ARYTMETYKA 2019, Lista nr 3

1. Niech $f(X)$ będzie niestałym wielomianem o całkowitych współczynnikach. Pokazać, że kongruencja $f(x) \equiv 0 \pmod{p}$ ma rozwiązanie dla nieskończenie wielu liczb pierwszych p. Rozwiązać względem poniższego schematu:

a) założyć, że teza zachodzi tylko dla $p_1, ..., p_r$;

b) niech $f(x_1) \equiv 0 \pmod{p_1}, ..., f(x_r) \equiv 0 \pmod{p_r}$;

c) niech $x \equiv x_1 \pmod{p_1}, ..., x \equiv x_r \pmod{p_r}$;

d) dla x j.w. jeśli $f(x) \neq 0$ to zapiszmy $f(x) = cp_1^{a_1} \cdot ... \cdot p_r^{a_r}$ przy pewnym c niepodzielnym przez $p_1, ..., p_r$;

e) wziąć $y = x + tp_1^{a_1+1} \cdot ... \cdot p_r^{a_r+1}$, i pokazać, że niezależnie od t $p_i \mid\mid f(y)$;

f) wywnioskować, że $f(x + tp_1^{a_1+1}, ...) = p_1^{a_1} \cdot ... \cdot p_r^{a_r} H(t)$ dla pewnego niestałego wielomianu $H(t)$ o całkowitych wyrazach, przy czym dla każdego t liczby $H(t)$ oraz $p_1 \cdot ... \cdot p_r$ są względnie pierwsze;

g) biorąc dostatecznie duże t pokazać, że dla pewnej liczby pierwszej $p =\neq p_1, ..., p_r$ liczba $H(t)$ jest podzielna przez p.

2. Ogólniej znaleźć warunek na całkowite k, l, m, n, że dla dowolnych całkowitych x, y zachodzi $(kx + ly, mx + ny) = (x, y)$.

Jeśli ogólna teza za trudna to sprawdzić dla $(k, l, m, n) = (3, 2, 5, 4), (7, 2, 5, 4)$.

3. Wykorzystując zadanie 1 oraz ostatnie zadanie z poprzedniej listy znaleźć do czego $\pmod{p}$ przystaje iloczyn wszystkich p.p. $\pmod{p}$.

4. Niech g jakiś pierwiastek pierwotny $\pmod{p}$. Pamiętając o $\sum_{d|n} \mu(d) = 0$ dla $n > 1$ pokazać, że

$$\sum_{d|p-1} \mu(d)(g^d + g^{2d} + ... + g^{p-1}) \equiv \text{suma pierwiastków pierwotnych modulo } p \pmod{p}.$$

Korzystając z sumy szeregu geometrycznego, pokazać że lewa strona ostatniego wyrażenia przystaje do $\mu(p-1)$.

5. Ile rozwiązań ma kongruencja $6x^3 + 27x^2 + 17x + 20 \equiv 0 \pmod{60}$?

6. Ile rozwiązań ma kongruencja $x^2 \equiv 1 \pmod{64}$? Wywnioskować, że Z_{64}^* nie jest cykliczna.

7. Podać warunek typu kongruencyjnego na p pierwsze, aby $x^2 \equiv 6 \pmod{p}$ miała rozwiązanie.

Zrobić to dwoma sposobami: używając lematu Gaussa, oraz wyliczając odpowiedni symbol Legendre'a.

8. Podobnie j.w. ale dla $2x^2 - 3x + 2 \equiv 0 \pmod{p}$.

9. Niech liczba pierwsza będzie postaci $p = 4k + 1$. Pokazać, że jeśli a jest p.p. $\pmod{p}$ to $-a$ też. Jak to ma się do zad. 4?

10. Niech liczba pierwsza będzie postaci $p = 4k - 1$. Pokazać, że jeśli a jest p.p. $\pmod{p}$ to $-a$ nie jest.

11. Używając istnienia p.p $\pmod{p}$ pokazać tw. Wilsona, czyli $(p-1)! \equiv -1 \pmod{p}$.

12. Pokazać, że $x^4 \equiv -1 \pmod{p}$ ma rozwiązanie wtedy i tylko wtedy gdy $p \equiv 1 \pmod{8}$. Wsk. Zapisać $x = g^k$, gdzie g to p.p. $\pmod{p}$.

13. Pokazać, że jeśli liczba pierwsza p jest postaci $p = 2^n + 1$ to n jest potęgą 2.

Wsk. wykorzystać wzór na $x^n + y^n$.

14. Niech $F_n = 2^{2^n} + 1$. Pokazać, że $F_n \mid 2^{F_n - 1} - 1$. Jeśli F_n jest pierwsza to ostatnia podzielność wynika z małego tw.Fermata. Na podstawie ww. podzielności Fermat uważał że wszystkie F_n są pierwsze.

15.Niech $F_n :=$ będzie pierwsza. Pokazać, że wtedy 3 jest p.p. $\pmod p$. Wsk. Użyć kryterium z wykładu na bycie p.p. Tutaj będzie ono miało tylko jeden warunek, a potem użyć symbol Legendre'a.

16. Pokazać, że $1^k + 2^k + ... + (p-1)^k$ jest podzielna przez p, o ile $p - 1 \nmid k$.

17. Wykorzystując to że 2 jest p.p. $\pmod{29}$ rozwiązać $x^7 \equiv 1 \pmod{29}$ oraz $x^7 \equiv 13 \pmod{29}$.

18. Wykorzystując lemat Gaussa oblicz symbole Legendre'a $(15/61), (13/29)$.

19. Pokazać, że $(a, n) = 1$ implikuje $(n - a, n) = 1$. Wywnioskować

$$\sum_{i=1,(i,n)=1}^{n} i = \frac{1}{2} n\phi(n).$$

20. Oblicz $(245/3391), (210/2609), (920/7219)$.

21.Oblicz symbol Jacobiego $(345/7565431)$.

23 kwietnia 2019

T.Pezda