Draft.

PROVING PRIMALITY IN ESSENTIALLY QUARTIC EXPECTED TIME

DANIEL J. BERNSTEIN

1. Introduction

This paper presents a randomized algorithm that proves primality in $(4+o(1))$-power expected time:

- Section 2 proves that, if we are given a certificate (parameters satisfying various hypotheses) for n, then n is prime.
- Section 3 presents an algorithm to verify a reasonably small certificate in time $(\lg n)^{4+o(1)}$.
- Section 4 presents a randomized algorithm that, given a prime n, finds a reasonably small certificate for n in expected time $(\lg n)^{2+o(1)}$.

For comparison: The cyclotomic primality-proving method, which holds the current speed records for small n, takes time $(\lg n)^{O(\lg \lg \lg n)}$. The elliptic-curve primality-proving method is conjectured to take polynomial expected time, but with a larger exponent than $4+o(1)$. The Adleman-Huang variant takes polynomial expected time, but with a larger exponent and a much more difficult proof.

This algorithm is inspired by the recent Agrawal-Kayal-Saxena algorithm, which proves primality in polynomial time. The improvement of the time exponent to $4+o(1)$ relies on an idea by Pedro Berrizbeitia, twisting $x-s$ into $x-s\zeta^m$. Berrizbeitia used this idea to prove primality in $(4+o(1))$-power expected time for a sparse set of primes, namely the n's for which n^2-1 is divisible by a power of 2 around $(\lg n)^2$.

Independently of and slightly earlier than this paper, Qi Cheng proposed a primality-proving algorithm that is conjectured to take $(4+o(1))$-power expected time. Cheng used Berrizbeitia's idea to prove primality in $(4+o(1))$-power expected time for a larger set of primes, namely the n's for which $n-1$ is divisible by a prime around $(\lg n)^2$; Cheng then used one elliptic-curve primality-proving step to prove primality of any n, using an auxiliary prime in the larger set.

The best case for the algorithm in this paper is an even larger set of primes, namely the n's for which $n-1$ has any divisor around $(\lg n)^2$. Perhaps the algorithm will set speed records in that case; if so, using an elliptic-curve step to reduce to that case is also likely to be a good idea; I don't know whether more general cases of the algorithm will be useful.

Date: 20030128.
1991 *Mathematics Subject Classification.* Primary 11Y16.

2. The primality certificate

Theorem 2.1. *Let n, d, and e be positive integers. Let c, c_-, c_+ be integers. Let f be a monic polynomial in $(\mathbf{Z}/n)[y]$ of degree d. Define R as the ring $(\mathbf{Z}/n)[y]/f$. Let r be an element of R. Let S be a finite subset of R. Assume that*

- *e divides $n^d - 1$;*
- *$r^{n^d-1} = 1$ in R;*
- *$r^{(n^d-1)/q} - 1$ is a unit in R for each prime q dividing e;*
- *s is a unit in R for all $s \in S$;*
- *$s^e - (s')^e$ is a unit in R for all distinct $s, s' \in S$;*
- *$s^e - r$ is a unit in R for all $s \in S$;*
- *$\binom{e\#S}{c_-}\binom{c}{c_-}\binom{e\#S-c_-}{c_+}\binom{e-1-c}{c_+} \geq n^{d\lceil\sqrt{e/3}\rceil}$; and*
- *$(x-s)^{n^d} = x^{n^d} - s$ in the ring $R[x]/(x^e - r)$ for all $s \in S$.*

Then n is a power of a prime.

With the additional hypothesis that n is not a perfect power, the theorem shows that n is prime. This theorem improves on the theorems of Berrizbeitia and Cheng in two basic ways:

- d is allowed to be any positive integer. Berrizbeitia considered only $d \in \{1, 2\}$, and Cheng considered only $d = 1$. Larger d's are important for the $(\lg n)^{4+o(1)}$ theorem in this paper. On the other hand, the case $d = 1$ is the fastest case, and might end up being the only case used in practice.
- e is allowed to be any integer. Berrizbeitia considered only powers of 2 (although with slightly more general moduli $x^{2^i e} - r$), and Cheng considered only prime powers e; the proofs relied on e having only one prime divisor. Arbitrary e's are important for the $(\lg n)^{4+o(1)}$ theorem in this paper, and also save time in practice, whether or not $d = 1$.

This theorem also incorporates several smaller time-saving features. It uses negative powers as suggested by Voloch, with the lower bound suggested by Vaaler. It uses $\sqrt{e/3}$ as suggested by Lenstra, instead of $2\sqrt{e}$ or $\sqrt{e}$ or $\sqrt{e/2}$. It allows $\#S$ to vary; Berrizbeitia and Cheng considered only $\#S = 1$ (or $\#S = 2^i$ for modulus $x^{2^i e} - r$).

Proof. If $n = 1$ then n is a power of a prime, so assume that $n \geq 2$. Let p be a prime divisor of n.

Find an irreducible polynomial g in $\mathbf{F}_p[y]$ dividing the image of f. Then $k = \mathbf{F}_p[y]/g$ is a field. Write $N = n^d$ and $P = \#k = p^{\deg g}$. Note that P divides N. If $N = P$ then n must be a prime power, so assume that $N > P$. Similarly, assume that $N \neq P^2$.

Define ζ as the image of $r^{(N-1)/e}$ in k. Then ζ has order e in k; consequently e divides $P - 1$. (Indeed, $r^{N-1} = 1$ in R by hypothesis, so $\zeta^e = 1$ in k. Furthermore, if q is a prime dividing e, then $r^{(N-1)/q} - 1$ is a unit in R by hypothesis, so its image $\zeta^{e/q} - 1$ in k is a unit; hence $\zeta^{e/q} \neq 1$ in k.)

Find an irreducible polynomial h in $k[x]$ dividing the image of $x^e - r$. Then $k[x]/h$ is a field. Note that x is invertible in $k[x]/h$.

Observe that $x^{N-1} = r^{(N-1)/e} = \zeta$ in $k[x]/(x^e - r)$, hence in $k[x]/h$. Similarly, $(x^{P-1})^e = r^{P-1} = 1$ in $k[x]/h$, so x^{P-1} is a power of ζ in $k[x]/h$; say $x^{P-1} = \zeta^\ell$ in $k[x]/h$. By induction, $x^{N^i P^j} = \zeta^{i+j\ell}x$ in $k[x]/h$ for all $i \geq 0$ and $j \geq 0$.

$$\begin{tikzcd}
 & k[x]/h \\
R[x]/(x^e - r) \arrow[r] & k[x]/(x^e - r) \arrow[u] \\
R[x] \arrow[r] \arrow[u] & k[x] \arrow[u] \\
R = (\mathbf{Z}/n)[y]/f \arrow[r] \arrow[u] & k = \mathbf{F}_p[y]/g \arrow[u] \\
(\mathbf{Z}/n)[y] \arrow[r] \arrow[u] & \mathbf{F}_p[y] \arrow[u] \\
\mathbf{Z}/n \arrow[r] \arrow[u] & \mathbf{F}_p \arrow[u]
\end{tikzcd}$$

In particular, the powers $x, x^N, x^{N^2}, \ldots, x^{N^{e-1}}$ are all different in $k[x]/h$: they are exactly $x, \zeta x, \zeta^2 x, \ldots, \zeta^{e-1}x$. Conclusion to remember: a polynomial with roots $x, x^N, x^{N^2}, \ldots, x^{N^{e-1}}$ in $k[x]/h$ must be a multiple of $(z-x)(z-\zeta x)\cdots(z-\zeta^{e-1}x) = z^e - x^e = z^e - r$ where z is the polynomial variable.

Define L as the set of $(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z}$ such that e divides $\alpha + (\beta - \alpha)\ell$; then L is a lattice of determinant e. Define C as the set of $(\alpha, \beta) \in \mathbf{R} \times \mathbf{R}$ such that $\max\{|\alpha| \lg(N/P), |\beta| \lg P, |\alpha \lg(N/P) + \beta \lg P|\} \le \sqrt{e/3} \lg N$; then C is a convex symmetric set of area $3(e/3)(\lg N)^2/(\lg P)\lg(N/P) > 4e$. By Minkowski's theorem, there is a nonzero point $(\alpha, \beta) \in L \cap C$. Assume without loss of generality that $\alpha \ge 0$. If $\beta \ge 0$, define $u = (N/P)^\alpha P^\beta$ and $v = 1$; then $\lg u = \alpha \lg(N/P) + \beta \lg P \le \sqrt{e/3} \lg N$ by definition of C, and $x^{uP^\alpha} = x^{N^\alpha P^\beta} = \zeta^{\alpha + \beta\ell} x = \zeta^{\alpha\ell} x = x^{vP^\alpha}$. If $\beta < 0$, define $u = (N/P)^\alpha$ and $v = P^{-\beta}$; then $\lg u = \alpha \lg(N/P) \le \sqrt{e/3} \lg N$ and $\lg v = -\beta \lg P \le \sqrt{e/3} \lg N$ by definition of C, and $x^{uP^\alpha} = x^{N^\alpha} = \zeta^\alpha x = \zeta^{(\alpha-\beta)\ell} x = x^{P^{\alpha-\beta}} = x^{vP^\alpha}$.

The rest of the proof will use the facts that uP^α and vP^α are products of powers of N and P, that $x^{uP^\alpha} = x^{vP^\alpha}$, and that $|u - v| < N^{\sqrt{e/3}}$, to show that $u = v$. Thus $N^\alpha = P^{\alpha-\beta}$. If $\alpha = 0$ then $P^{-\beta} = 0$ so $\beta = 0$, but (α, β) was nonzero by construction; contradiction. Hence n is a power of p.

By hypothesis, if $s \in S$, then

- $(x - s)^N = x^N - s$ in $R[x]/(x^e - r)$, hence in $k[x]/(x^e - r)$; substitute $\zeta^{-m}x$ for x to obtain
- $(\zeta^{-m}x - s)^N = \zeta^{-mN}x^N - s$ in $k[x]/((\zeta^{-m}x)^e - r) = k[x]/(x^e - r)$; now multiply by $\zeta^{mN} = \zeta^m$ to obtain
- $(x - s\zeta^m)^N = x^N - s\zeta^m$ in $k[x]/(x^e - r)$; substitute x^{N^i} for x to obtain
- $(x^{N^i} - s\zeta^m)^N = x^{N^{i+1}} - s\zeta^m$ in $k[x]/(x^{N^i e} - r)$, hence in $k[x]/(x^e - r)$, since $x^{N^i e} - r = x^{N^i e} - r^{N^i}$ is a multiple of $x^e - r$; so by induction

- $(x - s\zeta^m)^{N^i} = x^{N^i} - s\zeta^m$ in $k[x]/(x^e - r)$ for all $i \ge 0$.

By Fermat's little theorem, $(x^{N^i} - s\zeta^m)^{P^j} = x^{N^i P^j} - (s\zeta^m)^{P^j} = x^{N^i P^j} - s\zeta^m$ in $k[x]$ for all $j \ge 0$. Thus $(x - s\zeta^m)^{N^i P^j} = x^{N^i P^j} - s\zeta^m$ in $k[x]/(x^e - r)$, hence in $k[x]/h$.

In particular, $(x - s\zeta^m)^{uP^\alpha} = x^{uP^\alpha} - s\zeta^m = x^{vP^\alpha} - s\zeta^m = (x - s\zeta^m)^{vP^\alpha}$ in $k[x]/h$. Pth powering is invertible in $k[x]/h$, so $(x - s\zeta^m)^u = (x - s\zeta^m)^v$ in $k[x]/h$.

Define $T = \{x - s\zeta^m : s \in S, m \in \mathbf{Z}\} \subseteq k[x]$. Then $t^u = t^v$ in $k[x]/h$ for all $t \in T$. Observe that $\#T = e\#S$. (There are e powers of ζ and $\#S$ choices of s. If $x - s\zeta^m = x - s'\zeta^{m'}$ in $k[x]$ then $s\zeta^m = s'\zeta^{m'}$ in k, so $s^e = (s')^e$ in k. If $s \ne s'$ then $s^e - (s')^e$ is a unit in R by hypothesis, so it is a unit in k; contradiction. Thus $s = s'$; so $s\zeta^m = s\zeta^{m'}$; also s is a unit in R by hypothesis, so $\zeta^m = \zeta^{m'}$.)

Each element of T is a unit in $k[x]/h$. (The remainder $(x^e - r) \bmod (x - s\zeta^m)$ is $(s\zeta^m)^e - r = s^e - r$, which is a unit in k by hypothesis; so $x^e - r$ and $x - s\zeta^m$ are coprime in $k[x]$; so h and $x - s\zeta^m$ are coprime in $k[x]$.)

Consider functions $a : T \to \mathbf{Z}$ satisfying the following conditions:

- $\#\{t \in T : a(t) < 0\} = c_-$;
- $\sum_t -a(t)[a(t) < 0] \le c$;
- $\#\{t \in T : a(t) > 0\} = c_+$;
- $\sum_t a(t)[a(t) > 0] \le e - 1 - c$.

There are $\binom{\#T}{c_-}\binom{c}{c_-}\binom{\#T-c_-}{c_+}\binom{e-1-c}{c_+} \ge N^{\lceil\sqrt{e/3}\rceil} \ge N^{\sqrt{e/3}} > |u - v|$ such functions.

Associate to each function a the product $\pi = \prod_{t\in T} t^{a(t)} \in (k[x]/h)^*$. This product satisfies $\pi^u = \pi^v$. I will show that these products are all distinct, so there are more than $|u - v|$ of them; but a field cannot have more than $|u - v|$ nonzero roots of $\pi^u = \pi^v$ if $u \ne v$. Thus $u = v$ as claimed.

So assume that b is another such function with $\prod_{t\in T} t^{a(t)} = \prod_{t\in T} t^{b(t)}$ in $k[x]/h$. Clear denominators to see that $A = B$ in $k[x]/h$, where A is the polynomial $\prod_{t\in T} t^{a(t)[a(t)>0]-b(t)[b(t)<0]}$ and B is the polynomial $\prod_{t\in T} t^{b(t)[b(t)>0]-a(t)[a(t)<0]}$. Each element $t \in T$ satisfies $t(x^{N^i}) = t^{N^i}$ in $k[x]/h$, so $A(x^{N^i}) = A^{N^i} = B^{N^i} = B(x^{N^i})$ in $k[x]/h$. Hence the polynomial $A - B$ has roots $x, x^N, x^{N^2}, \dots, x^{N^{e-1}}$ in the field $k[x]/h$; so $A - B$ is a multiple of $x^e - r$ in $k[x]$. However, A has degree $\sum_{t\in T} a(t)[a(t) > 0] - b(t)[b(t) < 0] \le e - 1 - c + c < e$, and similarly B has degree below e, so $A - B$ has degree below e; thus $A = B$ in $k[x]$. By unique factorization $a(t)[a(t) > 0] - b(t)[b(t) < 0] = b(t)[b(t) > 0] - a(t)[a(t) < 0]$, so $a(t) = b(t)$. □

3. Checking a primality certificate

Say we are given an alleged certificate $n, d, e, c, c_-, c_+, f, r, S$. How quickly can we check the conditions of Theorem 2.1?

The answer is $(\lg n)^{4+o(1)}$ for a reasonably small certificate. A reasonably small certificate has $d \in (\lg n)^{o(1)}$; $\#S \in (\lg n)^{o(1)}$; e at most $(\lg n)^{2+o(1)}$; and at most $(\lg n)^{2+o(1)}$ digits in the product of binomial coefficients $\binom{e\#S}{c_-}\binom{c}{c_-}\binom{e\#S-c_-}{c_+}\binom{e-1-c}{c_+}$.

Computing $n^d - 1$, and checking that it is divisible by e, takes time $(\lg n)^{1+o(1)}$.

Multiplying in $\mathbf{Z}/n$ takes time $(\lg n)^{1+o(1)}$. Thus multiplying in $R = (\mathbf{Z}/n)[y]/f$ takes time $(\lg n)^{1+o(1)}$. Computing the $n^d - 1$ power of r in R takes $(\lg n)^{1+o(1)}$ multiplications in R, hence time $(\lg n)^{2+o(1)}$.

There are only $(\lg n)^{o(1)}$ primes q dividing e; computing them in the simplest way takes time $(\lg n)^{2+o(1)}$. Computing the $(n^d-1)/q$ power of r in R takes time $(\lg n)^{2+o(1)}$. Checking whether $r^{(n^d-1)/q}-1$ is a unit in R takes time $(\lg n)^{2+o(1)}$.

Computing s^e in R for each $s \in S$ takes time $(\lg n)^{1+o(1)}$. Checking all the remaining units takes time $(\lg n)^{2+o(1)}$.

Computing the product of binomial coefficients takes time $(\lg n)^{2+o(1)}$. Computing $n^{d\left\lceil\sqrt{e/3}\right\rceil}$ takes time $(\lg n)^{2+o(1)}$.

Multiplying in $R[x]/(x^e-r)$ takes time $(\lg n)^{3+o(1)}$. Computing each $(x-s)^{n^d}$ and $x^{n^d}-s$ in $R[x]/(x^e-r)$ takes $(\lg n)^{1+o(1)}$ multiplications in $R[x]/(x^e-r)$, hence time $(\lg n)^{4+o(1)}$; more precisely, $(\#S)d^2e(\lg n)^2$ times logarithmic factors.

Finally, checking whether n is a perfect power takes time $(\lg n)^{1+o(1)}$.

4. Finding a primality certificate

Assume now that n is prime.

For simplicity, take $S=\{1\}$, $c=0$, $c_-=0$, and $c_+=\lfloor e/2\rfloor$. The inequality in Theorem 2.1 then says, roughly, that 2^e has to exceed $n^{d\sqrt{e/3}}$, i.e., that e has to exceed $d^2(\lg n)^2/3$.

The Adleman-Pomerance-Rumely theorem says that the product of the small primes dividing n^d-1 grows, at a minimum, almost exponentially with d. One can find d (with $n^d \ge 3$) and a divisor e of n^d-1, meeting the inequality in Theorem 2.1, with $e \in (\lg n)^{2+o(1)}$ and $d \in \exp(O(\lg\lg\lg n \lg\lg\lg\lg n))$. Furthermore, this computation can be performed very quickly.

There are two random steps in the construction of a certificate. The first is to find a monic irreducible polynomial f over $\mathbf{Z}/n$ of degree d. One can generate a random f and check whether it has factors in common with $x^n-x, x^{n^2}-x, \ldots, x^{n^{d-1}}-x$; this takes time $(\lg n)^{2+o(1)}$.

The second random step is to find an r in $(\mathbf{Z}/n)[y]/f$ such that $r \ne 1$ and $r^{(n^d-1)/e}$ has order e. One can generate random r's and check the powers $r^{(n^d-1)/q}$ for primes q dividing e. This takes time $(\lg n)^{2+o(1)}$.

The $n, d, e, c, c_-, c_+, f, r, S$ produced by this process is then a certificate for n.

If n is actually composite, this algorithm may fail in various ways. Of course, even if it produces an output $n, d, e, c, c_-, c_+, f, r, S$, that will not be a certificate for n.

A more sophisticated certificate-generation algorithm will produce much faster certificate verification. More comments on certificate optimization in the next draft.

Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois at Chicago, Chicago, IL 60607–7045

E-mail address: `djb@cr.yp.to`