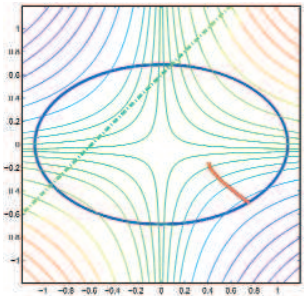
American Mathematical Society

Current Events in Mathematics

An AMS Special Session Organized by AMS President

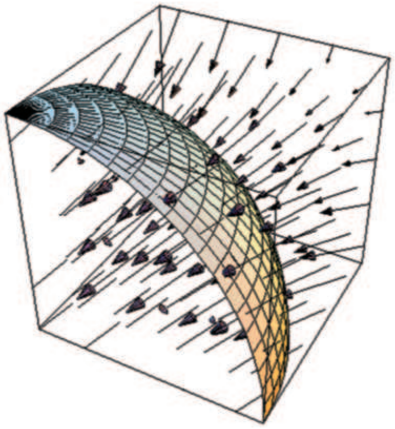
David Eisenbud

Friday, January 9 - 1:00 to 5:10 p.m.
Phoenix Civic Plaza, Room 41



The Interior-Point Revolution in Optimization: History, Recent Developments and Lasting Consequences

MARGARET H. WRIGHT



What Is Motivic Integration?

THOMAS C. HALES

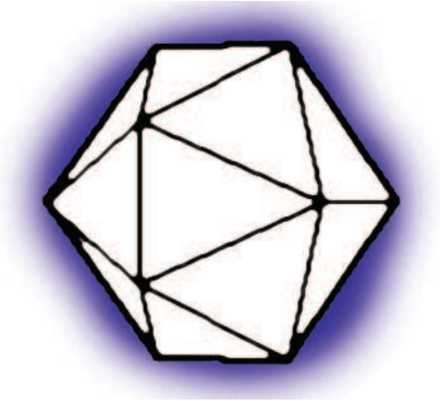
"SEVEN AND A HALF LOGS SHOULD DO IT!"

It Is Easy to Determine Whether or Not a Given Integer Is Prime

ANDREW GRANVILLE

Perelman's Recent Work on the Classification of 3-Manifolds

JOHN W. MORGAN



IT IS EASY TO DETERMINE WHETHER A GIVEN INTEGER IS PRIME

Andrew Granville

Dedicated to the memory of W. 'Red' Alford, friend and colleague.

Abstract. "The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and difficult that even for numbers that do not exceed the limits of tables constructed by estimable men, they try the patience of even the practiced calculator. And these methods do not apply at all to larger numbers ... It frequently happens that the trained calculator will be sufficiently rewarded by reducing large numbers to their factors so that it will compensate for the time spent. Further, *the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated* ... It is in the nature of the problem that *any* method will become more complicated as the numbers get larger. Nevertheless, in the following methods the difficulties increase rather slowly ... The techniques that were previously known would require intolerable labor even for the most indefatigable calculator."

from article 329 of *Disquisitiones Arithmeticae* (1801) by C. F. GAUSS.

In August 2002, three Indian computer scientists, Manindra Agrawal, Neeraj Kayal and Nitin Saxena, constructed a "polynomial time primality test", a much sought-after but elusive goal of researchers in the algorithmic number theory world. Most shocking was the simplicity and originality of their test ... whereas the "experts" had made complicated modifications on existing tests to gain improvements, these authors rethought the direction in which to push the usual ideas with stunning success. Their algorithm is based on the following elegant characterization of prime numbers.

Agrawal, Kayal and Saxena (2004). *For given integer $n \geq 2$, let r be a positive integer for which n has order $> (\log n)^2$ modulo r. Then n is prime if and only if*

- *n is not a perfect power,*
- *n does not have any prime factor $\leq r$,*
- *$(x+a)^n \equiv x^n + a \pmod{(n, x^r - 1)}$ for each integer $a, 1 \leq a \leq \sqrt{r} \log n$.*

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

In this talk we will explain their test, with complete proofs, and put the result and ideas in appropriate historical context. Details will be elaborated on in a forthcoming article.

1.1. Our objective is to find a "quick" foolproof algorithm to determine whether a given integer is prime. Everyone knows *trial division*, when we try to divide n by every integer m in the range $2 \leq m \leq \sqrt{n}$. The number of steps in this algorithm will be at least the number of integers m we consider, which is something like $\sqrt{n}$, in the worst case (when n is prime). Note that $\sqrt{n}$ is roughly $2^{d/2}$ where d is the number of digits of n when written in binary (and d is roughly $(\log n)/(\log 2)$).

The *objective* in this area has been to come up with an algorithm which works in no more than cd^A steps in the worst case, where c and A are some fixed positive constants; that is, an algorithm which works in *Polynomial Time* (which is often abbreviated as $\mathtt{P}$). With such an algorithm one expects that one can rapidly determine whether any "reasonably sized" integer is prime.

Before the work of Agrawal, Kayal and Saxena the fastest algorithm worked in about $d^{\log\log d}$ steps. Their algorithm works in about $d^{7.5}$ steps (and thus "*Seven-and-a-half logs suffice*"); and a modification by Lenstra and Pomerance in about d^6 steps.

1.2. Recognizing primes. Are there ways to recognize primes other than by trial division? One way that comes to mind is by using

Wilson's Theorem (1770). *Integer $n \geq 2$ is prime if and only if n divides $(n-1)!+1$.*

The problem here though is that there is no obvious way to compute $(n-1)!$ rapidly (or even $(n-1)! \pmod{n}$). Another idea is to use

Matijasevič's polynomial (1970). *There exists a polynomial $f(x_1, x_2, \ldots, x_{26}) \in \mathbb{Z}[x_1, x_2, \ldots, x_{26}]$ of degree 25, with the property that the set of positive values $f(m_1, m_2, \ldots, m_{26})$ where $m_1, \ldots, m_{26}$ are all taken to be positive integers, is the same as the set of primes.*

We might hope to somehow quickly identify whether a given integer is a value of f, but no one has yet figured out how.

There are many places that primes come up in the mathematical literature, and many of these might suggest a way to identify primes — some of us who are interested in primality testing always look at anything new that we learn with one eye open to this application. However, for the remainder of this first half of my talk I want to focus on one classical approach.

1.3. Prime numbers have many interesting properties. One of the most amazing is known as

Fermat's Little Theorem (1637). *If n is a prime then n divides $a^n - a$ for all integers a.*

Conversely, if integer n *does not divide* $a^n - a$ for some integer a, then n is composite.

For example[1], taking $a = 2$ we calculate that

$$2^{1001} \equiv 123 \pmod{1001},$$

so we know that 1001 is composite.

We might ask whether this always works. In other words,

Is it true that *if n is composite then n does not divide* $2^n - 2$?

For, if so, we have a very nice way to distinguish primes from composites. Unfortunately the answer is "no" since, for example,

$$2^{341} \equiv 2 \pmod{341},$$

but $341 = 11 \times 31$. Note though that by taking $a = 3$ above we get

$$3^{341} \equiv 168 \pmod{341},$$

so we can use these ideas to prove that 341 is composite.

But then we might ask whether this always works, whether there is always *some* value of a that helps us prove a composite n is indeed composite.

In other words,

Is it true that *if n is composite then there
is some integer a for which n does not divide $a^n - a$?*

Again the answer is "no" since 561 divides $a^{561} - a$ for all integers a, yet $561 = 3 \times 11 \times 17$. Composite integers n which divide $a^n - a$ for all integers a are called *Carmichael numbers*, $561, 1105$ and 1729 being the smallest three examples. Carmichael numbers are a nuisance, masquerading as primes like this, though computationally they only appear rarely. Unfortunately it was recently proved that there are infinitely many of them, and that when we go out far enough they are not so rare as it first appears.

1.4. Square Roots. In a field, a non-zero polynomial of degree d has at most d roots. For the particular example $x^2 - 1$ this implies that 1 has just two squareroots mod p, a prime > 2, namely 1 and -1.

If we consider odd composite n then we quickly find $1^2 \equiv 4^2 \equiv 11^2 \equiv 14^2 \pmod{15}$, that is, there are four squareroots of 1 $\pmod{15}$. In general if odd n is divisible by two distinct primes then we have *at least* four distinct squareroots of 1 $\pmod{n}$. Thus we might try to prove n is composite by finding a squareroot of 1 $\pmod{n}$, which is neither 1 nor -1.

Now, by Fermat's Little Theorem, if p is prime then $(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \pmod{p}$, so $a^{\frac{p-1}{2}} \pmod{p}$ is a squareroot of 1 $\bmod p$ and must be 1 or -1. Therefore if $a^{\frac{n-1}{2}} \pmod{n}$ is neither 1 nor -1 then n is composite. Let's try an example: We have $64^{948} \equiv 1 \pmod{949}$, and the squareroot $64^{474} \equiv 1 \pmod{949}$. Hmmmm, we failed to prove 949 is

[1] A few definitions for the uninitiated: We say that $a \equiv b \pmod{m}$ if and only if m divides $b - a$; the main advantage of this notation is that we can do most regular arithmetic operations $\pmod{m}$. The *order* of $n \pmod{m}$ is the least positive integer k for which $n^k \equiv 1 \pmod{m}$.

composite like this but, wait a moment, since 474 is even so we can take the squareroot again, and a calculation reveals that $64^{237} \equiv 220 \pmod{949}$, so that 949 is composite. In general, integer a is a *witness* to n being composite if the finite sequence

$$a^{n-1} \pmod{n},\ a^{(n-1)/2} \pmod{n}, \ldots,\ a^{(n-1)/2^u} \pmod{n}$$

(where $n-1 = 2^u v$ with v odd) is not equal to either $1, 1, \ldots, 1$ or $1, 1, \ldots, 1, -1, *, \ldots, *$.

It is known that, for all odd composite n, at least three-quarters of the integers a, $1 \leq a \leq n$ are witnesses for n. So can we find a witness "quickly" if n is composite?

- One idea is to try $a = 2, 3, 4, \ldots$ consecutively until we find a witness. We believe that there is a witness $\leq 2(\log n)^2$, though we cannot prove this except under the assumption of a big tool, the Generalized Riemann Hypothesis.

- Pick integers a in $\{1, 2, 3, \ldots, n\}$ at random until we find a witness. By what we wrote above, if n is composite then the probability that none of the first k integers chosen are witnesses is $< 1/4^k$. Thus with a hundred or so such tests we get a probability that is so small that it is inconceivable that it could occur in practice; so we believe that any integer n for which none of a hundred randomly chosen a's is a witness, is prime. We call such n "*industrial strength primes*".

The big problem with the above method is that although we strongly believe that an industrial strength prime is indeed a prime, we have no proof, and mathematicians like proof. Indeed if you claim such integers are prime, without proof, then a cynic might not believe that your randomly chosen a are so random, or that you are unlucky, or ... No, what we need is a proof that a number is prime when we think that it is.

1.5. Proofs and the complexity class NP.

At the 1903 meeting of the American Mathematical Society, F.N. Cole came to the blackboard and without a word wrote down

$$2^{67} - 1 = 193707721 \times 761838257287,$$

long-multiplying the numbers out on the right side of the equation, and determining the decimal expansion of $2^{67} - 1$ to prove that he was indeed correct. Afterwards he said that figuring this out had taken him "three years of Sundays". The moral of this tale is that although it took Cole a great deal of work and perseverance to find these factors, it did not take him long to justify his result to a room full of mathematicians (and, indeed, to give a proof that he was correct). Thus we see that one can provide a short proof, even if finding that proof takes a long time.

In general one can exhibit factors of a given integer n to give a short proof that n is composite (such proofs are called *certificates*). By "short" we mean that the proof can be verified in polynomial time, and we say that such problems are in class NP ("*non-deterministic polynomial time*[2]"). We are not suggesting that the proof can be found in polynomial time, only that the proof can be checked in polynomial time; indeed we have

[2] Note that NP is **not** "non-polynomial time", a common source of confusion.

no idea whether it is possible to factor numbers in polynomial time, and this is now the outstanding problem of this area.

What about primality testing? If someone gives you an integer and asserts that it is prime, can you check that this is so is in polynomial time? Can they give you better evidence than their say-so that it is a prime number? Can they provide some sort of "certificate" that gives you all the information you need to verify that the number is indeed a prime? It is not, as far as I can see, obvious how to do so; certainly not as obvious as with the factoring problem. It turns out that some old remarks of Lucas from the 1870's can be modified for this purpose:

First note that n is prime if there are precisely $n-1$ integers a in the range $1 \leq a \leq n-1$ which are coprime to n. Therefore if we can show the existence of $n-1$ such integers then we have a proof that n is prime. In fact if n is prime then these values form a cyclic group, and so have a generator g; that is, there exists an integer g for which $1, g, g^2, \ldots, g^{n-2}$ are all coprime to n and distinct mod n. Thus to show that n is prime we need simply exhibit g and prove that these numbers are distinct mod n. In fact g is a generator if and only if g has order $n-1 \pmod{n}$. It can be shown that any such order must divide $n-1$, and so one can show that if g is not a generator then $g^{(n-1)/q} \equiv 1 \pmod{p}$ for some prime q dividing $n-1$. Thus a "certificate" to show that n is prime would consist of g and $\{q$ prime $: q$ divides $n-1$ $\}$, and the checker would need to verify that $g^{n-1} \equiv 1 \pmod{n}$ whereas $g^{(n-1)/q} \not\equiv 1 \pmod{p}$ for all primes q dividing $n-1$, something that can be accomplished in polynomial time.

There is a problem though: One needs certification that each such q is prime. The solution is to iterate the above algorithm; and one can show that no more than $(\log n)/(\log 2)$ odd primes need to be certified after one has iterated all the way down. Thus we have a polynomial time certificate (short proof) that n is prime, and so primality testing is in the class NP.

But isn't this the algorithm we seek? Doesn't this give a polynomial time algorithm for determining whether a given integer n is prime? The answer is "no" because along the way we would have to factor $n-1$ quickly, something no-one knows how to do.

1.6. Random polynomial time algorithms.

In section 1.4 we introduced the notion of "industrial strength primes". In fact if our given integer is composite then there is a probability of at least 1/2 that each application of that "witness" test succeeds in providing a short certificate verifying that the number is composite (the certificate provides a witness a). This is a *random polynomial time* test for compositeness (complexity class RP). As we noted it is almost certain to provide such a proof in 100 runs of the test if n is indeed composite, so if it fails then it is very likely that n is prime. Our main objection was that this doesn't provide a proof that n is prime.

One objective, just short of finding a polynomial time test for primality, is to find a random polynomial time test for primality. This was achieved by Adleman and Huang in 1992 using a method of counting points on elliptic and hyperelliptic curves over finite fields (based on ideas of Goldwasser and Kilian). Although beautiful in structure, their test is very complicated and almost certainly impractical, as well as being rather difficult to justify theoretically in all its details. It does however provide a short certificate verifying that a given prime is prime, and proves that primality testing is in complexity class RP.

1.7. An old beginning.

The new work of Agrawal, Kayal and Saxena is much simpler than many of the more recent developments in this subject. Their starting point is the following result, which is good exercise for an elementary number theory course.

Theorem 1. *Integer n is prime if and only if $(x+1)^n \equiv x^n + 1 \pmod{n}$ in $\mathbb{Z}[x]$.*

Proof. Since $(x+1)^n - (x^n+1) = \sum_{1\le j\le n-1} \binom{n}{j} x^j$, we have that $x^n + 1 \equiv (x+1)^n \pmod{n}$ if and only if n divides $\binom{n}{j}$ for all j in the range $1 \le j \le n-1$. If $n = p$ is prime then p appears in the numerator of $\binom{p}{j}$ but is larger than, and so does not divide, any term in the denominator.

If n is composite let p be a prime dividing n. In the expansion $\binom{n}{p} = n(n-1)(n-2)\dots(n-(p-1))/p!$ we see that the only terms p divides are the n in the numerator and the p in the denominator, and so if p^k is the largest power of p dividing n then p^{k-1} is the largest power of p dividing $\binom{n}{p}$; and therefore n does not divide $\binom{n}{p}$. □

This simple theorem is the basis of the new primality test: Why don't we compute $(x+1)^n - (x^n+1) \pmod{n}$ and determine whether or not n divides each coefficient? This is a valid primality test, but computing $(x+1)^n \pmod{n}$ is obviously slow since it will involve storing n coefficients!

Since our difficulty is that the answer here involves many coefficients (as the degree is so high), one idea is to compute mod some small degree polynomial as well as mod n, so that neither the coefficients nor the degree get large. The simplest polynomial of degree r is perhaps $x^r - 1$. So we could verify whether

$$(x+1)^n \equiv x^n + 1 \pmod{(n, x^r - 1)}.$$

This can be computed rapidly, and it is true for any prime n (as a consequence of the theorem above), but it is unclear whether this fails for all composite n and thus provides a primality test. The main theorem (at the start of the talk) provides a modification of this congruence, which can be shown to succeed for primes and fail for composites, thus providing a polynomial time primality test. In the second part of our talk we shall investigate this in detail.

1.Appendix. Fast Exponentiation.

An astute reader might ask how we can raise something to the nth power "quickly" (where by "quickly" we mean that the number of steps is bounded by a power of $\log n$). This problem was beautifully solved by computer scientists long ago:

We wish to compute $(x+a)^n \pmod{(n, x^r-1)}$ quickly. Define $f_0(x) = (x+a)$ and then $f_{j+1}(x) \equiv f_j(x)^2 \pmod{(n, x^r-1)}$ for $j \ge 0$ (at each step we determine $f_j(x)^2$ and then reduce mod $x^r - 1$ so the degree of the resulting polynomial is $< r$, and then reduce mod n to obtain f_{j+1}). Note that $f_j(x) \equiv (x+a)^{2^j} \pmod{(n, x^r-1)}$.

Writing n in binary, say as $n = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_\ell}$ with $a_1 > a_2 > \cdots > a_\ell \geq 0$, let $g_1(x) = f_{a_1}(x)$ and then $g_j(x) \equiv g_{j-1}(x) f_{a_j}(x) \pmod{(n, x^r - 1)}$ for $j = 1, 2, \ldots, \ell$. Therefore

$$g_\ell(x) \equiv (x+a)^{2^{a_1}+2^{a_2}+\cdots+2^{a_\ell}} = (x+a)^n \pmod{(n, x^r - 1)}.$$

Thus we have computed $(x+a)^n \pmod{(n, x^r - 1)}$ in $a_1 + \ell \leq 3 \log n$ such steps, where a step involves multiplying two polynomials of degree $< r$ with coefficients in $\{0, 1, \ldots, n-1\}$, and reducing $\pmod{(n, x^r - 1)}$.

2. Proof of the Theorem. The AKS algorithm

In the second half of the talk we will prove the theorem of Agrawal, Kayal and Saxena. We will assume that we are given an odd integer n which we know is not a perfect power, and has no prime factor $\leq r$. For simplicity we will assume that n has order $> 9(\log n)^2$ modulo r, and that[3]

$$(x+a)^n \equiv x^n + a \pmod{(n, x^r - 1)} \tag{1}$$

for each integer $a, 1 \leq a \leq A$ where we take $A = 3\sqrt{r} \log n$. (One can replace each of the constants “9” and “3” by “1” with extra work). By Theorem 1 we know that these hypotheses hold if n is prime, so we must show that they cannot hold if n is composite.

Let p be a prime dividing n. We can factor $x^r - 1$ into irreducibles in $\mathbb{Z}[x]$, as $\prod_{d|r} \Phi_r(x)$, where $\Phi_r(x)$ is the rth cyclotomic polynomial, whose roots are the primitive rth roots of unity. Let $h(x)$ be an irreducible factor of $\Phi_r(x) \pmod{p}$. Then (1) implies that

$$(x+a)^n \equiv x^n + a \pmod{(p, h(x))} \tag{2}$$

for each integer $a, 1 \leq a \leq A$, since $(p, h(x))$ divides $(n, x^r - 1)$.

The congruence classes $\pmod{(p, h(x))}$ are really the elements of the ring $\mathbb{Z}[x]/(p, h(x))$, which is isomorphic to the field of p^m elements (where m is the degree of h). In particular the non-zero elements form a cyclic group of order $p^m - 1$. (Below it will be occasionally convenient to suppress the “mod” notation.)

Let G be the (cyclic) subgroup generated by $x+1, x+2, \ldots, x+A$. Notice that if $g(x) = \prod_{1 \leq a \leq A} (x+a)^{e_a} \in G$ then

$$g(x)^n = \prod_a ((x+a)^n)^{e_a} \equiv \prod_a (x^n + a)^{e_a} = g(x^n) \pmod{(p, h(x))}.$$

We define S to be the set of integers k for which $g(x^k) = g(x)^k$ for all $g \in G$. Note that $p, n \in S$.

Our plan is to give upper and lower bounds on the size of G to establish a contradiction.

2.1. Upper bounds on $|G|$.

[3] We write $f(x) \equiv g(x) \pmod{(m, h(x))}$ where m is an integer and $f(x), g(x), h(x) \in \mathbb{Z}[x]$ if there exists $u(x), v(x) \in \mathbb{Z}[x]$ for which $f(x) - g(x) = m u(x) + h(x) v(x)$

Lemma 1. *If $a, b \in S$ then $ab \in S$.*

Proof. (Here we work in the ring $\mathbb{Z}[x]/(p, h(x)))$. If $g(x) \in G$ then $g(x^a) = g(x)^a \in G$ since G is a group. Therefore $g((x^a)^b) = g(x^a)^b$ as $b \in S$ and so

$$g(x)^{ab} = (g(x)^a)^b = g(x^a)^b = g((x^a)^b) = g(x^{ab}).$$

Lemma 2. *If $a, b \in S$ and $a \equiv b \mod r$ then $a \equiv b \mod |G|$.*

Proof. For any $g(x) \in \mathbb{Z}[x]$ we have that $u-v$ divides $g(u)-g(v)$. Therefore $x^r - 1$ divides $x^{a-b} - 1$, which divides $x^a - x^b$, which divides $g(x^a) - g(x^b)$. Reducing mod p, so that $h(x)$ divides $x^r - 1$, we deduce that $g(x)^a = g(x^a) = g(x^b) = g(x)^b$ in $\mathbb{Z}[x]/(p, h(x))$ for all $g \in G$, and so $g(x)^{a-b} = 1$ for all $g \in G$. Now G is a cyclic group, so taking g to be a generator of G we deduce that $|G|$ divides $a - b$.

Let R be the subgroup of $(\mathbb{Z}/r\mathbb{Z})^*$ generated by n and p. Since n is not a power of p, the integers $n^i p^j$ with $i, j \geq 0$ are distinct. There are $> |R|$ such integers with $0 \leq i, j \leq \sqrt{|R|}$ and so two must be congruent $\pmod r$, say

$$n^i p^j \equiv n^I p^J \pmod r.$$

By Lemma 1 these integers are both in S. By Lemma 2 their difference is divisible by $|G|$, and therefore

$$|G| \leq |n^i p^j - n^I p^J| \leq (np)^{\sqrt{|R|}} \leq n^{2\sqrt{|R|}}. \tag{3}$$

2.2. Lower bounds on $|G|$.

We wish to show that there are many distinct elements of G. If $f(x), g(x) \in \mathbb{Z}[x]$ with $f(x) \equiv g(x) \pmod{(p, h(x))}$ then we can write $f(x) - g(x) \equiv h(x)k(x) \mod p$ for some polynomial $k(x) \in \mathbb{Z}[x]$. Thus if f and g both have smaller degree than h then $k(x) \equiv 0 \pmod p$ and so $f(x) \equiv g(x) \pmod p$. Thus all polynomials of the form $\prod_{1 \leq a \leq A}(x-a)^{e_a}$ of degree $< m$ (the degree of $h(x)$) are distinct elements of G, and this gives a lower bound for G. One can show that m is the order of $p \pmod r$ and so if one can show that this value is large then we can get good lower bounds on G.

This was what Agrawal, Kayal and Saxena did in their first preprint, and to prove such r exist they needed to use deep tools of analytic number theory. In their second preprint, inspired by a remark of Lenstra, they were able to replace m by $|R|$ in this result, which allows them to give an entirely elementary proof of their theorem, and to get a stronger result when they do invoke the deeper estimates.

Lemma 3. *Suppose that $f(x), g(x) \in \mathbb{Z}[x]$ with $f(x) \equiv g(x) \pmod{(p, h(x))}$, and $f, g \in G$. If f and g both have degree $< |R|$ then $f(x) \equiv g(x) \pmod p$.*

Proof. Let $\Delta(y) := f(y) - g(y)$. If $k \in S$ then

$$\Delta(x^k) = f(x^k) - g(x^k) \equiv f(x)^k - g(x)^k \equiv 0 \pmod{(p, h(x))}.$$

It can be shown that x has order r mod $(p, h(x))$ so that $\{x^k : \ k \in R\}$ are all distinct roots of $\Delta(y)$ mod $(p, h(x))$. Now, $\Delta(y)$ has degree $< |R|$, but $\geq |R|$ distinct roots mod $(p, h(x))$, and so $\Delta(y) \equiv 0$ mod $(p, h(x))$, which implies that $\Delta(y) \equiv 0 \pmod p$ since its coefficients are independent of x.

By definition R contains all the elements generated by $n \pmod r$, and so R is at least as large as the order of $n \pmod r$, which is $> 9(\log n)^2$ by assumption. Therefore A, $|R| > B$, where $B := [3\sqrt{|R|}\log n]$. Lemma 3 implies that the products $\prod_{a \in T}(x+a)$ for every $T \subset \{1, 2, \dots, B\}$ give distinct elements of G, and so

$$|G| \geq 2^B > n^{2\sqrt{|R|}}$$

since $2^3 > e^2$, which contradicts (3). This completes the proof of the theorem of Agrawal, Kayal and Saxena.

2.3. Running time.

One can write an algorithm (using standard techniques) to test the steps of the theorem of Agrawal, Kayal and Saxena, which runs in roughly $r^{3/2}(\log n)^3$ steps (bit operations).

We must have $r > (\log n)^2$ since n must have order $> (\log n)^2$ mod r; and thus we would not expect the AKS algorithm to run in much fewer than $(\log n)^6$ steps. It is expected that there exists a prime r in $[1 + (\log n)^2, 2(\log n)^2]$ for which n is a primitive root $\pmod r$, and thus has order[4] $r - 1$ mod r. Therefore we expect (and it is borne out in practice) that we have a running time of around $(\log n)^6$. However we cannot **prove** that such r exist.

In the next section we will give an elementary proof that such an r exists with r around $(\log n)^5$, which thus leads to a running time of around $(\log n)^{10\frac{1}{2}}$ (since $10\frac{1}{2} = \frac{3}{2} \times 5 + 3$).

In the accompanying article I will show how basic tools of analytic number theory can be used to show that such an r exists with r around $(\log n)^{24/7}$ (using an old argument of Goldfeld), which leads to a running time of around $(\log n)^{8\frac{1}{7}}$

Using much deeper tools, a result of Fouvry[5] implies that such an r exists with r around $(\log n)^3$, which leads to a running time of around $\ll (\log n)^{7\frac{1}{2}}$. This can be improved using a recent result of Baker and Harman to $(\log n)^{7.49}$.

2.4. Large orders mod r.

The prime number theorem can be paraphrased as: *The product of the primes up to x is roughly e^x.* A weak explicit version states that the product of the primes between N and $2N$ is $\geq 2^N$ for all $N \geq 1$.

Lemma 4. *If $n \geq 6$ then there is a prime $r \in [(\log n)^5, 2(\log n)^5]$ for which the order of n mod r is $> (\log n)^2$.*

[4] In fact, it should suffice to restrict attention to primes r for which $(r-1)/2$ is also prime.

[5] Fouvry's 1984 result was at the time immediately applied to prove a result about Fermat's Last Theorem (then an open problem). In the accompanying article we will see how other tools developed to attack Fermat's Last Theorem can be used on the problem here.

Proof. If not, then the order of n mod r is $\leq I := (\log n)^2$ for every prime $r \in [N, 2N]$ with $N := (\log n)^5$, so that their product divides $\prod_{i \leq I}(n^i - 1)$. But then

$$2^N \leq \prod_{N \leq r \leq 2N} r \leq \prod_{i \leq I}(n^i - 1) < n^{\sum_{i \leq I} i} < 2^{(\log n)^5},$$

for $n \geq 6$, giving a contradiction.

The bound on r here holds for all $n \geq 6$, and thus using this bound our running time analysis of AKS is *effective*; that is, one can explicitly bound the running time of the algorithm for all $n \geq 6$. In the better bounds on r discussed in the previous section, the proofs are not effective, in that they do not imply how large n must be in order for the given upper bound for r to hold.

3. Even more recent developments

Can we achieve the feasible $(\log n)^6$ running time? One approach is to achieve better lower bounds on the size of G (than were obtained in section 2.2): Although this has not yet been done in a way to achieve our goal, Voloch had the beautiful idea that one can bound how often different high degree products of $(x + a)$ can be equal $\pmod{(p, h(x))}$ by using the *abc*-theorem for polynomials. However this goal has now been achieved in a different manner: Lenstra and Pomerance have extended the idea in AKS (with extra complications) to obtain the desired running time of around $(\log n)^6$ steps, as we will discuss in the next section.

Following up on ideas of Berrizbeitia, Bernstein has modified AKS to obtain an algorithm that runs in around $(\log n)^4$ steps, but which only succeeds half the time in providing a certificate of primality; in other words this is an RP algorithm for primality testing which is faster, easier and more elegant than that of Adleman and Huang. In practice this makes the original AKS algorithm irrelevant. For if we run the "witness" test, which is an RP algorithm for compositeness, by day, and run the AKS-Berrizibeita-Bernstein RP algorithm for primality by night, then a number n is, in practice, certain to yield its secrets faster (in around $(\log n)^4$ steps) than by the original AKS algorithm!

3a. Stop the press: Lenstra and Pomerance achieve the desired running time. Lenstra and Pomerance replace the polynomial $\Phi_r(x)$ in AKS by a polynomial $f(x)$ with certain properties: If $f(x)$ is a monic polynomial of degree m with integer coefficients and n is a positive integer for which

- $f(x^n) \equiv 0 \text{ mod } (n, f(x))$,
- $x^{n^m} - x \equiv 0 \text{ mod } (n, f(x))$,
- $x^{n^{m/q}} - x$ is a unit in $\mathbb{Z}[x]/(n, f(x))$ for all primes q dividing m,

then we say that $\mathbb{Z}[x]/(n, f(x))$ is a *pseudofield*. When n is prime and $f(x)$ is irreducible mod n then these criterion are all true, and $\mathbb{Z}[x]/(n, f(x))$ is a field.

Lenstra and Pomerance. *For given integer $n \geq 2$ let m be a positive integer $> 4(\log n)^2$ for which there exists a monic polynomial $f(x)$ of degree m with integer coefficients, such that $\mathbb{Z}[x]/(n, f(x))$ is a pseudofield. Then n is prime if and only if*

- *n is not a perfect power,*
- *n does not have any prime factor $\leq A := 2\sqrt{m}\log n$,*
- *$(x+a)^n \equiv x^n + a \bmod (n, f(x))$ for each integer $a, 1 \leq a \leq A$.*

Evidently for a given f one can quickly determine whether one gets a pseudofield, and if so check the criteria of the theorem. Thus if we can quickly find an f which gives a pseudofield this approach will lend itself to a quick primality test. Lenstra and Pomerance's construction of f comes back full circle to Gauss's *Disquisitiones*, and his construction of regular n-gons, in particular what are now known as "Gaussian periods". For $M := 4(\log n)^2$ their polynomial has degree $q_1 q_2 \dots q_k \in (M, 4M]$ where the q_i are coprime positive integers for which there exists a prime $r_i \leq M$ such that $n^{(r_i-1)/q_i}$ has order q_i mod r_i for each i. They show how to determine these numbers, and thus f, in less than $(\log n)^3$ bit operations, once n is bigger than some n_0, which can be effectively determined.

References

1. Leonard M. Adleman and Ming-Deh A. Huang, *Primality testing and abelian varieties over finite fields*, Lecture Notes in Mathematics, vol. 1512, Springer-Verlag, Berlin.
2. Leonard M. Adleman, Carl Pomerance and Robert S. Rumely, *On distinguishing prime numbers from composite numbers*, Annals of Mathematics **117** (1983), 173–206.
3. Manindra Agrawal, Neeraj Kayal and Nitin Saxena, *PRIMES is in P* (to appear).
4. W. R. Alford, Andrew Granville and Carl Pomerance, *There are infinitely many Carmichael numbers*, Annals of Mathematics **139** (1994), 703–722.
5. Roger C. Baker and Glynn Harman, *The Brun-Titchmarsh Theorem on average*, Progr. Math. **138,** (1996), 39-103.
6. D. J. Bernstein, *Proving primality in essentially quartic random time* (to appear).
7. Pedro Berrizbeitia, *Sharpening "PRIMES is in P" for a large family of numbers* (to appear).
8. Richard Crandall and Carl Pomerance, *Prime numbers. A computational perspective*, Springer-Verlag, New York, 2001.
9. Etienne Fouvry, *Theoreme de Brun-Titchmarsh; application au theoreme de Fermat*, Invent. Math **79** (1985), 383–407.
10. Dorian M. Goldfield, *On the number of primes p for which p+a has a large prime factor*, Mathematika **16** (1969), 23-27.
11. Shafi Goldwasser and Joe Kilian, *Almost all primes can be quickly certified*, Proceedings of the 18th annual ACM symposium on theory of computing, Association for Computing Machinery, New York, 1986.
12. Donald E. Knuth, *The art of computer programming, volume 2: Seminumerical algorithms*, Addison-Wesley, Reading, 1969.
13. H.W. Lenstra, Jr. and Carl Pomerance, *Primality testing with Gaussian periods* (to appear).
14. Yu. V. Matijasevich, *Hilbert's Tenth Problem.*, MIT Press, Cambridge, MA, 1993.
15. Paulo Ribenboim, *The new book of prime number records*, Springer-Verlag, New York, 1995.
16. José Felipe Voloch, *On some subgroups of the multiplicative group of finite rings* (to appear).

Département de Mathématiques et statistique, Université de Montréal, CP 6128 succ. Centre-Ville, Montréal QC H3C 3J7, Canada

E-mail address: andrew@dms.umontreal.ca