Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 15 (1960)
Heft: 3

Rubrik: Aufgaben

Am Schlusse sei dieses Ergebnis noch dahin verallgemeinert, dass es zu jedem «Geradheitsgrad» dieses Exponenten unendlich viele Primzahlen der Klasse $8n+1$ gibt. Es soll also der Exponent genau durch 2^k, nicht durch 2^{k+1} teilbar sein. Unter $k=1$ fallen die vorhin erwähnten $p = 16n + 9 = x^2 + 256y^2$. Und für $k \geqq 2$ bedienen wir uns der Primzahlen $x^2 + 16u^2$, nach welchen allen 2 nicht biquadratischer Rest ist. Durch geeignete Wahl der ungeraden Zahlen x und u lässt es sich stets so einrichten, dass $x^2 + 16u^2 \equiv 1 + 2^{k+1} \bmod 2^{k+2}$ wird. Und aus allen diesen Restklassen $x + 4ui \bmod 2^{k+1}$ gibt es unendlich viele Primideale. A. AIGNER, Graz

Aufgaben

Aufgabe 346. Wieviele modulo einer Primzahl p irreduzible, ganzzahlige Polynome mit dem ersten Koeffizienten 1 gibt es, wenn modulo p kongruente Polynome nicht unterschieden werden? H. LENZ, München

Lösung: Wir bezeichnen mit $A(m)$ die Anzahl aller unitärer irreduzibler Polynome vom Grad m über dem Primkörper $P = GF(p)$ der Charakteristik p. Bekanntlich ist

$$x^{p^m} - x$$

das Produkt aller unitärer irreduzibler Polynome vom Grad $d \mid m$. Daher ist

$$p^m = \sum_{d|m} dA(d) ,$$

und hieraus ergibt sich mittels der Umkehrformel von Möbius

$$A(m) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) p^d.$$

A. BAGER, Hjørring

Der Aufgabensteller gibt für die Anzahl der über einem Körper mit p^n Elementen irreduziblen Polynome mit dem ersten Koeffizienten 1 den allgemeineren Ausdruck

$$\frac{1}{m} \sum_{d|m} p^{nd} \mu\left(\frac{m}{d}\right).$$

Weitere Lösungen sandten J. FIEDLER (Regensburg) und W. JÄNICHEN (Berlin-Zehlendorf).

Aufgabe 347. In einer Ebene sind die Kreise K, K' und die Punkte P_1, P_2, P_3 gegeben. Gesucht werden die Punkte X_1, X_2, X_3 auf K und X'_1, X'_2, X'_3 auf K', so dass die drei Punkte-Quintupel $X_1X_2X'_1X'_2P_3$, $X_2X_3X'_2X'_3P_1$, $X_3X_1X'_3X'_1P_2$ je auf einem Kreis liegen. C. BINDSCHEDLER, Küsnacht

Lösung: Wir bezeichnen mit k_i den Kreis durch X_j, X'_j, X_k, X'_k $(i, j, k = 1, 2, 3)$. Je 2 dieser 3 Kreise k_i haben die Geraden $X_1X'_1$, $X_2X'_2$, $X_3X'_3$ zu Chordalen, die einander im Potenzzentrum A der Kreise k_i schneiden. Der Punkt A hat bezüglich der Kreise k_i die Potenz $\overrightarrow{AX_1} \cdot \overrightarrow{AX'_1} = \overrightarrow{AX_2} \cdot \overrightarrow{AX'_2} = \overrightarrow{AX_3} \cdot \overrightarrow{AX'_3} = q^2$. Der Kreis K durch X_1, X_2, X_3 und der Kreis K' durch X'_1, X'_2, X'_3 entsprechen einander in der Inversion am Orthogonalkreis k^* (Mittelpunkt A, Radius q) der Kreise k_i. A ist demnach ein (innerer oder äusserer) Ähnlichkeitspunkt von K und K'. Der Kreis k_i durch $X_jX'_jX_kX'_k$ und P_i enthält auch den an k^* gespiegelten Punkt P'_i von P_i. Die Kreise durch P_i und P'_i schneiden K in den Punktepaaren einer Involution mit dem Involutionszentrum Q_i, das auch auf der Geraden X_jX_k liegen muss. Das gesuchte Dreieck $X_1X_2X_3$ ist demnach dem Kreis K so eingeschrieben, dass seine Seiten X_jX_k durch die Punkte Q_i laufen (Problem des Ottaiano).

Dieses Problem hat für jedes der beiden Ähnlichkeitszentren von K und K' zwei (reell getrennte, zusammenfallende oder konjugiert komplexe) Lösungen. Aus $X_1 X_2 X_3$ erhalten wir durch Spiegelung an k^* die Punkte $X_1' X_2' X_3'$. K. GRÜN, Linz/Donau

Eine Lösung sandten auch G. GEISE (Dresden) und R. LAUFFER (Graz).

Aufgabe 348. Un triangle quelconque ABC admet une infinité de triangles inscrits MNP qui lui sont semblables. Indiquer une construction simple de ces triangles en supposant que $\sphericalangle M = \sphericalangle A$, $\sphericalangle N = \sphericalangle B$, $\sphericalangle P = \sphericalangle C$, et que M est sur BC, N sur AC et P sur AB. Trouver le lieu des centres des cercles circonscrits aux triangles MNP ainsi que l'enveloppe de ces cercles. A. LOEFFLER, Pully-Rosiaz

Lösung: Ein beliebiges Dreieck MNP der gesuchten Schar erhält man leicht aus dem kleinsten Dreieck $M_0N_0P_0$, dessen Seiten zu denen von ABC parallel sind, indem man die drei Höhen alle um den gleichen Winkel um ihren Schnittpunkt H dreht. Die Schnittpunkte M, N, P der gedrehten Höhen mit den Seiten von ABC bilden in der Tat ein Dreieck der Schar, das heisst MNP ist ähnlich zu $M_0N_0P_0$. Alle Dreiecke der Schar haben also den Höhenschnittpunkt H gemeinsam. Es handelt sich also um eine stetige Ähnlichkeitstransformation mit dem Fixpunkt H (Drehstreckung). Die einem Punkte R_0 in $M_0N_0P_0$ entsprechenden Punkte R liegen auf einer Geraden, die zu HR_0 senkrecht ist. Das gilt insbesondere für den Umkreismittelpunkt O, der also für alle Dreiecke der Schar auf einer Normalen zur Eulerschen Geraden HO_0 liegt.

Ist O_0 der Ursprung, die Eulersche Gerade HO_0 die x-Achse und der Ort der Umkreismittelpunkte der y-Achse eines rechtwinkligen Koordinatensystems, so ergibt sich als Gleichung der Schar der Umkreise

$$x^2 + (y - \lambda)^2 - a^2 - \lambda^2 \left(\frac{a}{c}\right)^2 = 0 .$$

Hier ist $\lambda = \overline{O_0O}$ der Parameter, $c = \overline{HO_0}$ und a ist der Umkreisradius von $M_0N_0P_0$. Die Gleichung der Enveloppe ergibt sich in bekannter Weise zu

$$\frac{x^2}{a^2} + \frac{y^2}{a^2 - c^2} = 1 .$$

Das ist eine Ellipse oder eine Hyperbel, je nachdem das Dreieck $M_0N_0P_0$, also auch ABC, spitz- oder stumpfwinklig ist. Ist $a = c$, also ABC rechtwinklig, so bilden die Umkreise ein Büschel durch H und den Höhenschnittpunkt von ABC. Im Fall $O_0 = H$, also $c = 0$, ist ABC gleichseitig und die Umkreise liegen alle konzentrisch. J. SCHAER, Bern

Der Aufgabensteller bemerkt noch, dass jede Seite des Dreiecks MNP eine Parabel einhüllt.

Eine weitere Lösung legte R. LAUFFER (Graz) vor.

Aufgabe 349. Man beweise: Besitzt das Polynom $f(z) = z^3 - 3\,a\,z^2 + 3\,b\,z - c$ $(a \neq 0)$ mit komplexen, also zum Beispiel reellen Koeffizienten a, b, c eine mindestens doppelte Wurzel (sie heisse $z = \zeta$), so ist, mit einem geeigneten Wert der Quadratwurzel, $\zeta = (b - \sqrt{b^2 - a\,c})/a$ eine rationale Funktion $\zeta = R(a, b, c)$ der 3 Koeffizienten; ebenso die eventuelle einfache Wurzel (sie heisse $z = \eta$) von $f(z)$. Der Fall $a = 0$ schliesst sich stetig an: $\zeta = R(0, b, c)$. I. PAASCHE, München

Lösung: Es seien η, ζ, ζ ($\eta = \zeta$ nicht ausgeschlossen) die drei Wurzeln des Polynoms $f(z)$. Dann bestehen, auch wenn $a = 0$ ist, die Gleichungen

$$3\,a = \eta + 2\,\zeta, \quad 3\,b = 2\,\eta\,\zeta + \zeta^2, \quad c = \eta\,\zeta^2. \tag{1}$$

Mittels dieser Gleichungen ergibt sich

$$9\,(a^2 - b) = (\eta - \zeta)^2, \quad 9\,(a\,b - c) = 2\,\zeta\,(\eta - \zeta)^2. \tag{2}$$

Ist nun $\eta \neq \zeta$, so folgt aus (2) und der ersten Formel in (1):

$$\zeta = \frac{a\,b - c}{2\,(a^2 - b)}, \quad \eta = 3\,a - 2\,\zeta = \frac{3\,a^3 - 4\,a\,b + c}{a^2 - b} . \tag{3}$$

Weil eine Doppelwurzel vorliegt, muss die Diskriminante verschwinden, das heisst

$$3 a^2 b^2 - 4 b^3 - 4 a^3 c + 6 a b c - c^2 = 0 .$$

Vermöge dieser Beziehung erfüllen die Wurzeln (3) auch die letzten beiden Bedingungen in (1).

Ist aber $\eta = \zeta$, so folgt aus (1): $\zeta = a$, $b = a^2$, $c = a^3$.

R. STEUERWALD, Alzing/Deutschland

Weitere Lösungen sandten L. CARLITZ (Durham, N. C./USA), J. FIEDLER (Regensburg), E. HERRMANN (Porz a. Rhein), W. JÄNICHEN (Berlin-Zehlendorf), R. LAUFFER (Graz), H. MEILI (Winterthur), H. VOGLER (Wien), H. ZEITLER (Weiden/Oberpfalz).

Aufgabe 350. Die Zahlen $x_1, x_2, \ldots, x_k$ sind (willkürlich) gegeben, und für $n = k + 1$, $k + 2$, $k + 3, \ldots$ ist x_n durch die Rekursionsbeziehung

$$x_n = \frac{x_{n-1} + x_{n-2} + \cdots + x_{n-k}}{k}$$

bestimmt. Man beweise, dass

$$\lim_{n \to \infty} x_n = \frac{x_1 + 2 x_2 + 3 x_3 + \cdots + k x_k}{1 + 2 + 3 + \cdots + k} .$$

G. PÓLYA, Stanford (California)

Lösung: Wir betrachten das Polynom

$$P(x) = k x^k - \sum_{i=1}^{k} x^{k-i}$$

und haben

$$Q(x) = (x - 1) P(x) = k x^{k+1} - (k + 1) x^k + 1.$$

Weil

$$Q'(x) = k(k + 1) x^{k-1} (x - 1)$$

nur die Wurzel 1 mit $Q(x)$ gemeinsam hat, hat $P(x)$ nur einfache, nicht verschwindende Nullstellen: $\alpha_1 = 1, \alpha_2, \ldots, \alpha_k$. Für α_r $(2 \leqq r \leqq k)$ gilt $|\alpha_r| < 1$, denn nach der Dreiecksungleichung folgt aus $|x| \geqq 1$ und $x \neq 1$

$$\left| \sum_{i=1}^{k} x^{k-i} \right| < k \left| x^k \right| = \left| k x^k \right| .$$

Die k Folgen $1, \alpha_i, \alpha_i^2, \alpha_i^3, \ldots, \alpha_i^n, \ldots$ $(1 \leqq i \leqq k)$ genügen für $n \geqq k + 1$ der Rekursionsformel

$$k x_n = x_{n-1} + x_{n-2} + \cdots + x_{n-k} \cdot \qquad (1)$$

Folglich wird (1) auch durch die Linearform

$$x_n = A_1 \alpha_1^n + A_2 \alpha_2^n + \cdots + A_k \alpha_k^n \qquad (2)$$

erfüllt. Da die Determinante

$$\left| \alpha_r^s \right| = \alpha_1 \alpha_2 \ldots \alpha_k \left| \alpha_r^{s-1} \right| \quad (r, s = 1, 2, \ldots, k)$$

nicht verschwindet (Vandermondesche Determinante!), lässt sich das Gleichungssystem

$$x_s = \sum_{r=1}^{k} A_r \alpha_r^s \quad (r, s = 1, 2, \ldots, k)$$

nach den A_r auflösen, wenn $x_1, x_2, \ldots, x_k$ gegeben sind.

Offensichtlich ist jetzt A_1 der Grenzwert von x_n. Setzt man

$$a_n = k x_n + (k - 1) x_{n-1} + \cdots + 2 x_{n-k+2} + x_{n-k+1} , \qquad (3)$$

so folgt für $n \geqq k + 1$ aus (1)

$$a_n = k\, x_{n-1} + (k - 1)\, x_{n-2} + \cdots + 2\, x_{n-k+1} + x_{n-k} = a_{n-1}$$

und damit

$$a_n = a_{n-1} = a_{n-2} = \cdots = a_k = k\, x_k + (k - 1)\, x_{k-1} + \cdots + x_1 .$$

Aus (3) ergibt sich jetzt

$$\lim_{n \to \infty} a_n = A_1 (1 + 2 + \cdots + k) ,$$

also

$$\lim_{n \to \infty} x_n = A_1 = \frac{x_1 + 2\, x_2 + \cdots + k\, x_k}{1 + 2 + \cdots + k} ,$$

was zu beweisen war.

Lösungen von diesem Typus sandten A. BAGER (Hjørring, Dänemark), H. MEILI (Winterthur), R. WAGNER (Karlsruhe) und H. ZEITLER (Weiden, Oberpfalz).

O. REUTTER (Ochsenhausen, Deutschland) bemerkt, dass die konvexe Hülle der Punkte $x_{(i-1)k+1}, x_{(i-1)k+2}, \ldots, x_{ik}$ in der komplexen Ebene ein Polygon P_i $(i = 1, 2, \ldots)$ ist, das alle Punkte x_n mit $n \geqq (i - 1)\, k + 1$ umfasst. Folglich liegt P_{i+1} in P_i. Man kann leicht zeigen, dass die maximalen Diagonalen dieser ineinandergeschachtelten Polygone gegen Null streben, womit die Existenz des Grenzwertes erbracht ist.

K. DANIEL (Berkeley, USA) weist darauf hin, dass die Aufgabe ein Spezialfall einer allgemeineren Fragestellung ist, die im Buch von FELLER: An Introduction to Probability Theory and its Applications, Vol. 1 (2. Aufl.), S. 308 behandelt wird.

Weitere Lösungen sandten C. BINDSCHEDLER (Küsnacht), J. BINZ (Bern), J. FIEDLER (Regensburg), K. GRÜN (Linz), E. HERRMANN (Porz a. Rhein), W. JÄNICHEN (Berlin), R. LAUFFER (Graz), G. RÉVÉSZ (Budapest).

Aufgabe 351. Man beweise: Ist p eine Primzahl der Gestalt $4\, n + 3$, so ist $q = 2\, p + 1$ dann und nur dann Primzahl, wenn $u^2 \equiv 2 \pmod q$ lösbar ist und

$$(1 + u)^{q-1} \equiv 1 \pmod q$$

gilt.

J. PIEHLER, Leuna

Lösung: 1. Wir setzen zunächst voraus, dass $q = 2\, p + 1$ Primzahl ist. Da q wegen $p = 4\, n + 3$ die Gestalt $8\, n + 7$ hat, ist die Kongruenz

$$u^2 \equiv 2 \pmod q \tag{1}$$

auf Grund des zweiten Ergänzungssatzes zum quadratischen Reziprozitätsgesetz lösbar. Dass für die Lösung u^*

$$(1 + u^*)^{q-1} \equiv 1 \pmod q \tag{2}$$

gilt, folgt aus dem kleinen Fermatschen Satz, sobald $(1 + u^*, q) = 1$ bewiesen ist. Aus $(1 + u^*, q) = t > 1$ folgt $t = q$, weil q Primzahl ist. Da in diesem Fall $u^* = k q - 1$ (k ganz) gilt, folgt aus der Kongruenz (1) der Widerspruch $1 \equiv 2 \pmod q$.

2. Es bleibt zu zeigen, dass q Primzahl ist, wenn die Kongruenz (1) lösbar und für die Lösung u^* (2) erfüllt ist. u^* und q sind relativ prim, da jeder gemeinsame Teiler t wegen der Kongruenz (1) auch 2 teilt, was wegen $q = 8\, n + 7$ nur für $t = 1$ der Fall ist. Die Ordnung von $1 + u^*$ werde mit e bezeichnet. Wegen (2) ist e ein Teiler von $q - 1 = 2\, p$. Als Ordnung von $1 + u^*$ kommen daher nur die Teiler von $2\, p$, also die Zahlen 1, 2 und p in Frage. 1 und 2 scheiden aus, weil aus $e = 1$ bzw. $e = 2$ in Widerspruch zu (1) $u^2 \equiv 0 \pmod q$ bzw. $u^2 \equiv 1 \pmod q$ folgt. $1 + u^*$ hat daher die Ordnung p. Daher ist p ein Teiler von $\varphi(q)$, da $(p, 2) = 1$, ist p sogar Teiler von $\frac{\varphi(q)}{2}$, also gilt $2\, p \leqq \varphi(q)$. Da andererseits $\varphi(q) \leqq q - 1 = 2\, p$, gilt $\varphi(q) = q - 1 = 2\, p$, was nur dann erfüllt ist, wenn q Primzahl ist.

HANS VOGLER, Wien

Weitere Lösungen sandten L. CARLITZ (Durham N. C. USA) und J. FIEDLER (Regensburg).

Neue Aufgaben

379. Die Punkte $P_0, P_1, \ldots, P_{k-1}$ $(k \geqq 3)$ seien die Eckpunkte eines geschlossenen Polygons Π in der Ebene. Die Punkte $P_0', P_1', \ldots, P_{k-1}'$ mögen die Seiten P_0P_1, $P_1P_2, \ldots, P_{k-1}P_0$ von innen im Verhältnis $m:n$ teilen. Die Teilpunkte sind dann die Eckpunkte eines neuen Polygons Π'. Durch Wiederholung des gleichen Konstruktionsverfahrens gelangt man von Π' zu einem Polygon Π'' usw. Nach n Schritten erhält man das Polygon $\Pi^{(n)}$ mit den Eckpunkten $P_0^{(n)}, P_1^{(n)}, \ldots P_{k-1}^{(n)}$. Man zeige, dass die Punkte $P_i^{(n)}$ $(0 \leqq i \leqq k-1)$ für $n \to \infty$ gegen den Schwerpunkt S von Π konvergieren. E. HERRMANN, Porz a. Rhein

380. Es sei G der Schwerpunkt, (O, r) die Umkugel eines n-dimensionalen Simplex A_i $(i = 1, 2, \ldots, n+1)$. Es sei weiterhin α_i der Winkel A_iOG.

a) Beweise, dass

$$\sum_{i=1}^{n+1} \cos \alpha_i = (n+1) \cdot \frac{\overline{OG}}{r}.$$

b) Was bedeutet die obige Gleichung, wenn $O \equiv G$? J. SCHOPP, Budapest

381. Aus den Beziehungen ($l = 1093$, Primzahl)

$$2^{14} = 15\,l - 11$$

$$3^2\,11^2 = l - 4$$

$$3^7 = 2\,l + 1$$

ist durch ganz kurze Rechnung

$$2^{l-1} \equiv 1 \pmod{l^2}$$

zu beweisen. L. HOLZER, Rostock

382. Show that

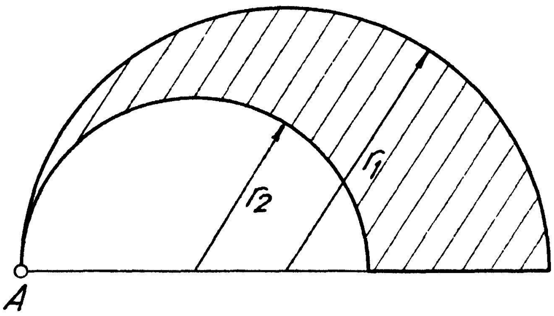
$$\sum_{x,y=0}^{p-1} \left(\frac{a\,x^2 y^2 - b\,x^2 - c\,y^2 + d}{p}\right) = \left(\frac{a}{p}\right) + p\left\{\left(\frac{a}{p}\right) + \left(\frac{b}{p}\right) + \left(\frac{c}{p}\right) + \left(\frac{d}{p}\right)\right\}\left(\frac{a\,d - b\,c}{p}\right),$$

where p is an odd prime, (a/p) is the Legendre symbol and $a\,b\,c \not\equiv 0 \pmod{p}$.
L. CARLITZ, Durham N.C. USA

Aufgaben für die Schule

Es wird kein Anspruch auf Originalität der Aufgaben erhoben; Autoren und Quellen werden im allgemeinen nicht genannt. Die Daten für Aufgaben aus der Darstellenden Geometrie sind durchwegs so festgelegt, dass der Ursprung des Koordinatensystems in der Mitte des linken Randes eines Blattes vom Format A 4 gewählt werden soll, x-Achse nach rechts, y-Achse nach vorn, z-Achse nach oben, Einheit 1 cm. Anregungen und Beiträge sind zu senden an Prof. Dr. WILLI LÜSSY, Büelrainstrasse 51, Winterthur.

1. Die Zahl 1 ist so darzustellen, dass alle Ziffern von 0 bis 9 genau einmal verwendet werden.
   ▶ Viele Lösungen, zum Beispiel $123456789^0 = 1$.
2. Man wählt willkürlich N Zahlen. Wie gross muss N mindestens sein, damit unter diesen Zahlen entweder n gleiche, oder dann sicher n verschiedene sind?
   ▶ $N_{min} = (n-1)^2 + 1$.
3. Die schraffierte Figur wird in A aufgehängt. Welchen Winkel bildet bei Gleichgewicht die Schwerlinie durch A mit dem Durchmesser?



▶ Denkt man sich den kleinen Halbkreis wieder eingefügt, so ändert sich nichts am Gleichgewicht, folglich

$$\operatorname{tg}\varphi = \frac{4}{3\pi}; \quad \varphi = 23{,}^\circ 0.$$

Der Grenzübergang $r_2 \to r_1$ ergibt *nicht* den Schwerpunkt der Halbkreislinie!

4. Konstruiere das Dreieck ABC, von dem der Mittelpunkt M des Umkreises, der Mittelpunkt I des Inkreises und derjenige (I_a) des Ankreises an a gegeben sind.
   ▶ Die Punkte B, I_a, C, I sind die Ecken eines Sehnenvierecks, dessen Umkreiszentrum auf dem Umkreis des Dreiecks liegt.
5. Es sind zwei Geraden a und b gegeben:

$$a\begin{cases} A_1(10;\ 7;\ 0), \\ A_2(\ 0;\ -2;\ 11); \end{cases} \qquad b\begin{cases} B_1(\ 0;\ 9;\ 0), \\ B_2(15;\ 0;\ 13). \end{cases}$$

Konstruiere die erste Hauptgerade, auf der a und b eine Strecke der Länge 6 bestimmen.
▶ Schnitt eines schiefen Kreiszylinders um a mit der Gerade b.

Mitteilung

1960 International Congress for Logic, Methodology and Philosophy of Science

An international congress for logic, methodology and philosophy of science will be held at Stanford University, Stanford, California, USA, from August 24 to September 2, 1960, under the auspices of the *International Union for History and Philosophy of Science*.

The proceedings of the congress will be organized into the following eleven sections:

1. Mathematical logic.
2. Foundations of mathematical theories.
3. Philosophy of logic and mathematics.
4. General problems of methodology and philosophy of science.
5. Foundations of probability and induction.
6. Methodology and philosophy of physical sciences.
7. Methodology and philosophy of biological and psychological sciences.
8. Methodology and philosophy of social sciences.
9. Methodology and philosophy of linguistics.
10. Methodology and philosophy of historical sciences.
11. History of logic, methodology and philosophy of science.

The proceedings will consist of a number of invited addresses, in addition to brief contributed papers. The closing date for submission of abstracts of contributed papers is March 1, 1960.

Information about membership fees and other details of the congress may be obtained by writing Professor Patrick Suppes, Serra House, Stanford University, Stanford, California, USA.