Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 30 (1975)
Heft: 6

Rubrik: Kleine Mitteilungen

Hence $(y - k_2)/(y - k_1) = \varepsilon_i$, $(i = 0, 1, 2)$, where ε_i are the three cube roots of

$$\frac{k_2}{k_1} = \frac{-\frac{r}{2} - \sqrt{\left(\frac{r}{2}\right)^2 + \left(\frac{q}{3}\right)^3}}{-\frac{r}{2} + \sqrt{\left(\frac{r}{2}\right)^2 + \left(\frac{q}{3}\right)^3}}.$$

Direct solution yields

$$y = \frac{k_2 - \varepsilon_i k_1}{1 - \varepsilon_i},$$

a formula which is readily simplified to give $y = -k_1(\varepsilon_i + \varepsilon_i^2)$, or more explicitly,

$$y = \frac{3}{q}\left[\frac{r}{2} - \sqrt{\left(\frac{r}{2}\right)^2 + \left(\frac{q}{3}\right)^3}\right](\varepsilon_i + \varepsilon_i^2), \quad (i = 0, 1, 2).$$

B. de la Rosa, University of the Orange Free State, Bloemfontein, S. A.

BIBLIOGRAPHY

[1] I. T. ADAMSON, *Introduction to Field Theory*, Oliver & Boyd (1964).
[2] H. W. TURNBULL, *Theory of Equations*, Oliver & Boyd (1944).
[3] J. V. USPENSKY, *Theory of Equations*, McGraw-Hill (1948).

Kleine Mitteilungen

On a theorem of Cipolla

Cipolla proved 1904 in [1] the following theorem: The number

$$\left(2^{2^m} + 1\right)\left(2^{2^n} + 1\right) \cdots \left(2^{2^s} + 1\right),$$

with $m > n > \ldots > s$, is a pseudoprime if and only if $2^s > m$ (a positive integer n is called a pseudoprime if $n \mid 2^n - 2$ and n is composite).

In many applications it is usefull to have 'strong' pseudoprimes. In the following definition we give a precise meaning to this concept:

Definition: The positive integer n is a k-th order pseudoprime if and only if $k \mid n - 1$, $2^{(n-1)/k} \equiv 1 \pmod{n}$ and n is composite.

In this paper we prove the following generalization of Cipolla's result:

Theorem: $L = \left(2^{2^m} + 1\right)\left(2^{2^n} + 1\right) \ldots \left(2^{2^s} + 1\right)$, with $m > n > \cdots > s$, is a 2^t-th order pseudoprime if and only if $2^s > m + t$.

Proof:

$$L - 1 = 2^{2^m + 2^n + \cdots + 2^s} + \cdots + 2^{2^m} + 2^{2^n} + \cdots + 2^{2^s} = 2^{2^s} \cdot M ,$$

where M is an odd number. We have

$$\frac{L-1}{2^t} = 2^{2^s - t} \cdot M$$

and moreover in view of the well-known identity

$$F_j = 2 + F_0 \cdot F_1 \cdot F_2 \ldots F_i \ldots F_{j-1} ,$$

where $F_i = F(i) = 2^{2^i} + 1$ is the i-th Fermat number, the factors F_j of L are coprime.

Hence in order to show that,

$$2^t \mid L - 1 \text{ and } 2^{(L-1)/2^t} \equiv 1 \pmod{L} \text{ if and only if } 2^s > m + t ,$$

it is enough to show that $2^s > m + t$ implies that $2^t \mid L - 1$ and $2^{(L-1)/2^t} \equiv 1 \pmod{F_u}$ for $u = s, \ldots, n, m$ and that $2^{(L-1)/2^t} \equiv 1 \pmod{F_m}$ implies that $2^s > m + t$.

Now $(L - 1)/2^t = 2^{2^s - t} \cdot M$ and so certainly $2^t \mid L - 1$ if $2^s > m + t$. Moreover

$$F_u \mid F_{u+1} - 2 \mid [F(2^s - t) - 1]^M - 1$$

if $u + 1 \leq 2^s - t$. Since $u + 1 \leq m + 1 \leq 2^s - t$ by the assumption this certainly holds. On the other hand if

$$F_m \mid [F(2^s - t) - 1]^M - 1$$

the known fact $a^m + 1 \mid a^n - 1 \iff n = 2mk,\ a, m, n, k \in \mathbf{N}, a > 1$, gives $2^{m+1} \mid 2^{2^s - t} \cdot M$, and since M odd this implies that $2^s > m + t$. This completes the demonstration.

A. Rotkiewicz (Warsaw) and R. Wasén (Uppsala)

REFERENCES

[1] M. Cipolla, Sui numeri composti P, che verificano la congruenza di Fermat $a^{P-1} \equiv 1 \pmod{P}$, Ann. Matematica (3), *9*, 139–160 (1904).

Congruences for Sums of Powers of Primitive Roots and Ramanujan's Sum

Let n be an integer > 2 which has primitive roots. It is well-known (cf. [4], Theorem 65) that n must be 4, p^α, or $2p^\alpha$, where p is an odd prime and α is a positive integer; and that the number of primitive roots of n is then $\varphi(\varphi(n))$, where φ is the Euler totient function. Let m be any positive integer and let $S_r^{(m)}$ denote the sum of the m-th powers of the primitive roots of n, which are less than n, taken r at a time, where $1 \leq r \leq \varphi(\varphi(n))$.

Throughout the following we write $k = \varphi(n)$ and $\zeta = \zeta_k = \exp(2\pi i/k)$. It is well-known (cf. [4], p. 157) that the numbers ζ^h, where $1 \le h \le k$, $(h, k) = 1$, will be the primitive k-th roots of unity. Let $T_r^{(m)}$ denote the sum of the m-th powers of the primitive k-th roots of unity taken r at a time, where $1 \le r \le \varphi(k)$.

In this paper we prove the following theorem and discuss some particular cases of the theorem. We also discuss a method of evaluating the sums $T_r^{(m)}$ in terms of the Ramanujan sum.

Theorem. For $1 \le r \le \varphi(k)$, $S_r^{(m)} \equiv T_r^{(m)} \pmod{n}$.

Proof: Let

$$f_k(x, m) = \prod_{1 \le h' \le k} (x - \zeta^{h' m}) \tag{1}$$

and

$$F_k(x, m) = \prod_{\substack{1 \le h \le k \\ (h, k) = 1}} (x - \zeta^{h m}) . \tag{2}$$

Then we have

$$f_k(x, m) = \prod_{1 \le h' \le k} (x - \zeta^{h' m}) = \prod_{d | k} \prod_{\substack{1 \le h' \le k \\ (h', k) = d}} \left[x - \exp\left(\frac{2\pi i h' m}{k}\right)\right]$$

$$= \prod_{d | k} \prod_{\substack{1 \le h \le k/d \\ (h, k/d) = 1}} \left[x - \exp\left(\frac{2\pi i h m}{k/d}\right)\right] .$$

Hence

$$f_k(x, m) = \prod_{d | k} F_{k/d}(x, m) . \tag{3}$$

Now using the Möbius inversion formula in the product form [see E. Landau, Elementary Number Theory (New York 1966), p. 236, exercise 10]

$$g(n) = \prod_{d | n} f(d) = \prod_{d | n} f(n/d) \Rightarrow f(n) = \prod_{d | n} (g(d))^{\mu(n/d)}$$

we obtain

$$F_k(x, m) = \prod_{d | k} f_d(x, m)^{\mu(k/d)} , \tag{4}$$

where μ is the Möbius function.

It follows from (1) that the degree of the polynomial $f_k(x, m)$ in x is k, so that the degree of the polynomial $f_d(x, m)$ is d and hence the degree of the polynomial on the r.h.s. of (4) is $\sum_{d | k} d \mu(k/d) = \varphi(k)$ (cf. [3], (16.3.1)). Also, the degree of the polynomial on the l.h.s. of (4) is $\varphi(k)$ in virtue of (2).

Let g be a primitive root of n. It is well known (cf. [4], Theorem 62) that the numbers g^h, where $1 \le h \le k$, $(h, k) = 1$, form a set of incongruent primitive roots modulo n. Let $\overline{S}_r^{(m)}$ denote the sum of the m-th powers of the numbers g^h taken r at a time, where $1 \le r \le \varphi(k)$. It is clear that

$$S_r^{(m)} \equiv \overline{S}_r^{(m)} \pmod{n} . \tag{5}$$

Since g is a primitive root of n, we have $g^k - 1 \equiv 0 \pmod n$ and $g^d - 1 \not\equiv 0 \pmod n$ for $1 \leq d < k$. Hence, if $d \mid k$ and $d \neq k$, we see from (1) that the numbers g^{hm}, where $1 \leq h \leq k$, $(h,k) = 1$, do not satisfy the congruence $f_d(x,m) \equiv 0 \pmod n$, but satisfy the congruence $f_k(x,m) \equiv 0 \pmod n$, since $f_k(g^{hm}, m) = \prod_{1 \leq h' \leq k} (g^{hm} - \zeta^{h'm})$, which is divisible by $\prod_{1 \leq h' \leq k} (g^h - \zeta^{h'}) = g^{hk} - 1 \equiv 0 \pmod n$. Hence from (4), it follows that the congruence $F_k(x,m) \equiv 0 \pmod n$ is satisfied by the $\varphi(k)$ incongruent numbers g^{hm}, where $1 \leq h \leq k$, $(h,k) = 1$. Since the degree of the congruence is also $\varphi(k)$, it follows that these numbers are all the incongruent roots of $F_k(x,m) \equiv 0 \pmod n$.

Hence it follows that

$$\prod_{\substack{1 \leq h \leq 1 \\ (h,k) = k}} (x - g^{hm}) \equiv F_k(x,m) \equiv \prod_{\substack{1 \leq k \leq k \\ (h,k) = 1}} (x - \zeta^{hm}) \pmod n ,$$

so that

$$x^{\varphi(k)} + \sum_{r=1}^{\varphi(k)} (-1)^r \overline{S}_r^{(m)} x^{\varphi(k)-r} \equiv x^{\varphi(k)} + \sum_{r=1}^{\varphi(k)} (-1)^r T_r^{(m)} x^{\varphi(k)-r} \pmod n .$$

Hence for $1 \leq r \leq k$, we have

$$\overline{S}_r^{(m)} \equiv T_r^{(m)} \pmod n . \tag{6}$$

Now the theorem follows from (5) and (6).

As particular cases of the theorem, we have the following:

Corollary 1.

$$S_1^{(m)} \equiv C_k(m) \pmod n ,$$

where $C_k(m)$ is the Ramanujan sum (cf. [3], § 16.6) defined by

$$C_k(m) = \sum_{\substack{1 \leq h \leq k \\ (h,k) = 1}} exp\left(\frac{2\pi i h m}{k}\right). \tag{7}$$

Proof: This follows by taking $r = 1$ in the above theorem, since $T_1^{(m)} = C_k(m)$, the sum of the m-th powers of the primitive k-th roots of unity.

Corollary 2.

$$S_2^{(m)} \equiv \frac{1}{2} \{C_k^2(m) - C_k(2m)\} \pmod n .$$

Proof: This follows by taking $r = 2$ in the above theorem, since

$$T_2^{(m)} = \sum_{\substack{1 \leq h_1, h_2 \leq k \\ h_1 \neq h_2 \\ (h_1, k) = (h_2, k) = 1}} \zeta^{h_1 m} \cdot \zeta^{h_2 m}$$

$$= \frac{1}{2} \left\{ \left(\sum_{\substack{1 \leq h \leq k \\ (h,k) = 1}} \zeta^{hm} \right)^2 - \sum_{\substack{1 \leq h \leq k \\ (h,k) = 1}} \zeta^{2hm} \right\}$$

$$= \frac{1}{2} \{C_k^2(m) - C_k(2m)\}, \quad \text{by (7)} .$$

Remark 1. It is known (cf. [3], Theorems 271 and 272) that

$$C_k(m) = \sum_{\substack{d \mid k \\ d \mid m}} d\, \mu \left(\frac{k}{d}\right) \tag{8}$$

and also

$$C_k(m) = \frac{\mu(k/a)\, \varphi(k)}{\varphi(k/a)}, \quad \text{where } a = (k, m) . \tag{9}$$

Hence from Corollary 1, we have

$$S_1^{(m)} \equiv \frac{\mu(k/a)\, \varphi(k)}{\varphi(k/a)} \pmod{n} . \tag{10}$$

As a particular case of (10), by taking $n = p$, an odd prime, we have the following result due to A. Czarnota [2]:

$$S_1^{(m)} \equiv \frac{\mu((p-1)/b)\, \varphi(p-1)}{\varphi((p-1)/b)} \pmod{p}, \text{ where } \quad b = (p-1, m) . \tag{11}$$

If S denotes the sum of the primitive roots of n which are less than n, then we have by Corollary 1 (taking $m = 1$),

$$S \equiv \mu(\varphi(n)) \pmod{n} , \tag{12}$$

since $C_k(1) = \mu(k)$, in virtue of (8). A particular case of result (12) in case $n = p$ (an odd prime) appears as problem 79 on page 129 of T. Nagell's book [4].

Remark 2. If S_2 denotes the sum of the primitive roots of n, which are less than n, taken 2 at a time, then we have by corollary 2 (taking $m = 1$),

$$S_2 \equiv \frac{1}{2} \left\{\mu^2(k) - \mu(k) - 2\mu\left(\frac{k}{2}\right)\right\} \pmod{n} , \tag{13}$$

since $C_k(1) = \mu(k)$ and $C_k(2) = \mu(k) + 2\,\mu(k/2)$ in virtue of (8).

As a particular case of (13), when $n = p$, an odd prime, we have

$$S_2 \equiv \left\{\frac{1}{2}\, \mu(p-1) \left(\mu(p-1) - 1\right) - 2\mu\left(\frac{p-1}{2}\right)\right\} \pmod{p} . \tag{14}$$

Remark 3. From (2) and the notation for $T_r^{(m)}$, we see that the m-th powers of the primitive k-th roots of unity are precisely the roots of the equation

$$x^{\varphi(k)} - T_1^{(m)} x^{\varphi(k)-1} + T_2^{(m)} x^{\varphi(k)-2} - \cdots + (-1)^{\varphi(k)} T_{\varphi(k)}^{(m)} = 0 .$$

Hence by Newton's theorem on sums of powers of the roots of an algebraic equation (cf. [1], p. 297), we have

$$s_r - T_1^{(m)} s_{r-1} + T_2^{(m)} s_{r-2} - \cdots + (-1)^{r-1} T_{r-1}^{(m)} s_1 + (-1)^r r\, T_r^{(m)} = 0 , \tag{15}$$

for $r = 1, 2, 3, \ldots \varphi(k)$; where

$$s_r = \sum_{\substack{1 \le h \le k \\ (h,k)=1}} \zeta^{hmr} .$$

But by (7), s_r turns out to be $C_k(mr)$, so that (15) turns out to be

$$\left.\begin{aligned} &C_k(mr) - T_1^{(m)} C_k(mr-m) + T_2^{(m)} C_k(mr-2m) - \cdots \\ &\qquad + (-1)^{r-1} T_{r-1}^{(m)} C_k(m) + (-1)^r r T_r^{(m)} = 0 , \end{aligned}\right\} \quad (16($$

for $r = 1, 2, 3, \ldots \varphi(k)$.

Using (16), we can express $T_1^{(m)}, T_2^{(m)}, \ldots T_{\varphi(k)}^{(m)}$ successively in terms of $C_k(m)$, $C_k(2m), \ldots C_k(\varphi(k)m)$. In particular, when $m = 1$, we can express the values of the elementary symmetric functions of the primitive k-th roots of unity in terms of the values of the Möbius μ-function. This is exactly what we have done in establishing the congruences (12) and (13).

D. Suryanarayana, Andhra University, Waltair, India

REFERENCES

[1] S. Barnard and J. M. Child, *Higher Algebra* (Macmillan and Company, Limited, London, 1949).

[2] A. Czarnota, *Congruences Satisfied by a Sum of Powers of Primitive Roots with Respect to a Prime Modulus* (Polish, Russian and English summaries), Prace. Mat. *8*, 131–142 (1963/64), M.R. 30, 1964.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Fourth edition (Clarendon Press, Oxford, 1960).

[4] T. Nagell, *Introduction to Number Theory* (John Wiley & Sons, Inc., New York, 1951).

Aufgaben

Aufgabe 729. If A, B, C denote the angles of an arbitrary triangle, then it is known (cf., e.g., O. Bottema et al., Geometric Inequalities, Groningen 1968, p. 120) that the three triples $(\sin A, \sin B, \sin C)$, $(\cos A/2, \cos B/2, \cos C/2)$, $(\cos^2 A/2, \cos^2 B/2, \cos^2 C/2)$ are sides of three triangles. Give a generalization which includes the latter three cases as special cases.

M. S. Klamkin, Dearborn, Michigan, USA

Erste Lösung: Ist M ein Punkt der Ebene des Dreiecks, so gilt nach der ptolemäischen Ungleichung für die Eckpunkte Q, R, S:

$$\overline{MQ} \cdot \overline{RS} \le \overline{MR} \cdot \overline{SQ} + \overline{MS} \cdot \overline{QR} \tag{1}$$

sowie die durch zyklische Vertauschung von Q, R, S entstehenden Ungleichungen. Das Tripel $(\overline{MQ} \cdot \overline{RS}, \overline{MR} \cdot \overline{SQ}, \overline{MS} \cdot \overline{QR})$ stellt also die Seitenlängen eines Drei-