Applied Deterministic Primality for Rational Integers Less than 2^{52}

J.A Sory

May 10, 2022

Goal-Motivation The goal of this paper is to provide a useful method of efficient primality checking. While work by other's such as Dana Jacobsen, Michal Forisek & Jacina, and Bradley Berg are useful in providing an efficient worst-case primality test. They omit many details and neglect the average case complexity to the point of faring no better than a standard hybrid Miller-rabin/trial division test. In contrast, this paper demonstrates a full implementation of a primality test, utilizing optimizations that may increase the worst-case complexity marginally in exchange for a considerable reduction in average complexity.

Mathematical algorithm The general algorithm is constructed of trial division, followed by a strong fermat test

Trial Division Trial division is normally performed by successively dividing by the primes under the sqrt(n) to prove that n has no factors other than itself and 1. However here the trial division is only meant to eliminate composites before performing the more computationally intensive fermat tests that prove the primality. Additionally in an applied setting division is slower than multiplication by a factor of 2 or greater. Fortunately we can exploit this by multiplying by multiplicative inverse modulo 2^{64}, as all machine-word size arithmetic is performed modulo 2^{64} this makes it a simple multiplication. Table

Fermat Test

Multiplicative Inverse of Primes $\mathbb{Z}_{[2^{64}]}$

$$
\begin{bmatrix}
12297829382473034411 & 14757395258967641293 & 7905747460161236407 & 3353953467947191203 \\
5675921253449092805 & 17361641481138401521 & 9708812670373448219 & 15238614669586151335 \\
3816567739388183093 & 17256631552825064415 & 1495681951922396077 & 10348173504763894809 \\
9437869060967677571 & 5887258746928580303 & 2436362424829563421 & 14694863923124558067 \\
5745707170499696405 & 17345445920055250027 & 1818693077689674103 & 9097024474706080249 \\
11208148297950107311 & 11779246215742243803 & 17617676924329347049 & 11790702397628785569 \\
4200743699953660269 & 15760325033848937303 & 8619973866219416643 & 12015769075535579493 \\
10447713457676206225 & 9150747060186627967 & 281629680514649643 & 16292379802327414201 \\
4246732448623781667 & 16094474695182830269 & 8062815290495565607 & 6579730370240349621 \\
2263404180823257867 & 10162278172342986519 & 9809829218388894501 & 17107036403551874683 \\
3770881385233444253 & 2124755861893246783 & 8124213711219232577 & 14513935692512591373 \\
2780916192016515319 & 13900627050804827995 & 7527595115280579359 & 1950316554048586955 \\
2094390156840385773 & 7204522363551799129 & 7255204782128442895 & 17298606475760824337 \\
2939720171109091891 & 18374966859414961921 & 15430736487513693367 & 10354863773718001093 \\
15383631589145234927 & 17181443938689762877 & 14245350405676059433 & 5149444458738708755 \\
2707201348701401773 & 17305088903023944187 & 9134400602415662215 & 6365010734698503433
\end{bmatrix}
$$