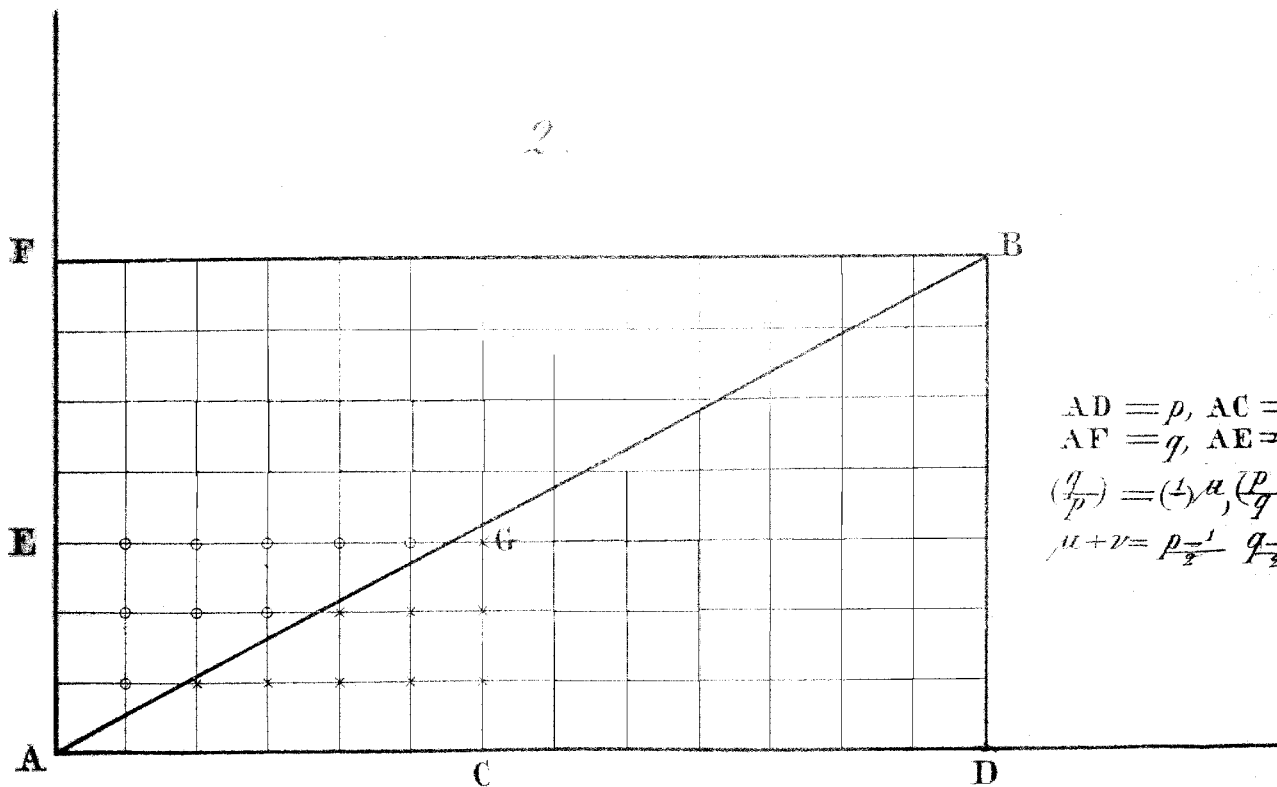
$m = \infty$ , so verwandelt sich die linke Seite in  $\pi$ , während die rechte Seite in  $4(1 - \frac{1}{3} + \frac{1}{5} - \text{etc.})$  übergeht, so daß man hier die *Leibnitz'sche* Formel für  $\pi$  erhält. Es giebt ähnliche Formeln für die Anzahl der Gitterpunkte eines Systems von Ellipsen oder Hyperbelsectoren; auch finden ähnliche Relationen im Raume und in Fällen mit mehr als 3 Dimensionen Statt. Wir werden auf diesen wichtigen Gegenstand, der aufs genaueste mit den Eigenschaften der höheren Formen zusammenhängt, bei einer andern Gelegenheit zurückkommen.

Berlin, im Juli 1844.

1.



2.



$$\begin{aligned}
 AD &= p, AC = p-1 \\
 AF &= q, AE = q^{\frac{p-1}{2}} \\
 \left(\frac{q}{p}\right) &= \binom{p}{1}^u, \left(\frac{p}{q}\right) = \binom{p}{1}^v \\
 \mu + \nu &= \frac{p-1}{2} \cdot \frac{q-1}{2}
 \end{aligned}$$