MATH 467, The Miller-Rabin Test

Algorithm MR.

0. Check that n is odd and stop if it is not.

1. Check n for small factors, say not exceeding $\log n$ and stop if it has one.

2. Check whether n is a prime power, for example by comparing $\lfloor n^{1/k} \rfloor$ with $n^{1/k}$ for $2 \le k \le \frac{\log n}{\log 2}$, and stop if it is.

3. Take out the powers of 2 in $n-1$ so that

$$n - 1 = 2^u v$$

with v odd.

4. For each a with $2 \le a \le \min\left\{2(\log n)^2, n-2\right\}$ check the statements

$$a^v \equiv 1 \pmod{n},\ a^v \equiv -1 \pmod{n}, \ldots, a^{2^{u-1}v} \equiv -1 \pmod{n}.$$

5. If a is such that they are all false, stop and declare that n is composite and a is a witness.

6. If no witness a is found with $a \le \min\left\{2(\log n)^2, n-2\right\}$, then declare that n is prime.

There are a couple of further wrinkles that can be tried in this process.

A. Before doing the congruence checks in 4, check that $(a,n) = 1$ because if $(a,n) > 1$, then one has a proper divisor of n and not only is n composite but one has found a factor.

B. With regard to the construction of a in the proof of Theorem 6.2, we see that a is a QNR with respect to one of the prime factors of n, and we observed in Section §5.1 that the least QNR modulo a prime is itself a prime. Thus it is no surprise that in the application of the Riemann Hypothesis described there the $a \le 2(\log n)^2$ which are used are in fact prime. Hence we could restrict our attention to prime values of a. This is a mixed blessing since although the primes are relatively infrequent it is conceivable that the least witness a is composite,