Problemy do przemyślenia

Spis ma na celu zainspirowanie do samodzielnych badań poprzez sformułowanie kilku elementarnych problemów, które mogą okazać się ciekawe i o których można zapewne powiedzieć wiele ciekawego bez uciekania się do stosowania głębokiej teorii.

1 $n^2 - n$, czyli o permutacjach z małą liczbą punktów stałych

Ustalmy n naturalne. Nieporządkami nazwijmy permutacje, które nie mają punktów stałych, czyli takie σ, że dla każdego x jest $\sigma(x) \neq x$. Czy istnieje podgrupa S_n złożona z samych nieporządków i permutacji identycznościowej ? Tak, wystarczy wziąć pod uwagę wszystkie potęgi ustalonej permutacji cyklicznej, np. σ takiego, że $\sigma(i) = i + 1$ dla i od 1 do (n-1) oraz $\sigma(n) = 1$. Otrzymamy n-elementową podgrupę S_n o szukanej własności i łatwo wykazać, że na większą nie możemy liczyć.

Pytanie 1. *Jak wyglądają n-elementowe podgrupy S_n złożone z nieporządków i identyczności ? W szczególności, ile ich jest?*

Rozważmy teraz takie permutacje, które albo są identycznością, albo mają co najwyżej jeden punkt stały. Nazwijmy je 2-nieporządkami i ogólniej nazwijmy k-nieporządkami takie permutacje, które albo są identycznością, albo mają mniej niż k punktów stałych. Możemy łatwo pokazać, że podgrupa S_n złożona z 2-nieporządków (k-nieporządków) ma nie więcej niż $n^2 - n$ (ogólniej $n(n-1)...(n-k+1)$) elementów. Tutaj jednak zadanie konstrukcji takiej podgrupy maksymalnego rozmiaru nie wydaje się już tak proste.

Pytanie 2. *Dla jakich n istnieje w S_n podgrupa złożona z 2-nieporządków rozmiaru n^2-n ? Jaki jest maksymalny rozmiar takiej podgrupy dla pozostałych n?*

Łatwo pokazać, że n będące potęgami liczb pierwszych spełniają ten warunek, bo istnieje wówczas ciało n elementowe, które pozwala na pewną prostą konstrukcję. Pozostaje jednak wciąż pytanie o to, jak wszystkie takie grupy wyglądają. Zaś w przypadku k-nieporządków dla $k \geqslant 3$ autor opracowania nie wie jeszcze niczego.

Pytanie 3. *Dla jakich n istnieje w S_n podgrupa złożona z k-nieporządków rozmiaru $n(n-1)...(n-k+1)$? Jaki jest maksymalny rozmiar takiej podgrupy dla pozostałych n? Jaka jest struktura takiej podgrupy? Ile ich jest?*

2 $f(f(x))$, czyli o składaniu wielomianu ze sobą

Pytanie 4. *Załóżmy, że mamy dany wielomian $p(x) \in \mathbb{R}[x]$. Jak rozpoznać, czy jest postaci $f(f(x))$ dla pewnego $f \in \mathbb{R}[x]$? Jak znaleźć f? Na ile f jest jednoznacznie wyznaczone ?*

Pytanie można też zadać np. dla wielomianów o współczynnikach całkowitych, bądź zespolonych. Interesujące może być już podanie efektywnego algorytmu, który by badał sformułowaną własność. Z podzielności $f(x) - x | f(f(x)) - x$ widać, że w pewnym sensie $f(x) - x$ można odnaleźć jako dzielnik $f(f(x)) - x$, zaś zróżniczkowanie obustronne $p(x) = f(f(x))$ pozwala otrzymać $f'(x)$ jako dzielnik $p'(x)$, więc być może jest od czego zacząć poszukiwania.

Można też zapytać o złożenie wielomianu ze sobą więcej niż 1 raz, np. o rozwiązanie równania $p(x) = f(f(f(x)))$ z danym p.

Pytanie 5. *Załóżmy, że $p(x) = f(f(f..(x))$ dla pewnej liczby złożeń f. Co możemy powiedzieć, mając dane p, o liczbie złożeń?*

3 Każda funkcja to wielomian

Dla liczby pierwszej p łatwo sprawdzić, że każda funkcja $f : \mathbb{Z}_p \to \mathbb{Z}_p$ daje się zapisać jednoznacznie w postaci funkcji wielomianowej (o współczynnikach $\mathbb{Z}_p$) stopnia co najwyżej $p - 1$ (analogicznie w innych ciałach skończonych).

Pytanie 6. *Jak rozpoznać, czy dany wielomian $\in \mathbb{Z}_p[x]$ stopnia $\leqslant p - 1$ zadaje funkcję różnowartościową/bijekcję?*

Ogólniej, jako funkcje wielomianowe można też zapisać każdą funkcję wielu zmiennych $f : (\mathbb{Z}_p)^n \to \mathbb{Z}_p$, więc postawione wyżej pytanie można uogólnić na wielomiany wielu zmiennych.

Patrzenie na funkcje jako na funkcje wielomianowe prowadzi np. do ciekawej metody rozwiązywania równań funkcyjnych w $\mathbb{Z}_p$ (i innych ciałach skończonych), takich jak $f(x)f(y) = f(xy)$, czy $f(x + y) = f(x) + f(y)$.

4 Wielomiany testujące postać reszty modulo p

Przypomnijmy sobie pewne ciekawe kryterium orzekające, czy dana reszta jest resztą kwadratową:

Twierdzenie 1. *Dla nieparzystej liczby pierwszej p, a jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $p | a^{\frac{p-1}{2}} - 1$.*

Testujemy tutaj, czy reszta a (modulo p) jest postaci $W(b) = b^2$ dla pewnego b i jednocześnie niezerowa. Po uwzględnieniu przypadku zerowego i zapisaniu wielomianu $S_p(x) = x^{\frac{p+1}{2}} - x$ dostajemy kryterium mówiące, że a jest postaci $W(b)$ dla jakiegoś b,

wtedy i tylko wtedy, gdy $S_p(a) = 0$. S_p nazwiemy tutaj wielomianem testującym dla W modulo p.

Ogólniej, niech $W(x)$ będzie pewnym wielomianem o współczynnikach całkowitych. Dla każdej liczby pierwszej p, możemy popatrzeć na jego współczynniki/argumenty/wartości modulo p i uzyskać wielomian o współczynnikach z $\mathbb{Z}_p$ określony jako $T_p(x) = (x - W(0))(x - W(1)) \cdots (x - W(p-1))$. Ów wielomian ma tę prostą własność, że a jest postaci $W(b)$ dla pewnego b (modulo p) wtedy i tylko wtedy, gdy $T_p(a) = 0$ (modulo p). W przypadku $W(x) = x^2$ otrzymamy dla prawie wszystkich p wielomian mający niewiele niezerowych współczynników (będzie to z grubsza kwadrat wielomianu $S_p(x)$ zdefiniowanego wcześniej).

Pytanie 7. *Czy dla każdego ustalonego $W(x)$ istnieje taka liczba N, że dla dowolnej liczby pierwszej p, $T_p(x)$ ma co najwyżej N niezerowych współczynników? A może chociaż da się podać jakieś nietrywialne ograniczenie na liczbę niezerowych współczynników zależne od p ?*

Odpowiedź na pierwsze pytanie okazuje się być twierdząca dla wielomianów postaci $W(x) = x^k$.