

**Zeitschrift:** Elemente der Mathematik  
**Herausgeber:** Schweizerische Mathematische Gesellschaft  
**Band:** 37 (1982)  
**Heft:** 4

**Artikel:** Eine Ortsaufgabe und der Satz von Ivory  
**Autor:** Stachel, H.  
**DOI:** <https://doi.org/10.5169/seals-36394>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 18.04.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

# ELEMENTE DER MATHEMATIK

Revue de mathématiques élémentaires – Rivista di matematica elementare

Zeitschrift zur Pflege der Mathematik  
und zur Förderung des mathematisch-physikalischen Unterrichts

El. Math.

Band 37

Nr. 4

Seiten 97–120

Basel, den 10. Juli 1982

## Eine Ortsaufgabe und der Satz von Ivory

W. Wunderlich behandelte in [10] im Zusammenhang mit einem Problem der Satellitengeodäsie die Aufgabe, die gegenseitige Lage von sechs Punkten  $E_1, E_2, E_3, F_1, F_2, F_3$  derselben Ebene aus den neun Distanzen  $\overline{E_i F_j}, i, j \in \{1, 2, 3\}$  zu ermitteln. Er wies nach, dass abgesehen von speziellen Annahmen mit einer stetigen Lösungsschar maximal acht Lösungen existieren, von denen keine zwei durch eine gleichsinnige oder ungleichsinnige Bewegung miteinander zur Deckung gebracht werden können. Besonderes Interesse galt dem *gefährlichen Fall* des Zusammenrückens zweier Lösungen; für diesen ist nach [7] kennzeichnend, dass die sechs Punkte derselben Kurve 2. Ordnung angehören.

Die Frage nach Beziehungen zwischen zwei verschiedenen Lösungen  $E_1, \dots, F_3$  und  $E'_1, \dots, F'_3$  (siehe Abb. 1) steht nun offensichtlich in engem Zusammenhang mit der folgenden

**Aufgabe (A).** *In der euklidischen Ebene  $\pi$  seien die paarweise verschiedenen Punkte  $F_1, F_2, F_3$  gegeben, in  $\pi'$  analog  $F'_1, F'_2, F'_3$ . Existieren Punkte  $E$  in  $\pi$ , deren Entfernungen  $\overline{E F_i}$  für  $i = 1, 2, 3$  übereinstimmen mit den Entfernungen  $\overline{E' F'_i}$  eines geeigneten Punktes  $E' \in \pi'$ ? Wo liegen diese Punkte  $E$ ?*

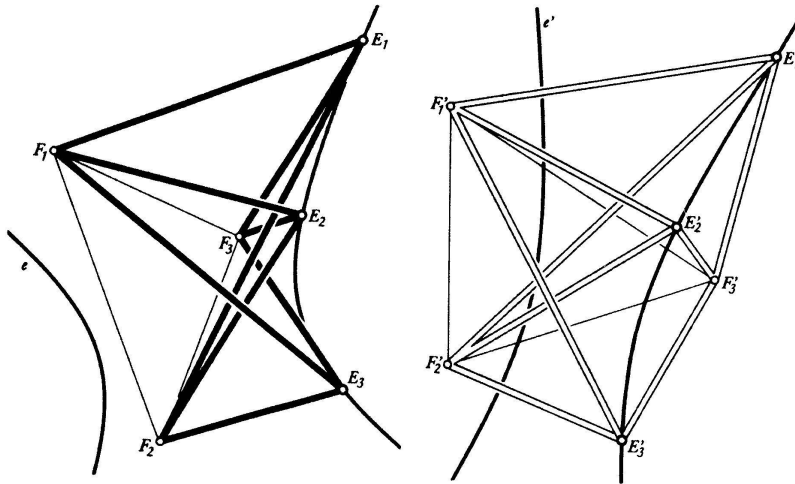
Es gibt mehrere Wege zur Lösung von (A):

1. K. Goldberg untersuchte in [3, 4] die Abhängigkeit der drei *Distanzkoordinaten*  $\overline{X F_1}, \overline{X F_2}, \overline{X F_3}$  von Punkten  $X \in \pi$ . Die Distanzkoordinaten der gesuchten Punkte  $E$  erfüllen gleichzeitig die analoge Beziehung hinsichtlich  $F'_1 F'_2 F'_3$ . Die dabei auftretenden Gleichungen sind allerdings kaum überblickbar.

2. Eine Lösung mit Hilfe der Blaschke-Grünwald-Abbildung ist [8] zu entnehmen.

3. Die Frage (A) lässt sich sofort beantworten, wenn man die *Jacobische Fokaleigenschaft der Flächen 2. Ordnung* heranzieht. Diese besagt (siehe [5, 6]): Konstruiert man für alle Punkte  $X' \in \pi'$  die Pyramiden mit der Basis  $F_1 F_2 F_3$  und den Kantenlängen  $\overline{X' F'_i}, i = 1, 2, 3$ , so bilden deren Spitzen eine Fläche  $\Phi$  2. Ordnung. Die von uns gesuchte Punktmenge  $e = \{E\}$  ist die Spurkurve von  $\Phi$  in  $\pi$ .

Im folgenden sei eine *Lösung der Aufgabe (A)* vorgeführt, die unmittelbar auf höhere Dimensionen zu verallgemeinern ist (vgl. [9]) und sich auch mit Zirkel und Lineal nachvollziehen liesse. Zugleich wird damit jener Hilfssatz erneut bewiesen, der für den in [6] gegebenen Nachweis der Fokaleigenschaft von grundlegender Bedeutung ist. Schliesslich zeigt dieser Lösungsweg einen weiteren Zugang zum *Satz von Ivory* (vgl. [1]).



Wir benützen in  $\pi$  und  $\pi'$  kartesische Koordinatensysteme, die später noch zu spezialisieren sein werden. Es sei

$$E = (\xi, \eta), \quad F_i = (x_i, y_i), \quad E' = (\xi', \eta'), \quad F'_i = (x'_i, y'_i).$$

Aus den für  $E$  und  $E'$  kennzeichnenden Bedingungen

$$(\xi - x_i)^2 + (\eta - y_i)^2 = (\xi' - x'_i)^2 + (\eta' - y'_i)^2 \quad \text{für } i = 1, 2, 3$$

folgt durch Subtraktionen bei  $x_{ij} := x_i - x_j, \dots$

$$\begin{pmatrix} x'_{21} & y'_{21} \\ x'_{31} & y'_{31} \end{pmatrix} \begin{pmatrix} \xi' \\ \eta' \end{pmatrix} = \begin{pmatrix} x_{21} & y_{21} \\ x_{31} & y_{31} \end{pmatrix} \begin{pmatrix} \xi \\ \eta \end{pmatrix} + \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \quad (1)$$

mit gewissen Konstanten  $c_1, c_2$ . Nun wird eine Fallunterscheidung notwendig:

*Fall 1:*  $\{F_1, F_2, F_3\}$  und  $\{F'_1, F'_2, F'_3\}$  sind zwei Dreiecke:

Damit sind die in (1) auftretenden Matrizen regulär; durch (1) ist eine Affinität

$$a: \pi \rightarrow \pi', \quad X = (\xi, \eta) \mapsto X' = (\xi', \eta')$$

dargestellt, die  $E$  auf  $E'$  abbildet (kurz:  $E' = Ea$ ).  $a$  ist durch

$$\overline{XF_j^2} - \overline{XF_1^2} = \overline{XaF_j'^2} - \overline{XaF_1'^2} \quad \text{für } j = 2, 3$$

gekennzeichnet<sup>1)</sup>. Für die gesuchte Punktmenge gilt offensichtlich

$$e = \{E\} = \{X \mid \overline{XF_1} = \overline{XaF_1'}\}.$$

1)  $Xa$  ist Potenzzentrum der drei Kreise mit Mittelpunkt  $F'_i$  und Radius  $\overline{XF'_i}$ .

Wir legen nun die Achsen unserer Koordinatensysteme in die Hauptverzerrungsrichtungen von  $a$  und erreichen – gegebenenfalls nach einer Spiegelung – die Darstellung

$$a: \begin{aligned} \xi' &= \lambda \xi + a_1 \\ \eta' &= \mu \eta + a_2 \end{aligned} \quad \text{mit } \lambda > 0, \quad \mu > 0. \quad (2)$$

Kann ein Punktepaar  $F_j, F'_j$  ohne Änderung von  $a$  und damit auch von  $e$  durch ein anderes Punktepaar  $F = (x, y), F' = (x', y')$  ersetzt werden? Notwendig dafür ist, dass

$$\overline{XF^2} - \overline{XF_1^2} = \overline{XaF'^2} - \overline{XaF_1'^2}$$

eine Identität in  $\xi$  und  $\eta$  darstellt. Dies ergibt

$$\begin{aligned} x &= \lambda x' + b_1 \\ y &= \mu y' + b_2 \end{aligned} \quad (3)$$

mit gewissen Konstanten  $b_1, b_2$ . Damit ist  $F' \mapsto F$  ein Punktepaar der in (3) dargestellten Affinität  $\beta: \pi' \rightarrow \pi$ , die durch  $F_i = F'_i \beta$  für  $i = 1, 2, 3$  bereits eindeutig festgelegt ist.

Wir unterscheiden vier Möglichkeiten:

(i)  $(\lambda - 1)(\mu - 1) \neq 0$ :

Nun existiert ein Punkt  $O \in \pi$  mit  $Oa\beta = O$ , nämlich

$$O = \left( \frac{\lambda a_1 + b_1}{1 - \lambda^2}, \frac{\mu a_2 + b_2}{1 - \mu^2} \right).$$

Wir wählen  $O$  und  $O' = Oa$  als Koordinatenursprung in  $\pi$  bzw.  $\pi'$  und erhalten

$$a: \begin{aligned} \xi' &= \lambda \xi \\ \eta' &= \mu \eta \end{aligned} \quad \beta: \begin{aligned} x &= \lambda x' \\ y &= \mu y' \end{aligned}. \quad (4)$$

(ii)  $\lambda = 1, \mu \neq 1^2$ :

$O$  sei nun ein Punkt mit derselben  $y$ -Koordinate wie in (i);  $O'$  sei Mittelpunkt der Strecke  $OaO\beta^{-1}$ . Werden  $O, O'$  wieder als Koordinatenursprung vorausgesetzt, so entsteht

$$a: \begin{aligned} \xi' &= \xi + a \\ \eta' &= \mu \eta \end{aligned} \quad \beta: \begin{aligned} x &= x' + a \\ y &= \mu y' \end{aligned}. \quad (4^*)$$

2) Dieser Fall bleibt in [6] unberücksichtigt.

Bei (iii)  $\lambda \neq 1, \mu = 1$  vertauschen wir die Koordinatenachsen. Bei (iv)  $\lambda = \mu = 1$  schliesslich sind die Dreiecke  $F_1F_2F_3$  und  $F'_1F'_2F'_3$  kongruent, was natürlich ganz  $\pi$  als Lösungsmenge  $\{E\}$  ergibt.

Die Forderung  $\overline{EF} = \overline{E'F'}$  mit  $E' = Ea, F = F'\beta$  ist nun genau dann erfüllt, wenn bei (i)

$$(\xi - \lambda x')^2 + (\eta - \mu y')^2 = (\lambda \xi - x')^2 + (\mu \eta - y')^2, \quad (5)$$

bei (ii)

$$(\xi - x' - a)^2 + (\eta - \mu y')^2 = (\xi + a - x')^2 + (\mu \eta - y')^2 \quad (5^*)$$

gilt. Wir formen beide Gleichungen so um, dass die linke Seite nur von  $E$ , die rechte nur von  $F'$  abhängt. Da Gleichheit insbesondere für  $F' = F'_1$  bestehen muss, sind beide Seiten konstant, d. h. bei (i)

$$\begin{aligned} e: & \quad (1 - \lambda^2) \xi^2 + (1 - \mu^2) \eta^2 = c \\ f' = \{F'\}: & \quad (1 - \lambda^2) x'^2 + (1 - \mu^2) y'^2 = c, \end{aligned} \quad (6)$$

bei (ii)

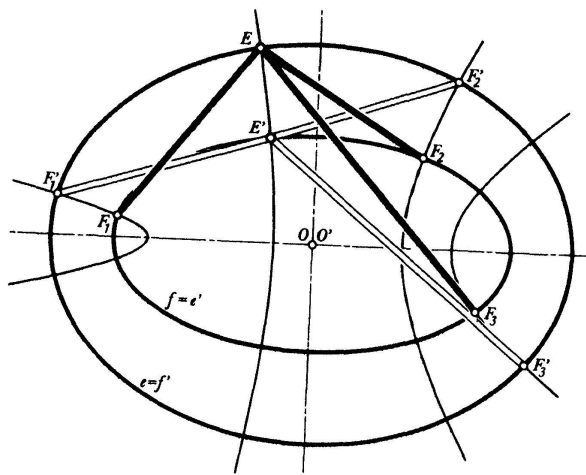
$$\begin{aligned} e: & \quad -4a\xi + (1 - \mu^2) \eta^2 = d \\ f': & \quad -4ax' + (1 - \mu^2) y'^2 = d. \end{aligned} \quad (6^*)$$

Durch Anwendung von  $a$  und  $\beta$  gemäss (4) bzw. (4\*) entstehen

$$\begin{aligned} e' = \{E'\}: & \quad \frac{1 - \lambda^2}{\lambda^2} \xi'^2 + \frac{1 - \mu^2}{\mu^2} \eta'^2 = c \\ f = \{F\}: & \quad \frac{1 - \lambda^2}{\lambda^2} x^2 + \frac{1 - \mu^2}{\mu^2} y^2 = c, \end{aligned} \quad (7)$$

$$\begin{aligned} e': & \quad -4a(\xi' - a) + \frac{1 - \mu^2}{\mu^2} \eta'^2 = d \\ f: & \quad -4a(x - a) + \frac{1 - \mu^2}{\mu^2} y^2 = d. \end{aligned} \quad (7^*)$$

Nun bringen wir die Koordinatenachsen von  $\pi'$  mit jenen von  $\pi$  zur Deckung (siehe Abb.2). Dann ist  $f' = e$  und  $f = e'$ . Bei  $ca \neq 0$  sind  $e$  und  $e'$  gleichartige konfokale Kegelschnitte und wegen  $F'_i \in e, F_i \in e'$  niemals nullteilig. Die Affinität  $a$  ist mit  $\beta$  identisch; sie bildet die Scheitel von  $e$  auf jene von  $e'$  ab. Im parabolischen Fall (ii) werden ferner die Punkte der Achse von  $e$  einer Translation unterworfen. Damit gehört jedes Punktepaar  $E, E'$  derselben Kurve aus der zu  $e$  und  $e'$  konfokalen Schar an.  $E \mapsto E'$  wie auch  $F' \mapsto F$  sind *korrespondierende Punkte*, und  $\overline{EF} = \overline{E'F'}$  ist genau die Aussage des Satzes von Ivory (siehe [2], S. 116). Bei  $\lambda = \mu \neq 1$ , also bei ähnlichen Ausgangsdreiecken, sind  $e$  und  $e'$  Kreise.



Bei  $c=0$  oder  $a=0$  zerfallen  $e$  und  $e'$  in Paare verschiedener, bezüglich der Koordinatenachsen symmetrischer Geraden. Die Einschränkung von  $\beta$  auf  $f'$  ist dann nach (4) und (6) bzw. nach (4\*) eine Kongruenz. Punktpaare  $E, E'$  wie auch  $F', F$  liegen bei (i) auf Kreisen um  $O$ , bei (ii) auf gemeinsamen Normalen der Parallelenpaare; die Ausgangsdreiecke stimmen in einer Seitenlänge überein. Umgekehrt zeigt die Rechnung, dass bei  $\overline{F_1 F_2} = \overline{F'_1 F'_2}$  nach (4) und (6) bzw. (4\*) und (6\*) die Verbindungsgerade  $F'_1 F'_2$  mit  $f'$  neben  $F'_1$  und  $F'_2$  auch noch den Fernpunkt gemein hat. Sie gehört damit ganz zu  $f' = e$ .

*Fall 2:  $\{F_1, F_2, F_3\}$  kollinear,  $\{F'_1, F'_2, F'_3\}$  nicht kollinear:*

Nun sind die Affinitäten  $\alpha$  und  $\beta$  singular; in (2) und (3) ist etwa  $\mu=0$  zu setzen. Die Gleichungen (4) bis (6\*) bleiben weiterhin gültig. Bei zusammenfallenden Koordinatenachsen ist  $f' = e$  wieder ein Kegelschnitt oder, wenn die gegebenen Punktetripel in einer Seitenlänge übereinstimmen, ein Geradenpaar durch  $F'_1, F'_2, F'_3$ .  $\alpha$  bildet die Punkte  $E \in e$  auf die korrespondierenden Punkte der (Haupt-)Achse von  $e$  ab;  $\overline{EF} = \overline{E'F'}$  ist wieder eine Aussage des Satzes von Ivory.

Der Fall *kollinear*  $\{F'_1, F'_2, F'_3\}$  bei *nicht kollinearen*  $\{F_1, F_2, F_3\}$  unterscheidet sich vom Fall 2 lediglich in der Bezeichnung. Nun enthält  $e$  nur Punkte einer Symmetrieachse von  $f$ ; die Randpunkte dieser Punktmenge sind bei nichtzerfallendem  $f$  genau die reellen Brennpunkte von  $f$ .

*Fall 3:  $\{F_1, F_2, F_3\}$  und  $\{F'_1, F'_2, F'_3\}$  sind je kollinear:*

Wir setzen  $y_i = x'_i = 0$  für  $i = 1, 2, 3$  voraus. Die Bedingungen

$$\overline{E'F_j'^2} - \overline{E'F_1'^2} = \overline{EF_j^2} - \overline{EF_1^2}, \quad j = 2, 3$$

führen auf das Gleichungssystem

$$2(x_j - x_1) \xi - 2(y'_j - y'_1) \eta' = (x_j^2 - y_j'^2) - (x_1^2 - y_1'^2), \quad j = 2, 3. \quad (8)$$

Genau dann, wenn die Teilverhältnisse  $(F_1 F_2 F_3)$  und  $(F'_1 F'_2 F'_3)$  verschieden sind,

gibt es eine eindeutige Lösung für  $\xi$  und  $\eta'$ , die wir nach Verschiebung der Koordinatenachsen als  $\xi = \eta' = 0$  voraussetzen wollen. Dies bewirkt

$$x_j^2 - y_j^2 = x_1^2 - y_1^2 \quad \text{für } j=2,3. \quad (9)$$

Für die gesuchten Punkte  $E = (0, \eta)$ ,  $E' = (\xi', 0)$  ist nun  $\overline{EF}_1 = \overline{E'F'_1}$ , also

$$\xi'^2 - \eta^2 = x_1^2 - y_1^2 \quad (10)$$

hinreichend.

Bringt man die Koordinatenachsen von  $\pi$  und  $\pi'$  zur Deckung, so zeigen (9) und (10): Die Punktepaare  $F_i, F'_i$  wie auch  $E', E$  sind Haupt- und Nebenscheitel von Ellipsen einer Konfokalschar. Je nachdem, ob  $E$  Neben- oder Hauptscheitel ist, umfasst  $e$  alle Punkte einer Geraden oder nur jene, die nicht zwischen den reellen Brennpunkten der Konfokalschar liegen. Analog ist  $e'$  Teilmenge der dazu orthogonalen Punktreihe.  $E \mapsto E'$  wie auch  $F'_i \mapsto F_i$  sind also korrespondierende Punkte der Koordinatenachsen. Wieder sind  $F_i, F'_i$  durch andere Punktepaare  $F, F'$  ersetzbar, und  $\overline{EF} = \overline{E'F'}$  ist ein Spezialfall des Satzes von Ivory.

Stimmen die Teilverhältnisse der gegebenen Punktetripel überein, so existiert kein Punkt  $E$  mit der gewünschten Eigenschaft, ausser im Trivialfall der Kongruenz der Tripel. Man ersieht dies aus (8), wobei Einfachheitshalber  $x_1 = y_1 = 0$  gesetzt werden kann.

Zusammenfassend erhalten wir folgende

**Lösung von (A):** Sind die Tripel  $F_1F_2F_3$  und  $F'_1F'_2F'_3$  kongruent, so gibt es zu jedem  $E \in \pi$  ein  $E' \in \pi'$  mit  $\overline{EF}_i = \overline{E'F'_i}$ . Sind die Tripel je kollinear mit gleichen Teilverhältnissen  $(F_1F_2F_3) = (F'_1F'_2F'_3)$ , aber nicht kongruent, so existiert kein Lösungspunkt  $E$ .

In allen anderen Fällen lässt sich  $\pi'$  so mit  $\pi$  zur Deckung bringen, dass  $F'_i \mapsto F_i$  für  $i=1,2,3$  korrespondierende Punkte zweier Kurven  $f', f$  einer Schar konfokaler Kegelschnitte (oder Geraden) sind. Die gesuchte Punktmenge  $e = \{E\}$  ist mit  $f'$  identisch und  $\{E'\}$  mit  $f$ . Die Beziehung  $\overline{EF}_i = \overline{E'F'_i}$  ist Aussage des Satzes von Ivory und gilt für alle Paare korrespondierender Punkte  $F' \in f'$  und  $F \in f$ .  $e$  zerfällt dann und nur dann in zwei verschiedene Geraden, wenn bei nicht kollinearen  $\{F'_1, F'_2, F'_3\}$  ein Paar  $(i, j)$  mit  $i \neq j$  und  $\overline{F_iF_j} = \overline{F'_iF'_j}$  existiert. Genau im Fall kollinearer  $\{F'_1, F'_2, F'_3\}$  enthält  $e$  als ausgeartete Kurve einer Konfokalschar nur Punkte einer einzigen Geraden.

H. Stachel, TU Wien

## LITERATURVERZEICHNIS

- 1 W. Böhm: Ein geometrischer Beweis des Satzes von Ivory. Arch. Math. 16, 135–137 (1965).
- 2 F. Dingeldey: Kegelschnitte und Kegelschnittssysteme. Enc. Math. Wiss. III C1.
- 3 K. Goldberg: Distance coordinates with respect to a triangle of reference. J. Res. nat. Bur. Stand., sect. B76, 145–152 (1972).
- 4 K. Goldberg: Distant coordinates in matrix form. J. Res. nat. Bur. Stand., sect. B81, 61–72 (1977).
- 5 O. Hermes: Die Jacobische Erzeugungsweise der Flächen 2. Grades. J. reine angew. Math. 73, 209–272 (1871).

- 6 C.G.J. Jacobi: Geometrische Theoreme. J. reine angew. Math. 12 (1834) oder 73, 179–206 (1871), oder: Gesammelte Werke, Bd. 7, S. 42–68. Verlag G. Reimer, Berlin 1891.
- 7 K. Killian und P. Meissl: Einige Grundaufgaben der räumlichen Trilateration und ihre gefährlichen Örter. Dt. Geod. Komm. Bayer. Akad. Wiss. (A) 61, 65–72 (1969).
- 8 H. Stachel: Eine Anwendung der kinematischen Abbildung. In Vorbereitung.
- 9 H. Stachel: Bemerkungen zur räumlichen Trilateration. In Vorbereitung.
- 10 W. Wunderlich: Gefährliche Annahmen der Trilateration und bewegliche Fachwerke I. Z. angew. Math. Mech. 57, 297–304 (1977).

© 1982 Birkhäuser Verlag, Basel

0013-6018/82/040097-07\$1.50 ± 0.20/0

## On primitive roots

Baum [2] has given useful criteria for certain primitive roots. Wilansky [6] pointed out that these results can be obtained without use of quadratic reciprocity. The purpose of this note is to derive their theorems and to obtain some more results with a quite simple counting method. We shall deal with odd primes  $p$ . We assume standard results on quadratic residues and primitive roots. An integer  $a$  relatively prime to  $p$  belongs to the exponent  $k > 0$ , modulo  $p$ , if  $a^k \equiv 1 \pmod{p}$  and  $a^n \not\equiv 1 \pmod{p}$  for  $0 < n < k$ . A primitive root modulo  $p$  is a residue which belongs to the exponent  $p-1$ . There are  $\varphi(p-1)$  primitive roots modulo  $p$ , where  $\varphi(x)$  is the Euler phi-function or totient. Euler's totient has the following property: if  $m$  is odd then  $\varphi(2^n \cdot m) = 2^{n-1} \varphi(m)$  ( $n \geq 1$ ) and  $\varphi(2^n \cdot m) = 2^n \varphi(m)$  if  $m$  is even. A quadratic residue, modulo  $p$ , is an integer  $a \neq 0$  such that  $x^2 \equiv a \pmod{p}$  has solutions. QR (QNR) denotes the set of residues, modulo  $p$ , which are quadratic residues (non-residues). With respect to the property of being a primitive root, modulo  $p$ , these sets are denoted by PR(NPR). We note the following familiar results:  $a$  is a quadratic residue modulo  $p$  if and only if  $a^{(p-1)/2} \equiv 1 \pmod{p}$ . This result is known as Euler's criterion. From Euler's criterion it follows that  $(-1/p) = (-1)^{(p-1)/2}$ , where  $(a/p)$  is the Legendre symbol, defined by  $(a/p) = +1$  if  $a \in \text{QR}$ ,  $(a/p) = -1$  if  $a \in \text{QNR}$ . Gauss has given a theorem - known as Gauss' lemma - that puts the information contained in Euler's criterion into a slightly different form. Gauss' lemma makes it possible to evaluate  $(2/p)$ ,  $(3/p)$ ,  $(7/p)$ .

The Legendre symbol has the properties:

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{a \cdot b}{p}\right), \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \quad \text{if } a \equiv b \pmod{p}$$

where  $a, b$  are relatively prime to  $p$ . This makes it possible to calculate  $(-a/p)$  if  $(a/p)$  is known. We give a list of values  $(a/p)$  needed in the sequel.

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv -1 \pmod{4} \end{cases}$$