

Лабораторна робота №7

Модульні обчислення

Мета роботи: навчитися застосовувати оператори SymPy для побудови функцій для дослідження властивостей модульних обчислень

Теоретичні відомості

https://uk.wikipedia.org/wiki/Китайська_теорема_про_залишки

https://uk.wikipedia.org/wiki/Символ_Лежандра

https://uk.wikipedia.org/wiki/Символ_Якобі

https://uk.wikipedia.org/wiki/Символ_Кroneckera_—_Якобі

Завдання:

Варіант 1. Китайську теорему про залишки можна сформулювати наступним чином. Нехай y_1, y_2, \dots, y_k довільні цілі числа, а n_1, n_2, \dots, n_k попарно взаємно прості числа. Тоді наступна система:

$$\begin{aligned} x &\equiv y_1 \pmod{n_1} \\ x &\equiv y_2 \pmod{n_2} \\ &\vdots \\ x &\equiv y_k \pmod{n_k} \end{aligned} \quad (*)$$

має розв'язок і всі її розв'язки рівні за модулем $M = n_1 n_2 \dots n_k$.

Розробити процедуру розв'язку системи (*) порівнянь, що приймає список цілих чисел y_1, y_2, \dots, y_k и (такої ж довжини) та список попарно взаємно простих модулів n_1, n_2, \dots, n_k та повертає розв'язок x та модуль M .

Варіант 2. Розробити та перевірити функцію `LEGENDREsymb(a,p)`, що обчислює символ Лежандра. Обчислити `LEGENDREsymb(2562357894096485,1000003)`; `LEGENDREsymb(80,2)`

Варіант 3. Розробити та перевірити функцію `JACOBSymb(a,m)`, що обчислює символ Якобі. Обчислити `JACOBSymb(-6,7)`; `JACOBSymb(-6,63)`

Варіант 4. Розробити та перевірити функцію `KRONECKERsymb(a,m)`, що обчислює символ Кронекера. Заповнити таблицю значень $\left(\frac{a}{m}\right)$ для $a=-4\dots4$ (відкладається по горизонталі) $m=-4\dots4$ (відкладається по вертикалі).