Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 17 (1962)
Heft: 3

Rubrik: Kleine Mitteilungen

Une conséquence immédiate de notre théorème est que le problème s'il existe une infinité de nombres triangulaires qui ne sont pas sommes de deux nombres triangulaires >0 équivaut au problème s'il existe une infinité de nombres premiers qui sont sommes de carrés de deux nombres naturels consécutifs. Il résulte sans peine de l'hypothèse H_0 de M. A. SCHINZEL, exprimée dans les Acta Arithmetica IV (1958), p. 188, qu'il existe une infinité de tels nombres premiers. Pour $n \leqq 10$ on obtient les nombres premiers de la forme $n^2 + (n+1)^2$ seulement pour $n = 1, 2, 4, 5, 7$ et 9: ce sont les nombres 5, 13, 41, 61, 113, 181. W. SIERPIŃSKI (Varsovie)

Ungelöste Probleme

Nr. 43. Ein dem Unterzeichneten von A. J. H. M. VAN DE VEN mitgeteiltes Problem lautet wie folgt: Gibt es in der euklidischen Ebene sechs nicht auf ein und demselben Kegelschnitt gelegene Punkte derart, dass alle sechs durch je fünf der Punkte bestimmten Kegelschnitte untereinander kongruent sind? – Prinzipiell lässt sich dieses Problem in endlich vielen Schritten auf algebraischem Wege entscheiden, die Rechnungen sind aber kaum zu übersehen. Dasselbe Problem für vier Punkte und Kreise führt auf die vollständige Lösung, die durch drei beliebige Punkte und das Orthozentrum des durch sie gebildeten Dreiecks gegeben ist.

J. J. SCHÄFFER, Montevideo

Kleine Mitteilungen

Einige Bemerkungen zu einer Aufgabe von L. CARLITZ

Die in einer Aufgabe von L. CARLITZ [1] gestellte Frage nach der Bestimmung der Anzahl N der Lösungen der Kongruenz

$$(x^2-1)(x^2-2)\dots\left(x^2-\frac{p-1}{2}\right) \equiv 0 \pmod p$$

erfordert für die beiden Fälle $p \equiv 1 \pmod 4$ und $p \equiv 3 \pmod 4$ eine ganz verschiedenartige Behandlung. Für den ersten Fall ergibt sich ohne weiteres

$$N = \frac{p-1}{2}, \quad p \equiv 1(4), \tag{1}$$

da es für $p = 4z+1$ zwischen 0 und $p/2$ gleich viele quadratische Reste und Nichtreste gibt. Für den Fall $p = 4z+3$ kann man die zuerst von DIRICHLET bewiesenen Formeln für die Klassenzahl des quadratischen Körpers $R(\sqrt{-p})$ benutzen, da in ihnen der Überschuss der Anzahl der zwischen 0 und $p/2$ liegenden quadratischen Reste über die Anzahl der Nichtreste, also der Ausdruck $N - (p-1)/2$ auftritt [2]. Man erhält so die Formeln [3]

$$\begin{aligned} N &= \frac{p-1}{2} + 3h(-p), \quad p \equiv 3(8), \\ N &= \frac{p-1}{2} + h(-p), \quad p \equiv 7(8). \end{aligned} \tag{2}$$

Im folgenden wollen wir zeigen, dass sich für den Fall $p = 4z+3$ N auch unabhängig von der Klassenformel bestimmen lässt und zwar als mod p kleinster positiver Rest eines geschlossenen Ausdrucks, der im wesentlichen von einer gewissen Bernoullischen Zahl abhängt. Umgekehrt ergibt sich daraus eine interessante Kongruenz, der im Falle $p = 4z+3$ die Klassenzahl $h(-p)$ genügt.

Im folgenden sei also $p = 4z + 3$. Da nach dem Eulerschen Kriterium $a^{p-1/2} \equiv \pm 1 \bmod p$ ist, je nachdem, ob a Rest oder Nichtrest ist, ist die gesuchte Anzahl N der Lösungen der vorgelegten Kongruenz

$$N \equiv \sum_{a=1}^{\frac{p-1}{2}} \left(1 + a^{\frac{p-1}{2}}\right) \equiv \frac{p-1}{2} + \sum_{a=1}^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \bmod p .$$

Es kommt zur Bestimmung von N auf die Summe

$$\sum_{a=1}^{\frac{p-1}{2}} a^{\frac{p-1}{2}} = 1^{\frac{p-1}{2}} + 2^{\frac{p-1}{2}} + \cdots + \left(\frac{p-1}{2}\right)^{\frac{p-1}{2}}$$

an. Nun gilt bekanntlich für die Summe der k-ten Potenzen der n ersten natürlichen Zahlen die Formel

$$1^k + 2^k + \cdots + n^k = \frac{n^{k+1}}{k+1} + \frac{n^k}{2} + \binom{k}{1}\frac{B_1}{2} n^{k-1} - \binom{k}{3}\frac{B_2}{4} n^{k-3} + \binom{k}{5}\frac{B_3}{6} n^{k-5} - + \cdots ,$$

worin die B_i die Bernoullischen Zahlen bedeuten.

$$\left(B_1 = \frac{1}{6},\ B_2 = \frac{1}{30},\ B_3 = \frac{1}{42},\ B_4 = \frac{1}{30},\ B_5 = \frac{5}{66}, \ldots\right)$$

Aus ihr folgt die andere

$$k\,[1^{k-1} + 2^{k-1} + \cdots + (n-1)^{k-1}] = n^k - k\frac{n^{k-1}}{2} + \binom{k}{2} B_1 n^{k-2} - \binom{k}{4} B_2 n^{k-4} + \\ + \binom{k}{6} B_3 n^{k-6} - + \cdots .$$

Während die linke Seite nur für ganzzahlige n Bedeutung hat, kann die rechte auch auf beliebige Werte n ausgedehnt werden. So ergibt sich die Bernoullische Funktion k-ter Ordnung

$$\varphi(n, k) = n^k - \frac{1}{2} k\, n^{k-1} + \binom{k}{2} B_1 n^{k-2} - \binom{k}{4} B_2 n^{k-4} + \binom{k}{6} B_3 n^{k-6} - + \cdots .$$

Es ist also

$$k\,[1^{k-1} + 2^{k-1} + \cdots + n^{k-1}] = \varphi(n, k) + k\, n^{k-1}$$

und

$$N \equiv \frac{p-1}{2} + \sum_{a=1}^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \equiv \frac{p-1}{2} + 2\,\varphi\left(\frac{p-1}{2}, \frac{p+1}{2}\right) + \left(\frac{p-1}{2}\right)^{\frac{p-1}{2}} \bmod p ,$$

also, da $k - 1 = \frac{p-1}{2}$, also $k = \frac{p+1}{2}$ (gerade) und $n = \frac{p-1}{2}$,

$$N \equiv \frac{p-1}{2} + 2\,\varphi\left(-\frac{1}{2}, \frac{p+1}{2}\right) + \left(\frac{p-1}{2}\right)^{\frac{p-1}{2}} \bmod p .$$

Nun ist für ein gerades k

$$\varphi\left(\frac{1}{2}, k\right) = \left(\frac{1}{2}\right)^k - \frac{1}{2} k \left(\frac{1}{2}\right)^{k-1} + \binom{k}{2} B_1 \left(\frac{1}{2}\right)^{k-2} - \binom{k}{4} B_2 \left(\frac{1}{2}\right)^{k-4} + - \cdots ,$$

$$\varphi\left(-\frac{1}{2}, k\right) = \left(\frac{1}{2}\right)^k + \frac{1}{2} k \left(\frac{1}{2}\right)^{k-1} + \binom{k}{2} B_1 \left(\frac{1}{2}\right)^{k-2} - \binom{k}{4} B_2 \left(\frac{1}{2}\right)^{k-4} + - \cdots ,$$

$$\varphi\left(-\frac{1}{2}, k\right) - \varphi\left(\frac{1}{2}, k\right) = k \left(\frac{1}{2}\right)^{k-1} .$$

Die Theorie der Bernoullischen Funktionen [4] liefert den Wert

$$\varphi\left(\frac{1}{2}, k\right) = (-1)^{\frac{k}{2}} \frac{2^k - 1}{2^{k-1}} B_{\frac{1}{2}k}, \text{ wenn } k \equiv 0 \bmod 2,$$

folglich

$$\varphi\left(-\frac{1}{2}, k\right) = (-1)^{\frac{k}{2}} \frac{2^k - 1}{2^{k-1}} B_{\frac{1}{2}k} + k\left(\frac{1}{2}\right)^{k-1}$$

und, da $k = \dfrac{p+1}{2} = 2z + 2$,

$$N = \frac{p-1}{2} + 2(-1)^{z+1} \frac{2^{\frac{p+1}{2}} - 1}{2^{\frac{p-1}{2}}} B_{z+1} + (2z+2)\left(\frac{1}{2}\right)^{2z} - \left(\frac{1}{2}\right)^{2z+1} \bmod p$$

$$\equiv \frac{p-1}{2} + 2(-1)^{z+1} \frac{2\left(\frac{2}{p}\right) - 1}{\left(\frac{2}{p}\right)} B_{z+1} + (p+1)\left(\frac{1}{2}\right)^{\frac{p-1}{2}} - \left(\frac{1}{2}\right)^{\frac{p-1}{2}} \bmod p,$$

$$N \equiv \frac{p-1}{2} + (-1)^{z+1} 2\left(2 - \left(\frac{2}{p}\right)\right) B_{z+1} \bmod p,$$

$$N \equiv \frac{p-1}{2} + (-1)^{\frac{p+1}{4}} 2\left(2 - \left(\frac{2}{p}\right)\right) B_{\frac{p+1}{4}} \bmod p,\ p = 4z + 3 > 3, \tag{3}$$

$$\begin{aligned} p &\equiv 3\ (8); \quad N \equiv \frac{p-1}{2} - 6\, B_{\frac{p+1}{4}} \bmod p, \\ p &\equiv 7\ (8); \quad N \equiv \frac{p-1}{2} + 2\, B_{\frac{p+1}{4}} \bmod p. \end{aligned} \tag{4}$$

Da B_{z+1} ein Bruch ist, hat die Kongruenz (3) nur dann eine Bedeutung, wenn der Nenner von $B_{z+1} = B_{(p+1)/4}$ relativ prim ist zu p. Nach dem v. Staudt-Clausenschen Satz [5] über die Beschaffenheit des Nenners einer Bernoullischen Zahl B_n enthält der Nenner von B_n nur solche Primzahlen α, für die $\alpha - 1$ ein Teiler von $2n$ ist, die also nicht grösser als $2n + 1$ sind. In unserem Fall ist $2n + 1 = (p+1)/2 + 1 = (p+3)/2$. Wäre p ein solcher Teiler, so wäre $p \leqq (p+3)/2$, $p = 3$, da p ungerade ist. Hier versagt in der Tat unsere Formel, da für $p = 3$ $(2/p) = -1$ ist, $N \equiv 1 - 2(2+1)\,1/6 \equiv 0 \bmod 3$, während doch $N = 2$ ist. (3) gilt also nur, wenn $p = 4z + 3 > 3$.

Die Kongruenz (3) steht im Zusammenhang mit einem anderen Problem der Zahlentheorie. Aus dem Wilsonschen Satz ergibt sich nämlich, dass für $p = 4z + 3$

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \equiv (-1)^{\beta} \bmod p,$$

wobei β die Anzahl der quadratischen Nichtreste von p ist, welche $< p/2$ sind (P. Bachmann, *Niedere Zahlentheorie I*, 1902, S. 178 und 179). Aus der Formel (3) ergibt sich nun unmittelbar β als mod p kleinster pos. Rest aus der Kongruenz

$$\beta \equiv \frac{p-1}{2} - \frac{N}{2} \equiv \frac{p-1}{4} + (-1)^{\frac{p-3}{4}} \left(2 - \left(\frac{2}{p}\right)\right) B_{\frac{p+1}{4}} \bmod p.$$

Satz: Für jede Primzahl $p = 4z + 3 > 3$ ist $\left(\dfrac{p-1}{2}\right)! \equiv (-1)^{\beta}$ mod p, wobei β der mod p kleinste pos. Rest ist, der sich aus der Kongruenz

$$\beta \equiv \frac{p-1}{4} + (-1)^{\frac{p-3}{4}} \left(2 - \left(\frac{2}{p}\right)\right) B_{\frac{p+1}{4}} \bmod p$$

ergibt.

Vergleicht man die Formeln (2) und (4), so erhält man

$$\begin{aligned} p \equiv 3\ (8);\quad h(-p) &\equiv -2\,B_{\frac{p+1}{4}} \bmod p\,, \quad p \neq 3 \\ p \equiv 7\ (8);\quad h(-p) &\equiv 2\,B_{\frac{p+1}{4}} \bmod p\,, \end{aligned} \tag{5}$$

also

$$p = 4z + 3;\quad h(-p) \equiv 2\left(\frac{2}{p}\right) B_{\frac{p+1}{4}} \bmod p\,. \tag{6}$$

Satz: Für $p = 4z + 3 > 3$ genügt die Klassenzahl $h(-p)$ des quadratischen Körpers $R(\sqrt{-p})$ der Kongruenz

$$h(-p) \equiv 2\left(\frac{2}{p}\right) B_{\frac{p+1}{4}}\ mod\ p\,.$$

W. Jänichen, Berlin-Zehlendorf

LITERATURVERZEICHNIS

[1] Aufgabe Nr. 359. El. d. Math. *14*, 89 (1959).
[2] David Hilbert, *Bericht über die Theorie der algebraischen Zahlkörper* (Georg Reimer, Berlin 1897), S. 320.
[3] El. Math. *15*, 110, 111 (1960).
[4] O. Schlömilch, *Compendium der höheren Analysis*, Bd. II (Fr. Vieweg, Braunschweig 1866), S. 207f.
[5] P. Bachmann, *Niedere Zahlentheorie* (B. G. Teubner, Leipzig) II. Bd., S. 43f. – Hardy-Wright, *Einführung in die Zahlentheorie* (Oldenburg, München 1958), S. 101.

Neue Aufgaben[1])

Aufgabe 429. Eine Ellipse mit gegebenem Achsenverhältnis $b : a = \beta$ und festem Mittelpunkt, aber mit nach Grösse und Richtung veränderlichen Achsen, berührt beständig zwei gegebene Parallelen im Abstand d vom Mittelpunkt. Man bestimme die beiden Ränder des Gebietes, das von der Ellipse überstrichen wird (Enveloppe der Schar im engeren Sinne). C. Bindschedler, Küsnacht

Aufgabe 430. Démontrer que chacune des formules

$$n \mid 2^n + 1\,, \quad n \mid 2^{2n} + 1\,, \quad n \mid 2^n + 2$$

a une infinité de solutions en nombres naturels n. W. Sierpiński, Varsovie

Aufgabe 431. Zu beweisen: Stimmen zwei auf einer Fläche Φ verlaufende Kurven c_1 und c_2 in einem Punkte U des wahren Umrisses von Φ in den Linienelementen von genau n-ter Ordnung überein, so haben ihre Projektionen c_1^* und c_2^* in der Projektion U^* von U ein Linienelement von mindestens $(n+1)$-ter Ordnung gemeinsam. Berühren die Flächenkurven c_1 und c_2 in U den wahren Umriss von Φ, so haben ihre Projektionen c_1^* und c_2^* sogar ein Linienelement von mindestens $(n+2)$-ter Ordnung gemeinsam, wobei vorausgesetzt wird, dass die Kurven c_1 und c_2 in U keine projizierende Tangente haben.
H. Vogler, Wien

[1]) Umständehalber enthält das vorliegende Heft ausnahmsweise keine Aufgabenlösungen.