15 мая 2015 г.

Доклад аспиранта Михаила Лысова на тему

«Оптимизация алгоритма умножения полиномов над кольцом»

Для многочленов над кольцом характеристики 2 получен новый алгоритм умножения. Для многочленов степени $n-1$ он использует $O(n \log n \log\log n)$ сложений в кольце и арифметических операций в $\mathbb{F}_2$ и $O(\frac{n \log n}{\log\log n} 2^{\log_2^* n})$ умножений в кольце. По сравнению с алгоритмом Кантора-Калтофена количество сложений не улучшилось, но мультипликативная сложность упала асимптотически с $O(n \log n)$, однако алгоритм Кантора-Калтофена работает над произвольным кольцом. Полученный алгоритм может эффективно применяться для умножения матричных многочленов, которые возникают, как часть алгоритма Томе. При построении алгоритма используются стандартное мультипликативное дискретное преобразование Фурье, а также аддитивное дискретное преобразование Фурье, введённое Гао и Матиром.