МЕТОДЫ И АЛГОРИТМЫ ПРОВЕРКИ ДЕЛИМОСТИ БОЛЬШИХ МАССИВОВ ЧИСЕЛ МЕРСЕННА РЕКОРДНОЙ ДЛИНЫ НА БАЗЕ СУПЕРКОМПЬЮТЕРНОГО КОМПЛЕКСА МГУ (ПРОЕКТ «ТРИАМЕР»)

Профессор К.Сомик

Проблема поиска простых чисел Мерсенна рекордной длины

- Числа Мерсенна: $M(p) = 2^p - 1,\ p -$ простое число.
- Проект распределенных вычислений GIMPS. Рекордное число: ***M*[43112609]; 12978189** разрядов. Найдено в 2008 году.
- Тест Люка-Лемера:

$$m_1 = 4;$$

$$\ldots$$

$$m_{i+1} = Mod[(m^2{}_i - 2), M(p)];$$

$$\ldots$$

$$m_{p-1} = Mod[(m^2{}_{p-2} - 2), M(p)] = 0 \rightarrow M(p) \rightarrow простое\ число.$$

Проект Триамер:
поиск рекордного числа Мерсенна на базе СКК МГУ

- Диапазон поиска: ***DM*[43112609,50298029]** содержит **406946 *M(p)* –** чисел.
- **Этап 1:** Отсев большей части составных ***M(p)* –** чисел в ***DM*** с помощью параллельного выполнения алгоритма ***Trimr_sv.***
- **Этап 2:** Сертификация оставшихся псевдопростых чисел с помощью алгоритма ***Trimr_str,*** который намного быстрее теста Люка-Лемера.

Алгоритм отсева составных чисел *Trimr_sv*

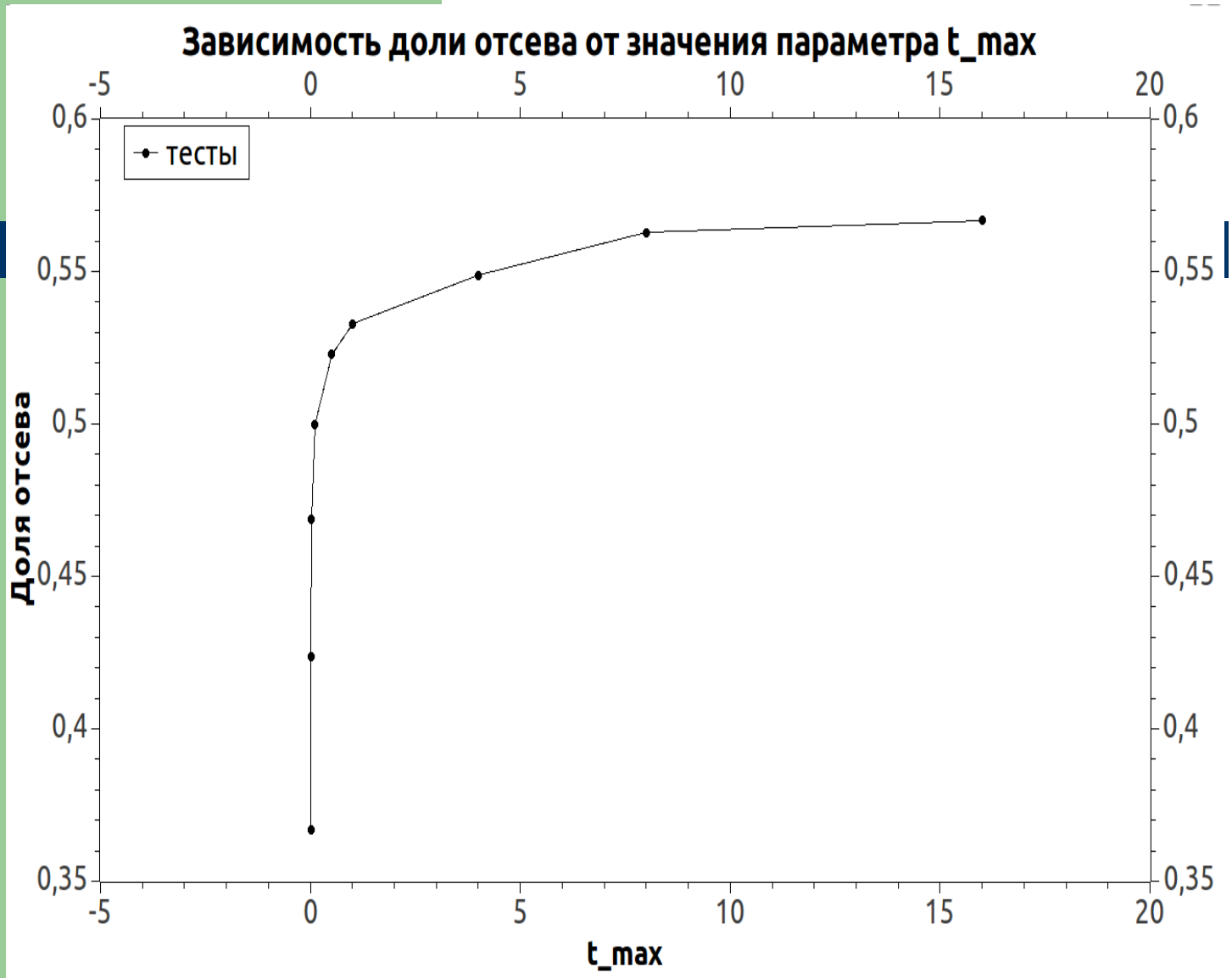
- Свойства **Триангулярной периодической системы чисел (ТПСЧ):**
- Формула допустимого делителя M(p) – чисел:
- $x = 24 \bullet p \bullet t_x + 2 \bullet p \bullet a_i + 1$ - параметр индекса делителя может принимать одно из четырех значений в зависимости от формы *p*:

Форма *p*	$a_1(p)$	$a_2(p)$	$a_3(p)$	$a_4(p)$
$6*s+1$	0	8	$12 - Mod[(18*s-3),12]$	$Mod[(6*s-1),12]$
$6*s-1$	0	4	$Mod[(6*s-3),12]$	$Mod[(6*s+1),12]$

- Редукция размерности делимого к размерности квадрата делителя.
- Локализации области нулевых значений целочисленного дифференциала частного k - го порядка

Результаты тестирования программы *Trimr_sv* на СКК МГУ

- Алгоритм реализован на языке C с применением технологий: Posix Threads (для распараллеливания между ядрами), OpenMPI (для межпроцессорного взаимодействия), GNU MP (для реализации больших чисел).
- Программа Trimr_sv тестировалась на суперкомпьютере «Ломоносов» на 10 и 20 узлах (20 и 40 процессоров соответственно).
- Изменяемым параметром был коэффициент $t\_\max$: $t\_\max = IP[\frac{t_x}{p}] = [0{,}0001 \Leftrightarrow 16]$
- Для каждого значения параметра измерялась доля отсева составных чисел и время обработки. Вывод: программа обеспечивает отсев более половины составных чисел за приемлемое время.
- При увеличении количества процессоров обеспечивается практически линейное увеличение быстродействия при заданной уровне параметра.


Зависимость доли отсева от значения параметра t_max
тесты
Доля отсева
t_max
-5
0
5
10
15
20
0,6
0,55
0,5
0,45
0,4
0,35

Сравнительная оценка быстродействия Trimr_sv

- Проводилось сравнение быстродействия алгоритма Trimr_sv и функции FactorIntegerECM пакета Математика (Wolfram Research, USA), реализующей алгоритм факторизации Х.Ленстра (один из наиболее быстродействующих алгоритмов, использующих метод эллиптических кривых).
- 1) Trimr_sv обеспечивает нахождение наименьшего делителя составных чисел Мерсенна с показателем в рекордном диапазоне за время чуть более **0,2 сек.,** тогда как функция FactorIntegerECM при обработке тех же чисел вообще не дает решения за приемлемое время.
- 2) функция FactorIntegerECM находит наименьший множитель числа Мерсенна с показателем p = 86423 за **7613.94 сек.,** тогда как Trimr.sv для такого же числа делает это за **0,531 сек.** (протоколы выполнения на слайде №8), т.е. в более чем в **14 000 раз** быстрее.
- Эти данные получены на обычном персональном компьютере без эффекта распараллеливания, который многократно ускоряет обработку.

Протокол выполнения алгоритмов Trimr.sv и FactorIntegerECM

- Mathematica 5.2 for Students: Microsoft Windows Version
- Copyright 1988-2005 Wolfram Research, Inc.
- -- Terminal graphics initialized --
- In[1]:= <<NumberTheory`FactorIntegerECM`
- 1. Trimr.sv and ECM Comparative Test: THE PROGRAMM of elimination of composite Mersenne numbers.Extraction of root from divident. p: 43143311 43143391 43133513 43127519 43123361
- p = 86423 jm = 9
- comp p = 86423 x = 4063955153 t = 23512
- **Out[19]= {0.531 Second, Null}**
- In[20]:= <<NumberTheory`FactorIntegerECM`
- In[21]:= \!\(Print["\< FactorIntegerECM (H.W.Lenstra) 21767 \>"];
- Timing[p = 86423; n = 2\^p - 1; x = FactorIntegerECM[n];
- Print["\< x = \>", x]]\)
- FactorIntegerECM (H.W.Lenstra) 21767
- x = 4063955153
- **Out[21]= {7613.94 Second, Null}**
- 2. Trimr.sv and ECM Comparative Test: THE PROGRAMM of elimination of composite Mersenne numbers.Extraction of root from divident. p: 43143311 43143391 43133513 43127519 43123361
- p = 43127519 jm = 13
- comp p = 43127519 x = 566264324471 t = 6565
- **Out[6]= {0.234 Second, Null}**

Таким образом, на базе суперкомпьютерного комплекса МГУ экспериментально установлена высокая эффективность новых методов и алгоритмов проверки делимости больших массивов чисел Мерсенна рекордной длины.

Благодарю за внимание!