News from India

There can be no question that *the* "News from India" these past three months has been the result by Agrawal, Kayal and Saxena that testing primality can be done in polynomial time. Here is a detailed account of the result by Jaikumar Radhakrishnan from TIFR, Mumbai.

Madhavan Mukund <madhavan@cmi.ac.in>
Chennai Mathematical Institute

Primes is in P

On 4 August 2002, an email message from Manindra Agrawal, Neeraj Kayal and Nitin Saxena left the computers of the Indian Institute of Technology, Kanpur. The subject line read "Primes is in P", and attached to the message was a paper with the same title. This made News.

The paper presented a polynomial time algorithm for recognizing prime numbers, solving a longstanding open problem in Complexity Theory, and passing a milestone in the centuries-old journey towards understanding prime numbers.

We describe below a version of the algorithm of Agrawal, Kayal and Saxena, and sketch a proof of correctness.

We want a polynomial-time method to determine if a given number n is prime, that is, a method that terminates after performing $O((\log n)^c)$ steps of computation. The starting point of the new test for primality is the following.

Proposition 1 *(a) If n is prime, then $(X-a)^n = X^n - a \pmod n$.*

(b) If $\gcd(a,n) = 1$ and n is composite, then $(X-a)^n \neq X^n - a \pmod n$.

Proof: (Sketch) (a) If n is prime $\binom{n}{i} = 0 \pmod n$ for $i = 1, 2, \ldots, n-1$ and $a^n = a \pmod n$. (b) If n is composite and p is a prime factor of n, then the coefficient of X^p in $(X-a)^n$, is $\binom{n}{p}(-a)^{n-p} \neq 0 \pmod n$. □

This proposition gives us the following algorithm.

If $(X-1)^n = X^n - 1 \pmod n$, then n is prime, otherwise it is composite.

Figure 1: A primality testing algorithm

This algorithm classifies numbers correctly as prime and composite; unfortunately, it cannot be implemented efficiently. There are two difficulties. First, the

If n is a k-bit number, then for $i = 0, 1, 2, \ldots, k$, compute $b_i = (X-1)^{2^i} \pmod{n}$ by repeated squaring, starting from $b_0 = X - 1$. Let $n = \sum_{j=0}^{k} \epsilon_i 2^i$, $\epsilon_i \in \{0, 1\}$ be the binary expansion of n. Then, $(X-1)^n = \prod_{i=0}^{k} b_i^{\epsilon_i}$.

Figure 2: Powering by repeated squaring

straightforward method for computing the polynomial $(X-1)^n$, requires $n-1$ multiplications, and we are allowing ourselves only $O((\log n)^c)$ time. This is not a serious problem. It is well-known that one can compute powers more efficiently by repeated squaring (see Figure 2). Interestingly, the use of repeated squaring for computing powers seems to have originated in India, but in the absence of email, it took some time for the word to get around[1].

The second problem with the algorithm of Figure 1, and this is more serious, is that the polynomial $(X-a)^n$ has too many coefficients, potentially $n+1$, and computing such a polynomial even by the repeated squaring, is not feasible in $O((\log n)^c)$ steps. The key idea in the new primality test is to perform computations modulo a polynomial of small degree. This way, the number of coefficients in the polynomial stays small.

Input: An integer $n \geq 2$.

Step 1: If n is of the form a^b, for integers $a, b \geq 2$, then n is composite.

Step 2: Choose the smallest prime r, so that r does not divide n, and the order of n modulo r is divisible by a prime $q \geq \lfloor 2\sqrt{r} \log n \rfloor + 2$. Let $\ell = \lfloor 2\sqrt{r} \log n \rfloor + 1$.

Step 3: For $a = 2, 3, \ldots, \ell$, if a divides n, then n is composite.

Step 4: For $a = 1, 2, \ldots, \ell$, if $(X-a)^n \neq X^n - a \pmod{X^r - 1, n}$, then n is composite.

Step 5: If n has not been declared composite by the earlier steps, then n is prime.

Figure 3: The new primality testing algorithm of Agrawal, Kayal and Saxena

[1]Knuth says: The method is quite ancient; it appeared before 200 B.C. in Pingala's Hindu classic Chandah-sutra [see B. Datta and A.N. Singh, *History of Hindu Mathematics* **2** (Lahore: Motilal Banarsi Das, 1935), 76]. There seems to be no other reference to this method outside of India during the next 1000 years, but a clear discussion of how to compute 2^n efficiently for arbitrary n was given by al-Uqlidisi of Damascus in A.D. 952; see *The Arithmetic of al-Uqlidisi* by A.S. Saidan (Dordrecht: D. Reidel, 1975), 341–342, where the general ideas are illustrated for $n = 51$.

To implement Step 2, we try all primes, starting from 2, one after the other. If at any stage we discover a non-trivial divisor of n, we declare that n is composite. It can be shown that for all large n, the prime r in Step 2, can be chosen to be $O((\log n)^6)$. We refer the reader to the original paper for a justification of this claim, which is based on a theorem due to Fouvry (1985). Assuming this, it is straightforward to check that this algorithm runs in polynomial-time. We will concentrate only on showing that this algorithm is correct.

The proof of correctness

It is easy to verify, using Proposition 1, that if n is prime, this algorithm will never declare that it is composite. So, we only need to argue that composite numbers are not declared prime. Compare Step 4 to the inefficient primality test of Figure 1. The only difference is that we are now performing the computations modulo $X^r - 1$. The main danger in this is that even if $(X-a)^n \neq X^n - a \pmod{n}$, it could be that $(X-a)^n = X^n - a \pmod{X^r - 1, n}$. To compensate for this, we now verify the identity for ℓ different values of a, instead of trying just one value, namely 1. The main point of the Agrawal, Kayal and Saxena paper is that this is adequate compensation.

To see this, let us assume the opposite and show that this leads to a contradiction.

Assumption: n is a composite number and the algorithm of Figure 3 declares that it is prime.

Because the number n passes all tests in Step 4, we know that

$$\text{for } a = 1, 2, \ldots, \ell,\ (X-a)^n = X^n - a \pmod{X^r - 1, n}. \tag{1}$$

Note that in the above identity we can replace the n in $(\text{mod } X^r - 1, n)$ by any divisor of n. Let p be a prime divisor of n. [Most of our discussion is valid for any prime divisor of n. In the end we will choose a special prime divisor of n based on the conditions established in Step 2.] Then, we have

$$\text{for } a = 1, 2, \ldots, \ell,\ (X-a)^n = X^n - a \pmod{X^r - 1, p}. \tag{2}$$

Since p is prime, we always have (see Proposition 1(a))

$$\text{for } a = 1, 2, \ldots, \ell,\ (X-a)^p = X^p - a \pmod{X^r - 1, p}. \tag{3}$$

We thus see that the numbers n and p satisfy similar identities in (2), (3).

Claim 1 *Suppose*

$$\begin{aligned} (X-a)^{m_1} &= X^{m_1} - a \pmod{X^r - 1, p} \text{ and} \\ (X-a)^{m_2} &= X^{m_2} - a \pmod{X^r - 1, p}. \end{aligned}$$

Then, $(X-a)^{m_1 m_2} = X^{m_1 m_2} - a \pmod{X^r - 1, p}$.

Proof: The second assumption says that $(X-a)^{m_2} - (X^{m_2}-a) = (X^r-1)g(X) \pmod{p}$, for some polynomial $g(X)$. By substituting X^{m_1} for X in this identity, we get

$$(X^{m_1}-a)^{m_2} - (X^{m_1 m_2}-a) = (X^{m_1 r}-1)g(X^{m_1}) \pmod{p}.$$

Since $X^r - 1$ divides $X^{m_1 r} - 1$, this shows that $(X^{m_1}-a)^{m_2} = X^{m_1 m_2} - a \pmod{X^r-1, p}$. Using this and the first assumption, we obtain

$$(X-a)^{m_1 m_2} = (X^{m_1}-a)^{m_2} = X^{m_1 m_2} - a \pmod{X^r-1, p}.$$

□

Now starting from (2) and (3), and repeatedly applying the above claim, we see that for each m of the form $p^i n^j$, $(i, j \geq 0)$, we have $(X-a)^m = X^m - a \pmod{X^r-1, p}$, for $a = 1, 2, \ldots, \ell$. (The case $i, j = 0$ corresponds to $m = 1$, and is trivially true.)

Consider the list $L = (p^i n^j : 0 \leq i, j \leq \lfloor \sqrt{r} \rfloor)$. This list has $(\sqrt{r}+1)^2 > r$ numbers. Thus, we have two numbers in the list that are congruent modulo r. Let these numbers be $m_1 = p^{i_1} n^{j_1}$ and $m_2 = p^{i_2} n^{j_2} = m_1 + kr$, where $(i_1, j_1) \neq (i_2, j_2)$. From now on we will concentrate on just these two elements of the list. Since $X^r = 1 \pmod{X^r-1}$, we have $(X-a)^{m_2} = X^{m_1+kr} - a = X^{m_1} - a = (X-a)^{m_1} \pmod{X^r-1, p}$. That is,

$$\text{for } a = 1, 2, \ldots, \ell, \ (X-a)^{m_1} = (X-a)^{m_2} \pmod{X^r-1, p}. \tag{4}$$

Claim 2 $m_1 = m_2$.

We will prove this claim below. Let us first complete the proof of correctness by assuming this claim. From this claim and the definition of m_1 and m_2 we see that $p^{i_1} n^{j_1} = p^{i_2} n^{j_2}$. Since $(i_1, j_1) \neq (i_2, j_2)$ and p is prime, this implies that n is a power of p. That is $n = p^s$ for some s. If $s \geq 2$, Step 1 of the algorithm would already have declared that n is composite. This contradicts our assumption that the algorithm declares that n is prime. On the other hand, if $s = 1$, then n is prime, again contradicting our assumption that n is composite. We have proved that the algorithm is correct assuming Claim 2.

Proof of Claim 2: Let $h(X)$ be an irreducible factor of $(X^r-1)/(X-1)$. Then, from (4) we see that

$$\text{for } a = 1, 2, \ldots, \ell, \ (X-a)^{m_1} = (X-a)^{m_2} \pmod{h(X), p}. \tag{5}$$

That is, each element of the field $\mathbb{F}_p[X]/(h(X))$ of the form $X - a$ satisfies the equation $Z^{m_1} - Z^{m_2} = 0$. Note that if e_1 and e_2 are two elements that satisfy this equation, then $e_1 e_2$ also satisfies this equation. Thus, each element of the set

$$S = \left\{ \prod_{a=1}^{\ell} (X-a)^{\alpha_a} : \alpha_a \in \{0, 1\} \right\}$$

satisfies this equation. We will argue (based on the choice of r in Step 2) that S has 2^ℓ distinct elements. Thus, the equation $Z^{m_1} - Z^{m_2} = 0$ has at least 2^ℓ roots in the field $\mathbb{F}_p[X]/(h(X))$. Note that $m_1, m_2 \leq n^{2\sqrt{r}} < 2^\ell$. That is, this polynomial has more roots than its degree. So, it must be the zero polynomial, that is $m_1 = m_2$, and we are done.

We need to argue that the 2^ℓ products of the form $\prod_{a=1}^{\ell}(X-a)^{\alpha_a}$, $\alpha_a \in \{0,1\}$, give distinct elements in $\mathbb{F}_p[X]/(h(X))$. By Step 3, $p > \ell$. So, $X - a$, for $a = 1, 2, \ldots, \ell$, are distinct irreducible elements of $\mathbb{F}_p[X]$. Since elements of $\mathbb{F}_p[X]$ factorize uniquely into irreducible factors, the 2^ℓ products, $\prod_{a=1}^{\ell}(X-a)^{\alpha_a}$, $\alpha_a \in \{0,1\}$, are distinct elements of $\mathbb{F}_p[X]$. But are they distinct in $\mathbb{F}_p[X]/(h(X))$? Each such product is a distinct element of $\mathbb{F}_p[X]$ of degree at most ℓ, so the difference of any two is a non-zero polynomial of degree at most ℓ. If we can somehow ensure that the degree of $h(X)$ is at least $\ell + 1$, then these products will be distinct in $\mathbb{F}_p[X]/(h(X))$.

How do we ensure that $h(X)$ has degree at least $\ell+1$? Recall that the number p in the argument so far is an arbitrary prime divisor of n. It is time to choose p. By Step 2, we know that the order of n modulo r is divisible by a prime $q \geq \ell+1$. Since q is prime there must be a prime factor p of n whose order w modulo r is divisible by q. In particular, $w \geq q \geq \ell + 1$. Fix one such p.

Claim 3 *w divides* $\deg(h)$*, so* $\deg(h) \geq w \geq \ell + 1$*. (Actually,* $\deg(h) = w$*, but we won't need this.)*

Proof: We have $X^r = 1$ in $\mathbb{F}_p[X]/(h(X))$, because $h(X)$ divides $X^r - 1$. In the implementation of Step 2, we ensure that r does not divide n; in particular, $r \neq p$. So, 1 is not a root of $(X^r - 1)/(X - 1)$ in $\mathbb{F}_p$, and $h(X) \neq X - 1$. Since r is prime, and $X \neq 1$, the order of X in $\mathbb{F}_p[X]/(h(X))$ is exactly r. But the order of an element must divide the order, $p^{\deg(h)} - 1$, of the multiplicative group of the field. That is, r divides $p^{\deg(h)} - 1$, implying that w divides $\deg(h)$. This completes the proof of Claim 3 and Claim 2. □

[This presentation is a result of discussions with T Kavitha and V Vinay, and is based on ideas taken from various sources over the past month.]

Jaikumar Radhakrishnan <jaikumar@tcs.tifr.res.in>
Tata Institute of Fundamental Research, Mumbai
