ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria I: PRACE MATEMATYCZNE VIII (1964)

A. CZARNOTA (Częstochowa)

Kongruencje spełniane przez sumy potęg pierwiastków pierwotnych względem modułu pierwszego

Zbiór N liczb naturalnych, mniejszych od liczby pierwszej p, możemy podzielić na dwa podzbiory. Pierwszy, to zbiór R pierwiastków pierwotnych względem modułu pierwszego p, liczący $\varphi(p-1)$ różnych elementów, gdzie $\varphi(n)$ oznacza funkcję Eulera. Drugi zbiór S składa się z pozostałych liczb, nie będących pierwiastkami pierwotnymi.

W pracy rozważane są zbiory R^m, złożone z m-tych potęg elementów zbioru R. Podstawowe twierdzenie pracy (twierdzenie 11) wyznacza pewną funkcję argumentów p i m, do której są przystające względem modułu p sumy $\bar{R}^m$ elementów zbioru R^m.

Nie znamy do tej pory ogólnej metody [1] wyznaczania jednego choćby elementu zbioru R, ale jeśli znamy jeden jego element r, możemy łatwo określić pozostałe elementy. Rozpatrujemy wtedy wzór

$$R' = \{r^{i_1}, r^{i_2}, \ldots, r^{i_x}\},$$

gdzie $x = \varphi(p-1)$, a wykładnikami potęgowymi są wszystkie różne od siebie liczby, pierwsze względem $p-1$, mniejsze od p.

Jeśli w zbiorze R' zastąpimy poszczególne elementy przez reszty, jakie te elementy dają względem modułu p, to otrzymamy zbiór R.

Podobnie możemy rozważyć zbiór

$$S' = \{r^{k_1}, r^{k_2}, \ldots, r^{k_y}\},$$

gdzie $y = (p-1)-\varphi(p-1)$, a zbiorem wykładników potęgowych są wszystkie różne od siebie liczby, mniejsze od p, nie pierwsze względem $p-1$.

Jeśli w zbiorze tym poszczególne elementy zastąpimy przez reszty, jakie te elementy dają względem modułu p, to otrzymamy zbiór S.

---

[1] Podana przez J. Winogradowa ([2], str. 102) metoda wyznaczania pierwiastków pierwotnych nie może być uważana za taką, gdyż wyznacza ona pierwiastki pierwotne drogą sprawdzania rachunkowego, redukując tylko ilość prób.

Analogicznie jak zdefiniowaliśmy R^m, określamy S^m jako zbiór m-tych potęg elementów zbioru S. Określamy dalej zbiory

$$(R^m)' = \{r^{mi_1}, r^{mi_2}, \ldots, r^{mi_x}\},$$
$$(S^m)' = \{r^{mk_1}, r^{mk_2}, \ldots, r^{mk_y}\}.$$

Oznaczmy sumy wszystkich liczb, należących do zbiorów R, S, R^m, S^m, R', S', $(R^m)'$, $(S^m)'$, odpowiednio przez $\bar{R}$, $\bar{S}$, $\bar{R}^m$, $\bar{S}^m$, $\bar{R}'$, $\bar{S}'$, $(\bar{R}^m)'$, $(\bar{S}^m)'$.

Z definicji zbiorów wynikają dla $m \geqslant 1$ kongruencje

$$\bar{R}^m \equiv (\bar{R}^m)' \pmod{p}, \qquad \bar{S}^m \equiv (\bar{S}^m)' \pmod{p}. \tag{1}$$

Pozwolą nam one zastąpić w rozumowaniach $\bar{R}$, $\bar{S}$, $\bar{R}^m$, $\bar{S}^m$ odpowiednio przez sumy $\bar{R}'$, $\bar{S}'$, $(\bar{R}^m)'$, $(\bar{S}^m)'$, które wiążą się ze znajomością rozkładu liczby $p-1$ na czynniki pierwsze.

TWIERDZENIE 1. *Dla dowolnego $m \geqslant 1$, takiego że $p-1 \nmid m$, zachodzi kongruencja*

$$\bar{S}^m + \bar{R}^m \equiv 0 \pmod{p}. \tag{2}$$

Dowód. Z rozwinięcia $(x+1)^m$ na sumę newtonowską i z sumowania stronami tożsamości dla $x = 1, 2, \ldots, p-1$, otrzymujemy związek, który możemy przekształcić na kongruencję o charakterze rekurencyjnym

$$\sum_{i=1}^{m-1} \binom{m}{i} (\bar{S}^{m-i} + \bar{R}^{m-i}) \equiv 0 \pmod{p}. \tag{3}$$

Wykorzystując związek: $\bar{S} + \bar{R} = \binom{p}{2} \equiv 0 \pmod{p}$, otrzymujemy z (3) kongruencję (2). Ze względu na (1) mamy także

$$(\bar{R}^m)' \equiv -(\bar{S}^m)' \pmod{p}. \tag{4}$$

Rozpatrywane w pracy moduły pierwsze można przedstawić w postaci

$$p = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s} + 1,$$

gdzie p_i, dla $i = 1, 2, \ldots, s$, oznaczają różne liczby pierwsze, większe od jedności, a_i zaś dowolne wykładniki naturalne.

Tym samym każdy moduł p wyznacza zbiór liczb pierwszych $Z = \{p_1, p_2, \ldots, p_s\}$. Iloczyn tych liczb oznaczamy symbolem $\psi(p-1) = p_1 p_2 \ldots p_s$. Ogólniej, przez funkcję $\psi(n)$ będziemy rozumieli iloczyn wszystkich podzielników liczby n, będących liczbami pierwszymi.

Oznaczmy dalej przez Z_t zbiór, zawierający wszystkie możliwe iloczyny $w_i = z_1 z_2 \ldots z_t$ elementów zbioru Z, gdzie $t \leqslant s$ i gdzie żaden czynnik z_j w iloczynie nie może się powtarzać.

Elementy zbioru Z_t można uporządkować w jakikolwiek sposób, nadając im kolejne numery od 1 do $\binom{s}{t}$.

Jeżeli i oznacza numer elementu zbioru Z_t, to przez Z_t^i będziemy rozumieli zbiór czynników pierwszych tego elementu.

Punktem wyjściowym dla dalszych rozważań jest suma podwójna

$$\bar{C}_t = \sum_{i=1}^{\binom{s}{t}} \sum_{h=1}^{\frac{p-1}{w_i}} h w_i,$$

gdzie $w_i \in Z_t$. Pewne składniki tej sumy są sobie równe. Utwórzmy zbiór A_t wszystkich różnych od siebie składników sumy $\bar{C}_t$. Praktycznie oznacza to, że z sumy $\bar{C}_t$ odrzucamy te składniki, w których, dla określonego $w_i \in Z_t$, h będzie krotnością jakiegokolwiek elementu zbioru $Z - Z_t^i$.

Przez B_t oznaczmy zbiór liczb postaci r^{ma}, gdzie $a \in A_t$, a m jest stałą liczbą całkowitą. Wyprowadzamy dalej sumy

$$\bar{A}_t = \sum_{n \in A_t} n, \qquad \bar{B}_t = \sum_{n \in B_t} n, \qquad \bar{D}_t = \sum_{\substack{i=1 \\ w_i \in Z_t}}^{\binom{s}{t}} \sum_{h=1}^{\frac{p-1}{w_i}} r^{mhw_i},$$

$$\bar{A} = \sum_{t=1}^{s} \bar{A}_t, \qquad \bar{B} = \sum_{t=1}^{s} \bar{B}_t.$$

Z definicji zbiorów wynika, że jeśli $t \neq t'$, to $A_t \cap A_{t'} = 0$ oraz $B_t \cap B_{t'} = 0$. Zbiór $A = \sum_{t=1}^{s} A_t$ jest identyczny ze zbiorem liczb mniejszych od p i nie pierwszych względem $p-1$. Tym samym zbiór $B = \sum_{t=1}^{s} B_t$ będzie identyczny ze zbiorem $(S^m)'$. Oznacza to, że

$$\bar{B} = (\bar{S}^m)'. \tag{5}$$

TWIERDZENIE 2. *Jeżeli* $n \leqslant t$, *to każda liczba zbioru* A_t *występuje* $\binom{t}{n}$ *razy wśród składników sumy* $\bar{C}_n$.

Dowód. Każdemu określonemu iloczynowi w_i, będącemu czynnikiem elementu zbioru A_t, można przeciwstawić $\binom{t}{n}$ składników sumy $\bar{C}_n$, podzielnych przez w_i.

Wnioskiem z powyższego twierdzenia jest oczywiście stwierdzenie, że każda liczba, należąca do zbioru A_t jest równa jednemu tylko składnikowi sumy $\bar{C}_t$.

TWIERDZENIE 3. *Jeżeli* $n > t$, *to żadna liczba, należąca do zbioru* A_t *nie jest składnikiem sumy* $\bar{C}_n$.

Dowód. Gdyby było inaczej, h musiałoby mieć podzielniki ze zbioru $Z - Z_t^i$.

TWIERDZENIE 4. *Zachodzą związki*:

$$\bar{A} = \sum_{t=1}^{s} (-1)^{t+1} \bar{C}_t, \tag{6}$$

$$\bar{B} = \sum_{t=1}^{s} (-1)^{t+1} \bar{D}_t. \tag{7}$$

Dowód. Każdy element należący do zbioru A jest określony jednoznacznie w zbiorze A_t. Poszczególny element występuje w sumie określonej wzorem (6) $\binom{t}{1} - \binom{t}{2} + \binom{t}{3} - \ldots + (-1)^t \binom{t}{t} = 1$ razy. Ponieważ w sumach $\bar{C}_t$ nie ma takich elementów, któreby nie znajdowały się w zbiorze A, zatem obie strony równania (6) muszą być identyczne.

Dowód związku (7) jest analogiczny.

WNIOSEK. *Ze względu na zależności* (4), (5) i (7), *mamy dla* $m \geqslant 1$, *takiego że* $p-1 \nmid m$, *kongruencję*

$$\bar{R}^m \equiv \sum_{t=1}^{s} (-1)^t \bar{D}_t \pmod{p}. \tag{8}$$

Oznaczmy teraz przez $F(\bar{C}_t)$ ilość składników sumy $\bar{C}_t$, które spełniają warunek

$$p-1 \mid m w_i. \tag{9}$$

Przyjmijmy dalej, że liczba m ma następujący rozkład na czynniki

$$m = l p_{i_1}^{b_{i_1}} p_{i_2}^{b_{i_2}} \ldots p_{i_r}^{b_{i_r}},$$

gdzie p_{i_k} należą do zbioru Z, $r \leqslant s$, $(l, p-1) = 1$. Określimy zbiór podzielników pierwszych m, które jednocześnie są podzielnikami $p-1$, przez

$$M = \{p_{i_1}, p_{i_2}, \ldots, p_{i_r}\}.$$

Oznaczmy przez $\mu(n)$ funkcję Möbiusa(2).

TWIERDZENIE 5. *Jeżeli* $\mu\left[\dfrac{p-1}{(p-1, m)}\right] = 0$, *to* $\sum_{t=1}^{s} F(\bar{C}_t) = 0$.

Dowód. Zauważymy, że $F(\bar{C}_t) = 0$, gdy zajdzie jeden z dwóch przypadków:

1. Jeżeli wykładniki, z którymi p_{i_k}, należące do zbioru M, występują w rozkładach na czynniki $p-1$ i m, spełniają nierówność $a_{i_k} > b_{i_k}+1$ choćby dla jednego czynnika.

---

(2) Funkcja Möbiusa przyjmuje wartość zero dla dowolnej liczby, podzielnej przez kwadrat większy od jedności oraz $(-1)^s$ dla liczby, która jest iloczynem s różnych liczb pierwszych ([1], str. 136).

2. Jeśli choć jedna liczba pierwsza, należąca do zbioru $Z-M$, występuje w rozkładzie $p-1$ w potędze $a_{i_k} > 1$.

Łatwo stwierdzić, że są to jedyne przypadki, w których dla żadnego składnika sumy $\bar{C}_t$ nie może być zachowany warunek (9).

TWIERDZENIE 6. *Jeśli* $\mu\left[\frac{p-1}{(p-1, m)}\right] \neq 0$, *to liczba* $\overline{w}_{t_0} = \frac{p-1}{(p-1, m)}$ *jest najmniejszą spośród wszystkich wartości* w_i, *dla których* $F(\bar{C}_t) \neq 0$.

Dowód. Zgodnie z założeniem, $\overline{w}_{t_0}$ składa się tylko z czynników w potędze pierwszej. Spełniony jest także warunek (9). Brak jakiegokolwiek z czynników występujących w $\overline{w}_{t_0}$ nie pozwalałby spełniać powyższego warunku.

Wskaźnik t_0 spełnia związek

$$(-1)^{t_0} = \mu\left[\frac{p-1}{(p-1, m)}\right]. \tag{10}$$

Dla $t < t_0$ mamy $F(\bar{C}_t) = 0$. Liczba $\overline{w}_{t_0}$ jest zatem najmniejszą z możliwych wartości w_i. Zbiór czynników

$$N = \{p_{k_1}, p_{k_2}, \ldots, p_{k_{t_0}}\}$$

jest jednoznacznie określony przez $\overline{w}_{t_0}$.

Każde w_i dla $t > t_0$, spełniające (9), musi zawierać czynnik $\overline{w}_{t_0}$, a pozostałe czynniki należą do zbioru $Z-N$. Elementy zbioru $Z-N$ tworzą czynniki pierwsze liczby

$$g = \frac{\varphi(p-1)}{\left[\frac{p-1}{(p-1, m)}\right]},$$

co jest równoważne związkowi

$$\overline{w}_{t_0} g = \varphi(p-1). \tag{11}$$

TWIERDZENIE 7. *Dla sum* $\bar{C}_t$, *gdzie* $t \geqslant t_0$, *zachodzi wzór*

$$F(\bar{C}_t) = \frac{p-1}{\varphi(p-1)} T_{s-t}, \tag{12}$$

przy czym $T_n = \sum p_{k_1} p_{k_2} \ldots p_{k_n}$, *a suma rozciąga się na wszystkie możliwe układy* $p_{k_i} \in Z-N$. *Dla* $s = t$ *przyjmujemy dodatkową definicję* $T_0 = 1$.

Dla $s = t$ suma $\bar{C}_t$ ma $\frac{p-1}{\varphi(p-1)}$ składników, przy czym każdy z nich spełnia warunek (9). Oznacza to, że

$$F(\bar{C}_t) = \frac{p-1}{\varphi(p-1)},$$

czyli że wzór (12) jest słuszny dla $t = s$.

Uzasadnienie wzoru (12) dla $t<s$ oprzemy na związku $F(\bar{C}_t)=\sum\frac{p-1}{w_i}$, gdzie symbol sumy rozciąga się na wszystkie możliwe wartości mianownika, spełniające warunek (9).

Zgodnie z końcową uwagą w twierdzeniu 6, w każdym iloczynie w_i występować musi czynnik $\overline{w}_{t_0}$ oraz $t-t_0$ elementów zbioru $Z-N$. Zatem

$$F(\bar{C}_t)=\frac{p-1}{g}\sum\frac{g}{\overline{w}_{t_0}p_{k_1}\dots p_{k_{t-t_0}}}. \tag{13}$$

Wprowadzamy jeszcze oznaczenie

$$L_n=\sum_{p_{k_i}\in Z-N}\frac{1}{p_{k_1}\dots p_{k_n}}.$$

Łatwo dostrzec związek

$$\sum_{p_{k_i}\in Z-N}\frac{g}{p_{k_i}\dots p_{k_n}}=\sum_{p_{r_i}\in Z-N}p_{r_1}\dots p_{r_{s-t_0-n}},$$

odpowiadający zapisowi $gL_n=T_{s-t_0-n}$. Wzór (13) przekształca się zatem w następujący

$$F(\bar{C}_t)=\frac{p-1}{g\overline{w}_{t_0}}T_{s-t},$$

który, wobec (11), daje (12).

TWIERDZENIE 8. *Jeśli* $\mu\left[\frac{p-1}{(p-1,m)}\right]\neq 0$, *to*

$$\sum_{t=1}^{s}(-1)^tF(\bar{C}_t)=\mu\left[\frac{p-1}{(p-1,m)}\right]\frac{\varphi(p-1)}{\varphi\left[\frac{p-1}{(m,p-1)}\right]}. \tag{14}$$

Zgodnie z wzorem (12) mamy

$$w=\sum_{t=1}^{s}(-1)^tF(\bar{C}_t)=\sum_{t=1}^{s}(-1)^t\frac{p-1}{\psi(p-1)}T_{s-t}.$$

Ponieważ $F(\bar{C}_t)=0$, dla $t<t_0$ otrzymujemy

$$w=\frac{p-1}{\psi(p-1)}\sum_{t=t_0}^{s}(-1)^tT_{s-t},$$

$$w=\frac{p-1}{\psi(p-1)}(-1)^s(1-p_{k_1})(1-p_{k_2})\dots(1-p_{k_{s-t_0}}),$$

$$w=(-1)^{t_0}\frac{p-1}{\psi(p-1)}\varphi\left[\frac{\psi(p-1)}{\frac{p-1}{(p-1,m)}}\right].$$

Wzór ten przekształcamy, opierając się na następujących własnościach funkcji Eulera $\varphi(n)$:

I. Jeżeli $b \mid a$, $a = \psi(a)$, $b = \psi(b)$, to $\varphi\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)}$.

II. $\varphi(a) = \frac{a}{\psi(a)}\varphi[\psi(a)]$.

Otrzymujemy zatem

$$w = (-1)^{t_0}\frac{\varphi(p-1)}{\varphi[\psi(p-1)]}\cdot\frac{\varphi[\psi(p-1)]}{\varphi\left[\frac{p-1}{(p-1,m)}\right]}.$$

Po redukcji, wykorzystując jeszcze (10) otrzymujemy (14). Uwzględniając twierdzenie 5 możemy uogólnić wzór (14) w sposób następujący:

TWIERDZENIE 9. *Dla dowolnych p, m, zachodzi związek*

$$\sum_{t=1}^{s}(-1)^t F(\bar{C}_t) = \mu\left[\frac{p-1}{(p-1,m)}\right]\frac{\varphi(p-1)}{\varphi\left[\frac{p-1}{(p-1,m)}\right]}. \tag{15}$$

TWIERDZENIE 10. *Zachodzi związek*

$$\bar{D}_t \equiv F(\bar{C}_t) \pmod{p}. \tag{16}$$

Dowód. Jeżeli poszczególny składnik sumy $\bar{C}_t$ spełnia warunek (9), to odpowiadający mu składnik sumy $\bar{D}_t$ jest przystający do 1 względem modułu p. Jeżeli składnik sumy $\bar{C}_t$ nie spełnia warunku (9), to dla danego w_i można utworzyć szereg geometryczny składników sumy $\bar{D}_t$, którego suma jest przystająca do zera względem modułu p.

$$\sum_{k=1}^{k_t} r^{kmw_i} \equiv r^{mw_i}\frac{r^{(p-1)m}-1}{r^{mw_i}-1} \equiv 0 \pmod{p}, \tag{17}$$

gdzie $k_t = \frac{p-1}{w_i}$.

TWIERDZENIE 11. *Dla dowolnych p i m zachodzi związek*

$$\bar{R}^m \equiv \mu\left[\frac{p-1}{(p-1,m)}\right]\frac{\varphi(p-1)}{\varphi\left[\frac{p-1}{(p-1,m)}\right]} \pmod{p}. \tag{18}$$

Dla m, spełniających warunek $p-1 \nmid m$, twierdzenie powyższe jest wnioskiem z wyników (8), (15) i (16).

Trzeba rozważyć zatem tylko przypadek, gdy $p-1 \mid m$, a więc gdy nie zachodzi ani wzór (2), ani (4). Ale dla tego przypadku, z definicji

pierwiastków pierwotnych, mamy

$$\bar{R}^{k(p-1)} \equiv \varphi(p-1) \pmod{p}.$$

Wzór (18) daje nam ten sam rezultat, a więc obejmuje także przypadek, wyłączony z dotychczasowych rozważań. Twierdzenie 11 stanowi główny wynik pracy.

WNIOSEK 1. *Jeżeli* $(p-1, m) = 1$, *to* $\bar{R}^m \equiv \mu(p-1) \pmod{p}$.

Przykłady:

$p = 11 = 2\cdot 5+1$, $\quad 2+6+7+8 = 23$, $\quad 23 \equiv 1 \pmod{11}$,

$p = 13 = 2^2\cdot 3+1$, $\quad 2+6+7+11 = 26$, $\quad 26 \equiv 0 \pmod{13}$,

$p = 19 = 2\cdot 3^2+1$, $\quad 2+3+10+13+14+15 = 57$, $\quad 57 \equiv 0 \pmod{19}$,

$p = 23 = 2\cdot 11+1$, $\quad 5+7+10+11+14+15+17+19+21 = 139$,
$139 \equiv 1 \pmod{23}$,

$p = 31 = 2\cdot 3\cdot 5+1$, $\quad 3+11+12+13+17+21+22+24 = 123$,
$123 \equiv -1 \pmod{31}$.

Dla $m \neq 1$, spełniającego warunek $(p-1, m) = 1$, sprawdzenie jest niepotrzebne, bo kongruencja $\bar{R}^m \equiv R \pmod{p}$ wynika ze znanych już własności pierwiastków pierwotnych.

WNIOSEK 2. *Jeżeli* $\mu\left[\dfrac{p-1}{(p-1, m)}\right] = 0$, to $\bar{R}^m \equiv 0 \pmod{p}$.

Przykłady:

$p = 17 = 2^4+1$, $\quad 3+5+6+7+10+12+14 = 68$, $\quad 68 \equiv 0 \pmod{17}$

$$\bar{R}^2 = 3^2+5^2+6^2+7^2+10^2+12^2+14^2,$$

$$\bar{R}^2 \equiv 9+8+2+15+15+2+8+9 \equiv 68 \equiv 0 \pmod{17},$$

$$\bar{R}^4 \equiv 13+13+4+4+4+4+13+13 \equiv 68 \equiv 0 \pmod{17}.$$

WNIOSEK 3. *Jeżeli* $\mu\left[\dfrac{p-1}{(p-1, m)}\right] \neq 0$, $m = 2^n$, $p-1 = 2^k l$, *gdzie* $2 \nmid l$, *to*

$$\bar{R}^m \equiv \mu\left[\frac{p-1}{2^{\min(k,n)}}\right] 2^{k-1} \pmod{p}. \tag{19}$$

Wyrażenie $\dfrac{p-1}{(p-1, m)}$ przyjmuje wartości $y = 2l$ dla $k = n+1$ oraz $y = l$ dla $k \leqslant n$. W obydwu przypadkach jest $\varphi(y) = \varphi(l)$. Mamy poza tym $\varphi(p-1) = 2^{k-1}\varphi(l)$. Po dokonaniu odpowiednich podstawień do (18) otrzymujemy (19).

Przykłady:

$$\bar{R}^8 \equiv 16+16+16+16+16+16+16+16 \equiv -8 \pmod{17},$$

$$\bar{R}^{16} \equiv +8 \pmod{17}, \quad \bar{R}^{32} \equiv \bar{R}^{16} \pmod{17}.$$

WNIOSEK 4. *Jeśli* $m = \frac{p-1}{2}$, *to wzór* (18) *daje nam* $\bar{R}^m \equiv -\varphi(p-1) \pmod{p}$.

Wniosek ten wynika również z definicji pierwiastków pierwotnych i twierdzenia Fermata.

WNIOSEK 5. *Jeśli* $m = \frac{p-1}{r}$, *gdzie* $r \mid p-1$, *wzór* (18) *daje nam*

$$\bar{R}^m \equiv \mu(r)\frac{\varphi(p-1)}{\varphi(r)} \pmod{p}.$$

WNIOSEK 6. *Jeśli w poprzednim wzorze założymy dodatkowo, że* $\left(\frac{p-1}{r}, r\right) = 1$, *to otrzymujemy*

$$\bar{R}^m \equiv \mu\left(\frac{p-1}{m}\right)\varphi(m) \pmod{p}.$$

W szczególności, jeśli $m = 2$ i $\left(\frac{p-1}{2}, 2\right) = 1$, to $\bar{R}^2 \equiv \mu\left(\frac{p-1}{2}\right) \pmod{p}$.

TWIERDZENIE 12. *Jeżeli przez* R^{-m} *oznaczymy wzór odwrotności elementów zbioru* R^m, *a przez* $\bar{R}^{-m}$ *sumę elementów tego zbioru, to*

$$\bar{R}^{-m} \equiv \bar{R}^m \pmod{p}. \tag{20}$$

Dowód. Kongruencja $\bar{R}^{-1} \equiv \bar{R}^{p-2} \pmod{p}$ wynika z tego, że zbiory R^{-1} i R^{p-2}, składają się z tych samych reszt względem modułu p. Wobec tego, że $\bar{R}^{p-2} \equiv \bar{R} \pmod{p}$, mamy także $\bar{R}^{-1} \equiv \bar{R} \pmod{p}$. Jeżeli w zbiorach R^{-1} i R każdy element podniesiemy do potęgi m, to otrzymamy również sumy (20) przystające do modułu p.

Prace cytowane

[1] W. Sierpiński, *Teoria liczb I*, Warszawa 1950.
[2] J. Winogradow, *Elementy teorii liczb*, Warszawa 1954.

А. ЧАРНОТА (Ченстохова)

КОНГРУЭНЦИИ ИСПОЛНЯЕМЫЕ ПОСРЕДСТВОМ СУММЫ СТЕПЕНЕЙ ПЕРВИЧНЫХ КОРНЕЙ ОТНОСИТЕЛЬНО ПРОСТОГО МОДУЛЯ

РЕЗЮМЕ

Дано простое число p в виде $p = p_1^{a_1}p_2^{a_2}\ldots p_s^{a_s}+1$, где p_i обозначает тоже простые числа. Вводим следующие обозначения определяющие множества: $Z = \{p_j\colon 1 \leqslant j \leqslant s\}$ и $Z_t = \{z_1 z_2 \ldots z_t\colon z_j \in Z,\ i \neq j \supset z_i \neq z_j\}$, где $t \leqslant s$.

Образуем суммы:

$$\bar{C}_t = \sum_{w \in Z_1} \sum_{h=1}^{\frac{p-1}{w}} hw, \qquad \bar{D}_t = \sum_{w \in Z_t} \sum_{h=1}^{\frac{p-1}{w}} r^{mhw} \quad \text{и} \quad \bar{R}_p^m = \sum_{r \in R_p} r^m,$$

где m обозначает определенное постоянное целое число, R_p — множество всех первичных корней по отношению к p, меньших от p, r — произвольный но определенный элемент R_p.

Обозначая через A_t множество всех слагаемых суммы $\bar{C}_t$, отличающихся друг от друга, вводим дополнительно следующие обозначения:

$$A = \sum_{t=1}^{s} A_t, \qquad \bar{A}_t = \sum_{n \in A_t} n, \qquad \bar{A} = \sum_{t=1}^{s} \bar{A}_t,$$

$$B_t = \{r^{ma} : a \in A_t\}, \qquad B = \sum_{t=1}^{s} B_t, \qquad \bar{B}_t = \sum_{n \in B_t} n, \qquad \bar{B} = \sum_{t=1}^{s} B_t.$$

После сравнения определений вытекает, что A и $\{x : x < p, (x, p-1) > 1\}$ — одинаковые.

Теорема 1.

$$\bar{A} = \sum_{t=1}^{s} (-1)^{t+1} \bar{C}_t, \qquad \bar{B} = \sum_{t=1}^{s} (-1)^{t+1} \bar{D}_t.$$

Теорема 2.

$$\bar{R}_p^m \equiv \sum_{t=1}^{s} (-1)^t \bar{D}_t \pmod{p} \qquad \text{для} \qquad p-1 \nmid m.$$

Теорема 3. *Если*

$$\mu\left[\frac{p-1}{(p-1, m)}\right] = 0, \qquad \text{то} \qquad \sum_{t=1}^{s} F(\bar{C}_t) = 0,$$

где $\mu(u)$ обозначает функцию Мобиуза, $F(\bar{C}_t)$ — число слагаемых суммы $\bar{C}_t$ таких, что $p-1 | mw$.

Теорема 4. *Если*

$$\mu\left[\frac{p-1}{(p-1, m)}\right] \neq 0, \qquad \text{то} \qquad \sum_{t=1}^{s} (-1)^t F(\bar{C}_t) = \mu\left[\frac{p-1}{(p-1, m)}\right] \frac{\varphi(p-1)}{\varphi\left[\frac{p-1}{(p-1, m)}\right]},$$

где $\varphi(n)$ обозначает функцию Эулера.

Теорема 5.

$$\bar{D}_t \equiv F(\bar{C}_t) \pmod{p}.$$

Теорема 6 (основный результат).

$$\bar{R}_p^m \equiv \mu\left[\frac{p-1}{(p-1, m)}\right] \frac{\varphi(p-1)}{\varphi\left[\frac{p-1}{(p-1, m)}\right]} \pmod{p}.$$

A. CZARNOTA (Częstochowa)

CONGRUENCES SATISFIED BY SUMS OF POWERS OF ROOTS PRIMITIVE WITH RESPECT TO A PRIMARY MODULE

SUMMARY

Given a prime number p of the form $p = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s} + 1$, where p_i are distinct primes, let us introduce the following symbols: Let $Z = \{p_j\colon 1 \leqslant j \leqslant s\}$ and $Z_t = \{z_1 z_2 \dots z_t\colon z_j \in Z;\ i \neq j \supset z_i \neq z_j\}$ where $t \leqslant s$.

Let us consider sums

$$\bar{C}_t = \sum_{w \in Z_t} \sum_{h=1}^{\frac{p-1}{w}} hw, \qquad \bar{D}_t = \sum_{w \in Z_t} \sum_{h=1}^{\frac{p-1}{w}} r^{mhw} \quad \text{and} \quad \bar{R}_p^m = \sum_{r \in R_p} r^m,$$

where m denotes a fixed integer, R_p is the set of all roots primitive with respect to p and smaller than p. Denoting by A_t the collection of all the components of the sum $\bar{C}_t$, different of each other, we introduce further definitions

$$A = \sum_{t=1}^{s} A_t, \qquad \bar{A}_t = \sum_{n \in A_t} n, \qquad \bar{A} = \sum_{s=1}^{s} \bar{A}_t,$$

$$B_t = \{r^{ma}\colon a \in A_t\}, \qquad B = \sum_{t=1}^{s} B_t, \qquad \bar{B}_t = \sum_{n \in B_t} n, \qquad \bar{B} = \sum_{t=1}^{s} \bar{B}_t.$$

By comparison of the definitions we conclude that the sets A and $\{x\colon x < p, (x, p-1) > 1\}$ are identical.

THEOREM 1.

$$\bar{A} = \sum_{t=1}^{s} (-1)^{t+1} \bar{C}_t, \qquad \bar{B} = \sum_{t=1}^{s} (-1)^{t+1} \bar{D}_t.$$

THEOREM 2.

$$\bar{R}_p^m \equiv \sum_{t=1}^{s} (-1)^t \bar{D}_t \pmod{p} \quad \textit{for} \quad p-1 \nmid m.$$

THEOREM 3. *If*

$$\mu\left[\frac{p-1}{(p-1, m)}\right] = 0, \quad \textit{then} \quad \sum_{t=1}^{s} F(\bar{C}_t) = 0,$$

where $\mu(n)$ denotes the Möbius function, $F(\bar{C}_t)$ the number of components of sum $\bar{C}_t$, such that $p-1 \mid mw$.

THEOREM 4. *If*

$$\mu\left[\frac{p-1}{(p-1, m)}\right] \neq 0, \quad \textit{then} \quad \sum_{t=1}^{s} (-1)^t F(\bar{C}_t) = \mu\left[\frac{p-1}{(p-1, m)}\right] \frac{\varphi(p-1)}{\varphi\left[\frac{p-1}{(p-1, m)}\right]},$$

where $\varphi(n)$ denotes the Euler function.

THEOREM 5.

$$\bar{D}_t \equiv F(\bar{C}_t) \pmod{p}.$$

THEOREM 6 (main result).

$$\bar{R}_p^m \equiv \mu\left[\frac{p-1}{(p-1,\,m)}\right] \frac{\varphi(p-1)}{\varphi\left[\dfrac{p-1}{(p-1,\,m)}\right]} \pmod{p}.$$