Average Case Error Estimates of the Strong Lucas Probable Prime Test

Semira Einsele

FU Berlin

Generating large prime numbers and testing numbers for primality are crucial in many public-key cryptography algorithms. A common choice of a probabilistic primality test is the strong Lucas probable prime test which is based on the Lucas sequences with fixed discriminant D. In this work we estimate bounds for average error behaviour of this test.

To do so, let us consider a procedure that draws k-bit odd integers independently from the uniform distribution, subjects each number to t independent iterations of the strong Lucas probable prime test with randomly chosen bases, and outputs the first number that passes all t tests. Let $q_{k,t}$ denote the probability that this procedure returns a composite number. We show that $q_{k,1}<\log(k)k^24^{2.3-\sqrt{k}}$ for $k\geq 2$. We see that slightly modifying the procedure by enforcing that only considering integers n with Jacobi symbol $\legendre{D}{n}=-1$ and doing trial division by the first l odd primes gives remarkable improvements in this error analysis. Let $q_{k,l,t}$ denote the probability that the modified procedure returns a composite number. We show that $q_{k,127,1}< k^24^{1.729 - 0.998\sqrt{k-1}}$ for $k\geq 2$. We also give general bounds for both $q_{k,t}$ and $q_{k,l,t}$ when $t\geq 2, k\geq 21$ and $l\in \N.$ In addition, we treat the numbers, that add the most to our probability estimate separately, obtaining an improved bound for large t. Moreover, every odd composite integer n that is not a product of twin primes is declared prime at most $4n/15$ times. Although this result does not directly imply that $q_{k,t}\leq (4/15)^t$, we are able to show that $q_{k,t}\leq (4/15)^t$ for $k\geq 118$.

Keywords: Strong Lucas test, secure prime generation, average case error estimate