30

Probabilistic Primality Testing

A. Oliver L. Atkin
University of Illinois, Chicago

[summary by François Morain]

he aim of this talk is to give a strong probabilistic pseudoprimality test that recognises a maximal number of composite numbers as fast as possible. As a by-product, it is shown how to get "free" square-roots of certain elements of $\mathbb{Z}/p\mathbb{Z}$.

1 Introduction

The prototype of pseudoprime tests is Fermat's theorem: If p is a prime and a an integer prime to p, then

$$a^{p-1} \equiv 1 \bmod p.$$

A pseudoprime to base a (psp-a) is a composite number N such that

$$a^{N-1} \equiv 1 \bmod N.$$

For all a, there exists an infinite number of psp-a. Moreover, there are numbers N such that N is a psp-a for all a. (These numbers are called Carmichael numbers.) A refinement of this test consists in writing $N = 1 + N_0 2^t$ with N_0 odd and

$$a^{N-1} - 1 = (a^{N_0} - 1)(a^{N_0} + 1)(a^{2N_0} + 1) \cdots (a^{2^{t-1}N_0} + 1).$$

If N is prime, it divides the left-hand side and so must divide one of the numbers on the right hand side. If N is composite and divides one of the numbers on the right, then N is called a strong pseudoprime to base a (spsp-a). As for psp-a's, there is an infinite number of spsp-a.

A classical way of proving the primality of N is to test whether N is spsp-2 (say) and then rely on some more sophisticated algorithm to finish the proof [3, 1]. In certain cases, however, one might want to be as confident as possible that N is prime, without using the above-mentioned methods. Typically, one wants a test whose running time is at most five times that of a modular exponentiation with the lowest error probability possible.

2 q-strong pseudoprimes

One way of achieving this is to find small factors of $N - 1$:

$$N - 1 = q^t N_0$$

with q a "small" prime and N_0 prime to q. For a given a, put

$$b \equiv a^{N_0} \bmod N.$$

If $b \equiv 1 \bmod N$, one chooses another a and try again. Otherwise, there exists a value of i such that

$$b^{q^{i-1}} \not\equiv 1 \bmod N$$

but

$$b^{q^i} \equiv 1 \bmod N.$$

Put $B = b^{q^{i-1}}$. If N is prime, then

$$N \mid B^q - 1 = (B-1)(B^{q-1} + B^{q-2} + \cdots + 1)$$

and therefore

$$N \mid B^{q-1} + B^{q-2} + \cdots + 1.$$

If N is composite and the preceding relation is true, then N is called a q-strong pseudoprime to base a ($\mathrm{spsp}_q(a)$). In that case, B behaves like a q-th root of unity modulo N. We shall use this fact in section 4.

3 Lucas sequences

Let A be a small rational (i.e., $A = u/v$ with u and v small) such that $\Delta = A^2 - 4$ is a quadratic non-residue modulo N. Let α and β be the two distinct roots of

$$X^2 - AX + 1 = 0$$

and put $S_n = \alpha^n + \beta^n = \alpha^n + \alpha^{-n}$. (Note that computing S_n can be done in $O(\log n)$ steps using the relations

$$S_{2n} = S_n^2 - 2 \bmod N,\ S_{2n+1} = \frac{S_{2n+2} + S_{2n}}{A} \bmod N.)$$

If N is a prime, and since Δ is a quadratic non-residue, α is in the Galois field $F = \mathrm{GF}(N^2)$. It is well known (see [2, 3]) that if N is prime, then α is of order $N+1$ or equivalently

$$S_{N+1} \equiv 2 \bmod N.$$

A composite number N satisfying this relation is called a Lucas-pseudoprime for parameter A (Lpsp-A). More generally, writing $N+1 = q^t N_0$, one can define the notion of q Lucas pseudoprimes. By analogy with the preceding section, we would like $\alpha^{(N+1)/2} = -1$. For this, we write $\alpha = \gamma^2$ in F. The norm of γ is $\gamma^{N+1} = \alpha^{(N+1)/2} = -1$. Then the minimal polynomial of γ is

$$X^2 - cX - 1$$

with c in $\mathbb{Z}/N\mathbb{Z}$. We write:

$$\gamma^2 - c\gamma - 1 = 0$$

or

$$(\gamma^2 - 1)^2 = c^2\gamma^2$$

which reads

$$(\alpha - 1)^2 = c^2\alpha$$

yielding

$$\alpha^2 + 1 - 2\alpha = c^2\alpha$$

and using the fact that $\alpha^2 + 1 = A\alpha$, one gets

$$A - 2 = c^2$$

in $\mathbb{Z}/N\mathbb{Z}$. This means that $A - 2$ is a quadratic residue modulo N.

4 Getting free square-roots modulo p

Let p be an odd prime. The aim of this section is to show how to find square-roots modulo p as by-products of other calculations.

4.1 By-products of q-strong tests

Let a be such that a is a square modulo p. Then, if $p \equiv 3 \bmod 4$, a square-root of a is given by

$$a^{(p+1)/4} \bmod p.$$

If $p \equiv 5 \bmod 8$, then 2 is a non-residue modulo p, therefore $2a$ is not a square. Put

$$\xi = (2a)^{(p-5)/8} \bmod p.$$

Then

$$\xi^2(2a) \equiv (2a)^{(p-1)/4} \equiv i \bmod p$$

where $i^2 \equiv (2a)^{(p-1)/2} \equiv -1$. We also deduce that $\xi a(i-1)$ is a square-root of a since

$$(\xi a(i-1))^2 = \xi^2 a^2 (i-1)^2 \equiv a \bmod p.$$

In this process, we were able to identify $\sqrt{-1} \bmod p$ as well as $\sqrt{a} \bmod p$.
Another way of getting square-roots uses Gaussian periods. For example, take $q = 7$. Let ζ be a primitive q-th root of unity (over $\mathbb{C}$). Define the two periods:

$$\eta_0 = \sum \zeta^{\mathcal{R}}, \ \eta_1 = \sum \zeta^{\mathcal{N}}$$

where $\mathcal{R}$ runs through the quadratic residues modulo q, and $\mathcal{N}$ through the non-residues. Then, it is well known (see e.g., [4]) that

$$\eta_0 + \eta_1 = -1, \ \eta_0 - \eta_1 = 2\eta_0 + 1 = \sqrt{(-1)^{(q-1)/2} q}.$$

Coming back to our problem, we replace ζ by B, a root of unity modulo p (i.e., a number $B \neq 1$ such that $B^q \equiv 1 \bmod p$), and get that

$$2(B + B^2 + B^4) + 1 \equiv \sqrt{-7} \bmod p.$$

4.2 By-products of Lucas sequences

We use the notations of section 2. In particular, $A-2$ is not a square modulo p and $\alpha^{(p+1)/2} = -1$ in $F = \mathrm{GF}(p^2) \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(X^2 - AX + 1)$.
Suppose first that $p \equiv 3 \bmod 4$. Then

$$S_{(p+1)/4} \equiv 0 \bmod p$$

since $S_{(p+1)/2} = -2 = S^2_{(p+1)/4} - 2$. Moreover

$$S_{(p+5)/4} \equiv \sqrt{4 - A^2}.$$

We check this with

$$\begin{aligned} S^2_{(p+5)/4} = &\quad (\alpha^{(p+5)/4} + \alpha^{-(p+5)/4})^2 = \alpha^{(p+5)/2} + \alpha^{-(p+5)/2} + 2 \\ = &\quad (-1)\alpha^2 + (-1)\alpha^{-2} + 2 = -(\alpha - 1/\alpha)^2 = 4 - A^2 \end{aligned}$$

using the fact that $\alpha^{(p+1)/2} = -1$.
If $p \equiv 7 \bmod 8$, then

$$S_{(p+1)/8} \equiv \sqrt{2} \bmod p$$

using the fact that $S_{(p+1)/4} = 0 = S^2_{(p+1)/8} - 2$.
If $p \equiv 3 \bmod 8$, we may write

$$\begin{aligned} -2S^2_{(p+5)/8} = &\quad -2(\alpha^{(p+5)/4} + \alpha^{-(p+5)/4} + 2) = -2(\sqrt{4 - A^2} + 2) \\ = &\quad -4 - 2\sqrt{4 - A^2} = (\sqrt{A-2} - \sqrt{-A-2})^2 \end{aligned}$$

so that

$$\sqrt{-2}S_{(p+5)/8} = \sqrt{A-2} - \sqrt{-A-2}.$$

When $p \equiv 1 \bmod 4$, we can show that

$$S_{(p-1)/4} \equiv \sqrt{2 - A}.$$

This comes from the fact that:

$$S^2_{(p-1)/4} = \alpha^{(p-1)/2} + \alpha^{-(p-1)/2} + 2 = \alpha^{-1}\alpha^{(p+1)/2} + \alpha\alpha^{-(p+1)/2} + 2 = -(\alpha + 1/\alpha) + 2 = 2 - A.$$

We can also use Gaussian periods. Let q be an odd prime and

$$\theta = \alpha^{(p+1)/q}$$

be a primitive q-th root of unity in F (i.e., $\theta \neq 1$). Then, using η_0 and η_1, one has:

$$\eta_0 - \eta_1 = \sqrt{(-1)^{(q-1)/2}q}.$$

We must distinguish two cases. The first one corresponds to $q \equiv 1 \bmod 4$. Then η_0 is in $\mathbb{Z}/p\mathbb{Z}$ and we get $\sqrt{q}$ as usual. For example, taking $q = 5$, one has

$$\eta_0 = \theta + \theta^4 = \theta + \theta^{-1} = S_{(p+1)/q}.$$

On the other hand, when $q \equiv 3 \bmod 4$, η_0 is in F. Put $\omega = \sqrt{\Delta} = \alpha - 1/\alpha$. Then $\omega(\eta_0 - \eta_1)$ is in $\mathbb{Z}/p\mathbb{Z}$. For instance, if $q = 7$, one has

$$\omega(\eta_0 - \eta_1) = \omega(\theta - \theta^{-1}) + \omega(\theta^2 - \theta^{-2}) + \omega(\theta^4 - \theta^{-4}).$$

We then use the fact that

$$\omega(\theta^i - \theta^{-i}) = (\alpha - 1/\alpha)(\theta^i - \theta^{-i}) = \alpha\theta^i + \alpha^{-1}\theta^{-i} - (\alpha\theta^{-i} + \alpha^{-1}\theta^i) = S_{i(p+1)/q+1} - S_{i(p+1)/q-1}.$$

5 Pseudoprimality and square-roots

Suppose we suspect that a given odd integer N is prime. Then, we might try to get square-roots of some numbers. If we can find two square-roots of a number Z that are different, we can factor N, since

$$X_1^2 \equiv X_2^2 \bmod N \Rightarrow \gcd(X_1 - X_2, N) \mid N.$$

For instance, if $N \equiv 3 \bmod 4$ is a $\mathrm{spsp}_q(a)$ and a Lpsp-A, one can try to find A such that $4 - A^2$ is a quadratic residue modulo N. Then, we compute $\sqrt{4 - A^2}$ in two ways, using $A^{(N+1)/4}$ and $S_{(N+5)/4}$ and try to factor N with it.
There is another application of this. The ECPP algorithm [1] requires the computation of square-roots of small numbers modulo N, N a probable prime. One can use the same ideas to get these square-roots as free, using the same method and thus speeding the whole process.

References

[1] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. Research Report 1256, Institut National de Recherche en Informatique et en Automatique, June 1990. Submitted to *Math. Comp.*

[2] J. Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Math. Comp.*, 29(130):620–647, 1975.

[3] H. Cohen and A. K. Lenstra. Implementation of a new primality test. *Math. Comp.*, 48(177):103–121, 1987.

[4] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer–Verlag, 2nd edition, 1980.