The AKS Primality Test

Results from Analytic Number Theory

Andreas Klappenecker

September 11, 2002

Agrawal, Kayal, and Saxena gave in [1] a deterministic algorithm to decide whether or not a given integer n is prime. We gave an exposition of this algorithm in the lecture notes [2]. We proved there that the AKS algorithm is correct. It is not obvious, however, that the AKS algorithm has a runtime that is polynomial in the number of digits of n, because the second step of the algorithm contains a while loop, which might have an exponential number of iterations, unless it terminates early. This second step is shown below:

Algorithm 1 Second step of the AKS primality test

Input: An integer $n > 1$.

$r := 2$;
while $(r < n)$ **do**
    if $\gcd(r, n) \neq 1$ **then output** `composite` **fi**;
    if r is prime **then**
        $q :=$ largest prime factor of $r - 1$;
        if $(q \geq 4\sqrt{r}\log n)$ and $(n^{(r-1)/q} \not\equiv 1 \bmod r)$ **then break fi**;
    fi;
    $r := r + 1$;
od;

Theorem 1 *Let $n > 1$. The while loop of Algorithm 1 is iterated at most $O((\log n)^6)$ times.*

The proof of this result depends on results of analytic number theory. First, we need a standard fact about the distibution of primes:

Lemma 2 *Let $\pi(n)$ denote the number of primes $\leq n$. Then for $n \geq 1$:*

$$\frac{n}{6\log n} \leq \pi(n) \leq \frac{8n}{\log n}.$$

Let $P(n)$ denote the greatest prime divisor of n. We will call a prime r **special** for n if and only if $P(r-1) > (c_2(\log_2 n)^6)^{2/3}$, where c_2 denotes an absolut constant. The following result by Fouvry will be essential in proving that a special prime exist for n.

Lemma 3 (Fouvry) *There exist constants $c > 0$ and n_0 such that for all $x > n_0$*

$$|\{p \,|\, p \text{ is prime}, p \leq x, P(p-1) > x^{2/3}\}| \geq c\frac{x}{\log x}$$

Roughly speaking, Fouvry's result asserts that there exist many primes $p < n$ such that the largest prime factor of $p-1$ is big, namely $P(p-1) > x^{2/3}$.

Lemma 4 *There exist positive constants c_1, c_2 for which there is a prime in the interval $[c_1(\log n)^6, c_2(\log n)^6]$ such that $r-1$ has a prime factor $q \geq 4\sqrt{r}\log n$ which satisfies $n^{(r-1)/q} \not\equiv 1 \bmod r$.*

Proof. Let c denote the same constant as in Lemma 3. For large n, the number of special primes between $c_1(\log n)^6$ and $c_2(\log n)^6$ is certainly greater than

$$\begin{aligned}
&(\#\text{ special primes in } [1..c_2(\log n)^6]) - (\#\text{ primes in } [1..c_1(\log n)^6]) \\
&\geq \frac{cc_2(\log n)^6}{6\log(c_2\log n)} - \frac{8c_1(\log n)^6}{6\log\log n} \quad \{\text{Lemma 3} - \text{upper bound of Lemma 2}\} \\
&\geq \frac{cc_2(\log n)^6}{7\log\log n} - \frac{8c_1(\log n)^6}{6\log\log n} \quad \{\text{for large } n\} \\
&= \frac{(\log n)^6}{\log\log n}\left(\frac{cc_2}{7} - \frac{8c_1}{6}\right)
\end{aligned}$$

We choose the constant $c_2 \geq 4^6$ such that the quantity in parentheses is a positive constant, say c_3. Let $x = c_2(\log n)^6$. Consider the product

$$\gamma = (n-1)(n^2-1)\cdots(n^{x^{1/3}}-1).$$

A number m has at most $\log m$ prime factors. Therefore, the product γ of $x^{1/3}$ numbers of size $\leq n^{x^{1/3}}$ has at most $x^{1/3}\log n^{x^{1/3}} = x^{2/3}\log n$ prime factors.

Since $x = c_2(\log n)^6$, we get at most $x^{2/3}\log n = c_2^{2/3}(\log n)^4\log n = c_2^{2/3}(\log n)^5$ prime factors of γ. For large n, this number is clearly smaller than $c_3(\log n)^6/\log\log n$, our lower bound for the number of special primes in the interval $[c_1(\log n)^6, c_2\log n)^6]$. We can conclude that there exists at least one special prime $r \leq c_2(\log n)^6$, which does not divide the product γ.

By definition, $r-1$ has a prime factor $q \geq (c_2(\log n)^6)^{2/3} = c_2^{2/3}(\log n)^4$. We have $r \leq c_2(\log n)^6$, hence $\sqrt{r} \leq c_2^{1/2}(\log n)^3$. Thus $4\sqrt{r}\log n$ is smaller than $4c_2^{1/2}(\log n)^4$. We have $c_2^{2/3}(\log n)^4 \geq 4c_2^{1/2}(\log n)^4$, because $c_2^{2/3-1/2} = c_2^{1/6} \geq 4$ due to the choice $c_2 \geq 4^6$. Therefore, we have established that

$$q \geq c_2^{2/3}(\log n)^4 \geq c_2^{1/2}(\log n)^4 \geq 4\sqrt{r}\log n.$$

It remains to show that $n^{(r-1)/q} \not\equiv 1 \bmod r$. We know that $q \geq c_2^{2/3}(\log n)^4$ and that $r-1 \leq c_2(\log n)^6$. Therefore,

$$\frac{r-1}{q} \leq \frac{c_2(\log n)^6}{c_2^{2/3}(\log n)^4} = c_2^{1/3}(\log n)^2. \qquad (1)$$

Since $\gamma \not\equiv 0 \bmod r$, we know that $n^k \not\equiv 1 \bmod r$ for all k in the range $1 \leq k \leq x^{1/3} = c_2^{1/3}(\log n)^2$. In particular, $n^{(r-1)/q} \not\equiv 1 \bmod r$ holds because of (1). □

Theorem 1 follows directly from Lemma 4.

Remark. We followed the excellent paper [1] in our exposition. However, we adapted the constant c_2 to make the argument work. In contrast to [1], we did not instist on $c_1 \geq 4^6$, which leads to an unnecessarily large constant c_2.

References

[1] M. Agrawal, N. Kayal, and N. Saxena. Primes is in P. Preprint, IIT Kanpur, August 2002.

[2] A. Klappenecker. An introduction to the AKS primality test. Lecture notes, September 2002.