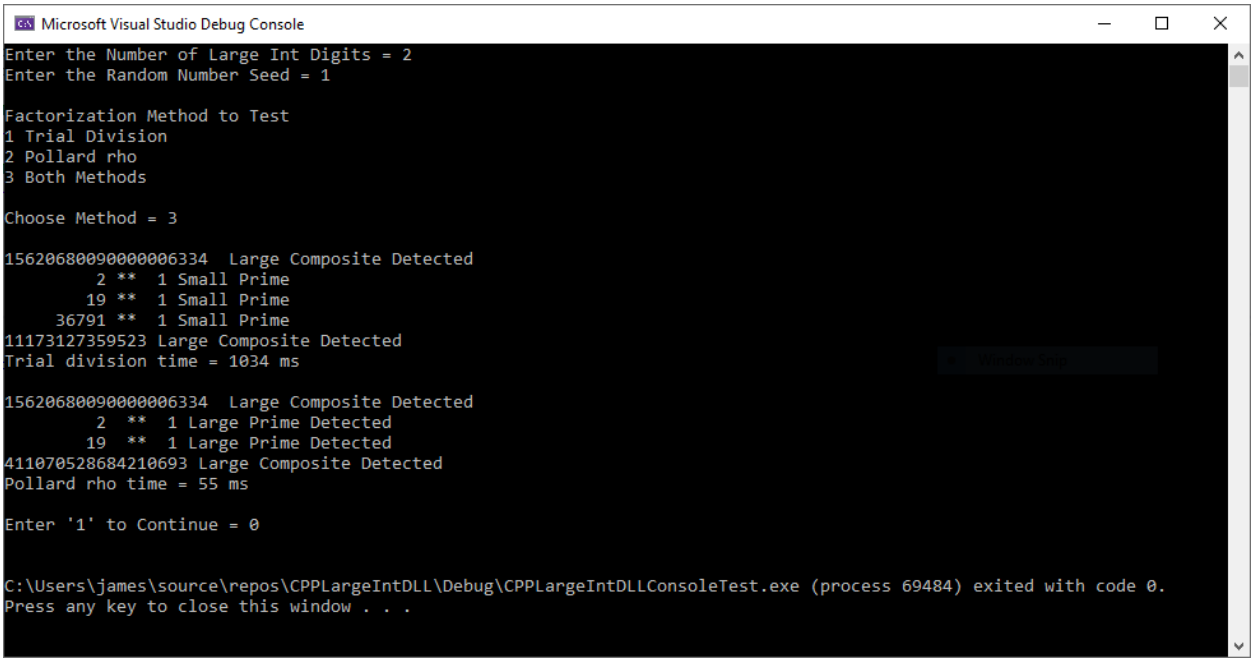
Blog Entry 02 20 2022 by James Pate Williams Jr

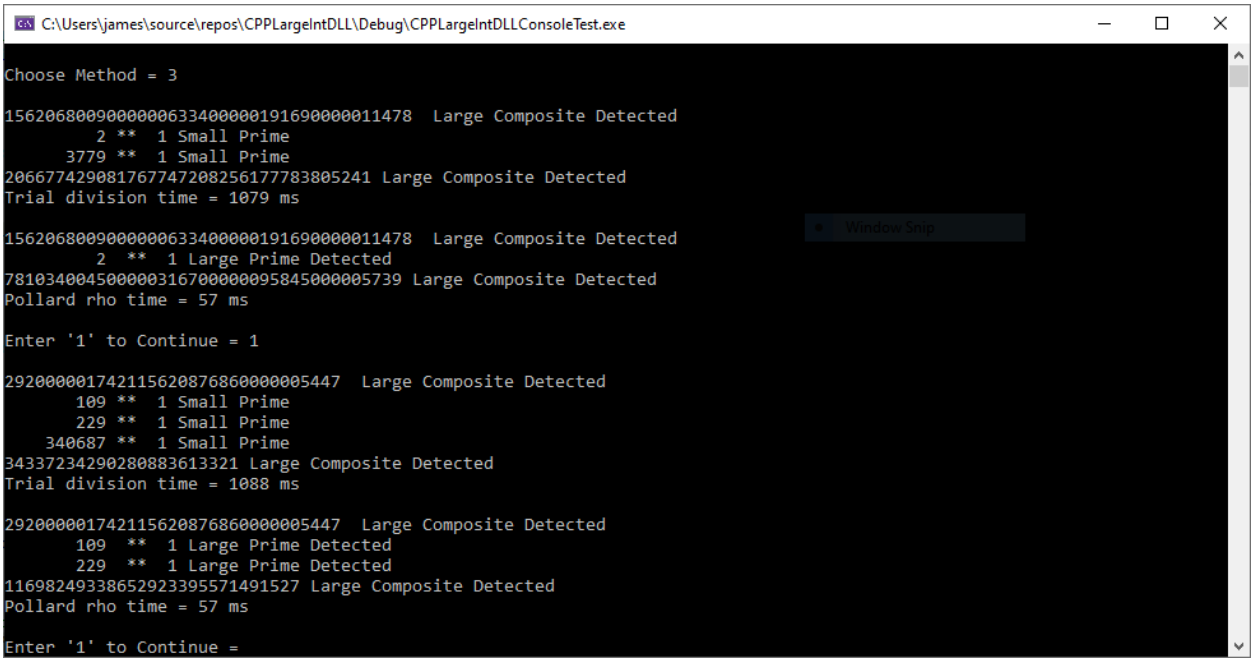
I got very dissatisfied with my efforts to port H. T. Lau's excellent NUMAL C code to Python. I think the reason was that I had mixed endian code, one part based on little endian and the other big endian. I used my C# unsigned large integer code to create a Microsoft Visual Studio 2019 Community C++ dynamic link library. It has been over two decades since I created C/C++ DLLs. I wrote several C# DLLs back in 2015. My new C++ DLL has a sieve of Eratosthenes capable of giving a user access to 664,579 primes which is the number of small prime numbers less than 10,000,000. I use an unsigned long long (ull) data type to create a 64-bit based sieve. Here is some information based on my multiple threading C++ standalone sieve applications. I personally developed the bit manipulation C code in around 1996 or 1997. The source code was then used for the initial permutation found in my DES (Data Encryption Standard) implementations (C, C++, C#, and Java). I have used two elementary number theory algorithms to test my DLL: the Miller-Rabin probabilistic primality test and the simple trial division factorization method. My plans for the next period are to port more number theoretical code to the DLL.

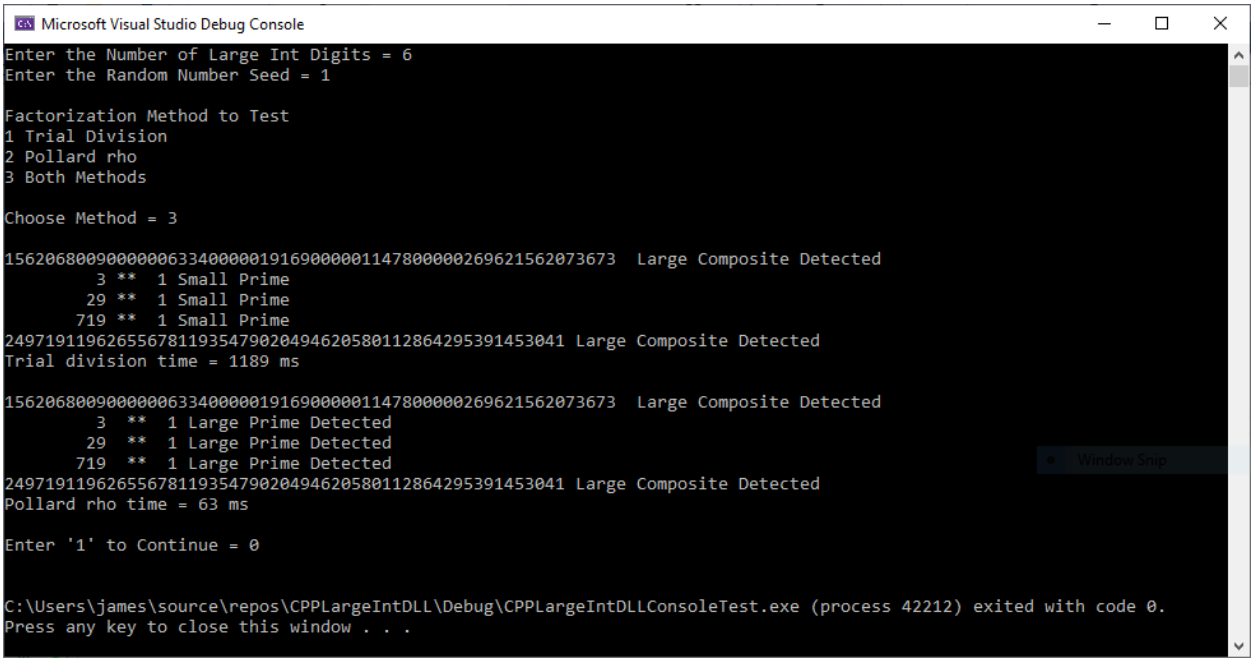
n	Sieve 1 (s)	Sieve 2 (s)
1000000	0.073	0.063
1000000	0.075	0.061
1000000	0.073	0.061
1000000	0.073	0.062
1000000	0.074	0.063
1000000	0.071	0.063
1000000	0.072	0.063
1000000	0.073	0.065
1000000	0.075	0.063
1000000	0.074	0.063
average	0.073	0.063

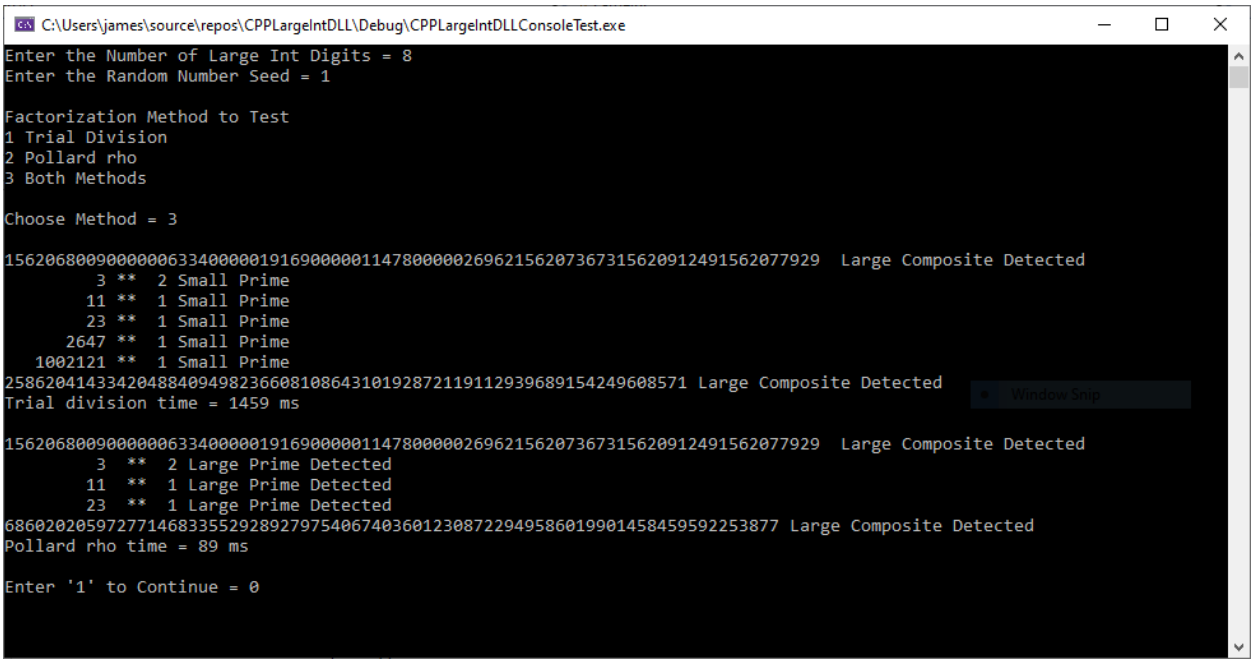
n	Sieve 1 (s)	Sieve 2 (s)	# of primes
1000000	0.074	0.064	78498
2000000	0.195	0.147	148933
3000000	0.32	0.236	216816
4000000	0.46	0.332	283146
5000000	0.593	0.443	348513
6000000	0.759	0.569	412849
7000000	0.919	0.692	476648
8000000	1.088	0.836	539777
9000000	1.267	0.994	602489

Sieve 1	Sieve of Eratosthenes
Sieve 2	Sieve of Atkin


Microsoft Visual Studio Debug Console
Enter the Number of Large Int Digits = 2
Enter the Random Number Seed = 1
Factorization Method to Test
1 Trial Division
2 Pollard rho
3 Both Methods
Choose Method = 3
15620680900000006334 Large Composite Detected
2 ** 1 Small Prime
19 ** 1 Small Prime
36791 ** 1 Small Prime
11173127359523 Large Composite Detected
Trial division time = 1034 ms
15620680900000006334 Large Composite Detected
2 ** 1 Large Prime Detected
19 ** 1 Large Prime Detected
411070528684210693 Large Composite Detected
Pollard rho time = 55 ms
Enter '1' to Continue = 0
C:\Users\james\source\repos\CPPLargeIntDLL\Debug\CPPLargeIntDLLConsoleTest.exe (process 69484) exited with code 0.
Press any key to close this window . . .


C:\Users\james\source\repos\CPPLargeIntDLL\Debug\CPPLargeIntDLLConsoleTest.exe
Choose Method = 3
1562068009000000633400000191690000011478 Large Composite Detected
2 ** 1 Small Prime
3779 ** 1 Small Prime
20667742908176774720825617778380524 1 Large Composite Detected
Trial division time = 1079 ms
1562068009000000633400000191690000011478 Large Composite Detected
2 ** 1 Large Prime Detected
781034004500000316700000095845000005739 Large Composite Detected
Pollard rho time = 57 ms
Enter '1' to Continue = 1
29200000174211562087686000000 5447 Large Composite Detected
109 ** 1 Small Prime
229 ** 1 Small Prime
340687 ** 1 Small Prime
34337234290280883613321 Large Composite Detected
Trial division time = 1088 ms
29200000174211562087686000000 5447 Large Composite Detected
109 ** 1 Large Prime Detected
229 ** 1 Large Prime Detected
11698249338652923395571491527 Large Composite Detected
Pollard rho time = 57 ms
Enter '1' to Continue =


Microsoft Visual Studio Debug Console
Enter the Number of Large Int Digits = 6
Enter the Random Number Seed = 1
Factorization Method to Test
1 Trial Division
2 Pollard rho
3 Both Methods
Choose Method = 3
1562068009000000633400000191690000011478000002696215620736 73 Large Composite Detected
3 ** 1 Small Prime
29 ** 1 Small Prime
719 ** 1 Small Prime
249719119626556781193547902049462058011286429539145304 1 Large Composite Detected
Trial division time = 1189 ms
1562068009000000633400000191690000011478000002696215620736 73 Large Composite Detected
3 ** 1 Large Prime Detected
29 ** 1 Large Prime Detected
719 ** 1 Large Prime Detected
249719119626556781193547902049462058011286429539145304 1 Large Composite Detected
Pollard rho time = 63 ms
Enter '1' to Continue = 0
C:\Users\james\source\repos\CPPLargeIntDLL\Debug\CPPLargeIntDLLConsoleTest.exe (process 42212) exited with code 0.
Press any key to close this window . . .


C:\Users\james\source\repos\CPPLargeIntDLL\Debug\CPPLargeIntDLLConsoleTest.exe
Enter the Number of Large Int Digits = 8
Enter the Random Number Seed = 1
Factorization Method to Test
1 Trial Division
2 Pollard rho
3 Both Methods
Choose Method = 3
1562068009000000633400000191690000011478000002696215620736731562091249156207792 9 Large Composite Detected
3 ** 2 Small Prime
11 ** 1 Small Prime
23 ** 1 Small Prime
2647 ** 1 Small Prime
1002121 ** 1 Small Prime
258620414334204884094982366081086431019287211911293968915424960857 1 Large Composite Detected
Trial division time = 1459 ms
1562068009000000633400000191690000011478000002696215620736731562091249156207792 9 Large Composite Detected
3 ** 2 Large Prime Detected
11 ** 1 Large Prime Detected
23 ** 1 Large Prime Detected
686020205972771468335529289279754067403601230872294958601990145845959225387 7 Large Composite Detected
Pollard rho time = 89 ms
Enter '1' to Continue = 0