

Точна арифметика цілих чисел

Написати частину бібліотеки класів цілочисельної арифметики, що дозволяє використання чисел довільної довжини. Для класів повинні бути перевантажені базові оператори (+, -, *, <<, при бажанні інші). В рамках бібліотеки потрібно реалізувати наступні алгоритми:

1. Множення невід'ємних цілих чисел методом Карацуби [Кнут, т.2, гл.4, 4.3.3].
2. Множення невід'ємних цілих чисел методом Тоома-Кука [Кнут, т.2, гл.4, 4.3.3].
3. Множення невід'ємних цілих чисел модулярним методом (Кнут також називає його методом Шенхаге) [Кнут, т.2, гл.4, 4.3.3].
4. Множення невід'ємних цілих чисел методом Шенхаге-Штрассена [Кнут, т.2, гл.4, 4.3.3].
5. Обчислення оберненої величини з високою точністю (алгоритм Кука) [Кнут, т.2, гл.4, 4.3.3].
6. Ділення цілих чисел алгоритмом Кука [Кнут, т.2, гл.4, 4.3.3].
7. Перевірка простоти числа методом Ферма [Шнайер, с. 297].
 - https://en.wikipedia.org/wiki/Fermat_primality_test
8. Перевірка простоти числа методом Рабіна-Міллера [Шнайер, с. 298].
 - https://en.wikipedia.org/wiki/Miller-Rabin_primality_test
9. Перевірка простоти числа методом Соловея-Штрассена [Шнайер, с. 298].
 - https://en.wikipedia.org/wiki/Solovay-Strassen_primality_test
10. Перевірка простоти числа методом Агравала
 - https://en.wikipedia.org/wiki/AKS_primality_test
 - <http://fatphil.org/math/AKS/>

Огляд ідей швидкого множення цілих чисел:

- <http://cr.yp.to/papers/m3.pdf>
- <https://members.loria.fr/PZimmermann/mca/mca-0.3.pdf>