Primality Tests Using Algebraic Groups

Masanari Kida

CONTENTS

We introduce primality tests using algebraic groups. Some previously known tests are naturally interpreted as special cases of these algebraic group tests. Moreover, in this framework we can generalize Lucas and $n+1$ tests in a natural way.

1. INTRODUCTION

The first deterministic polynomial-time algorithm for primality testing by Agrawal, Kayal, and Saxena [Agrawal et al. 02] has been epoch-making. On the other hand, some previously known primality (or pseudoprimality) tests are still of interest not only because they are faster practically but also because they offer interesting mathematical objects such as pseudoprimes.

The aim of this paper is to introduce primality tests, essentially of theoretical nature, using simple arithmetic of algebraic groups over finite fields. We show that if an algebraic group defined over the rational number field has certain good properties on reduction modulo a prime number, then we can construct primality tests analogous to classical tests such as the Fermat test, the Lucas test, and so on. These rather abstract tests give a unified viewpoint of existing tests and bring a natural and concrete generalization of some classical tests. In this paper, we stress primality testing using algebraic tori. We show that certain congruent properties of the Lucas sequence used for the primality testing can be regarded as a consequence of simple arithmetic of certain algebraic torus. This naturally leads to a generalization of primality tests using higher-order recurrence sequences.

For example, here we give a generalization of the Lucas sequences to the order-three recurrence sequence. Let $f(X) = X^3 + u_1X^2 + u_2X + u_3$ be an irreducible cubic polynomial over $\mathbb{Z}$ and ξ_1, ξ_2, ξ_3 the roots of $f(X)$. We assume that the Galois group of $f(X)$ is cyclic. For a triple (s, t, u) of elements in $\mathbb{Z}$ satisfying $(t, u) \neq (0, 0)$,

2000 AMS Subject Classification: Primary 11Y11, 11B39, 11A51, 11E92

Keywords: Primality test, algebraic group, algebraic torus, recurrence sequence 3

1058-6458/2004$0.50 per page

we set

$$\alpha_1 = s + t\xi_1 + u\xi_1^2,$$
$$\alpha_2 = s + t\xi_2 + u\xi_2^2,$$
$$\alpha_3 = s + t\xi_3 + u\xi_3^2.$$

Define three sequences $\{a_k^{(s)}\}$ $(s = 0, 1, 2)$ by

$$\begin{aligned}\sqrt{\Delta}\, a_k^{(0)} &= \xi_2\xi_3(\xi_3 - \xi_2)\alpha_1^k + \xi_1\xi_3(\xi_1 - \xi_3)\alpha_2^k \\ &\quad + \xi_1\xi_2(\xi_2 - \xi_1)\alpha_3^k, \\ \sqrt{\Delta}\, a_k^{(1)} &= (\xi_2^2 - \xi_3^2)\alpha_1^k + (\xi_3^2 - \xi_1^2)\alpha_2^k + (\xi_1^2 - \xi_2^2)\alpha_3^k, \\ \sqrt{\Delta}\, a_k^{(2)} &= (\xi_3 - \xi_2)\alpha_1^k + (\xi_1 - \xi_3)\alpha_2^k + (\xi_2 - \xi_1)\alpha_3^k, \end{aligned} \tag{1–1}$$

where $\sqrt{\Delta} = (\xi_1 - \xi_2)(\xi_2 - \xi_3)(\xi_3 - \xi_1)$ is a square root of the discriminant of $f(X)$. These sequences satisfy a recurrence relation arising from the minimal equation of α_1. Namely, if $\Phi(X) = X^3 + v_1X + v_2X + v_3$ is a minimal polynomial of α_1, then $\{a_k^{(i)}\}(i = 1, 2, 3)$ satisfy $a_{k+3}^{(i)} + v_1a_{k+2}^{(i)} + v_2a_{k+1}^{(i)} + v_3a_k^{(i)} = 0$. Here the coefficients v_1, v_2, v_3 can be given explicitly in terms of s, t, u, u_1, u_2, and u_3. We can show that all terms in the sequences are contained in $\mathbb{Z}$. For these sequences, the following theorem holds.

Theorem 1.1. *Let p be a prime number prime to* $\mathrm{disc}(f) \cdot \mathrm{disc}(\Phi)$. *Assume* $\gcd(f(X), X^{p-1} - 1) \equiv 1 \pmod p$. *Then we have*

$$a_{p^2+p+1}^{(0)} \equiv N_{K/\mathbb{Q}}(\alpha_1) \quad \textit{and}$$
$$a_{p^2+p+1}^{(1)} \equiv a_{p^2+p+1}^{(2)} \equiv 0 \pmod p.$$

From this theorem, we can deduce an analogue of the Lucas test.

Corollary 1.2. *Let n be a positive integer prime to* $\mathrm{disc}(f) \cdot \mathrm{disc}(\Phi)$. *Assume* $\gcd(f(X), X^{n-1} - 1) \equiv 1 \pmod n$. *If*

$$a_{n^2+n+1}^{(0)} \not\equiv N_{K/\mathbb{Q}}(\alpha_1) \quad \textit{or}$$
$$a_{n^2+n+1}^{(1)} \not\equiv 0 \quad \textit{or}$$
$$a_{n^2+n+1}^{(2)} \not\equiv 0 \pmod n,$$

then n is a composite number.

In this corollary, we have to compute a greatest common divisor in $\mathbb{Z}/n\mathbb{Z}[X]$. If the usual procedure of Euclidean algorithms does not work, we can readily conclude that n is not a prime number.

Since we have the freedom to choose the triple (s, t, u), we can try another triple if the above test fails for one triple.

Primality tests using higher-order linear recurrence sequences are studied by several authors such as Adams and Shanks [Adams and Shanks 82] and Gurak [Gurak 89]. Our approach is completely different from theirs. Our construction is simpler than theirs in some respect, though we use an algebro-geometric machinery. The relation between these constructions are not pursued here. We concentrate our construction of the primality tests on the theoretical aspects used in the previous tests.

The outline of the paper is as follows. In Section 1, we explain primality tests in an abstract form. From these tests, some classically-known tests are deduced. In Section 2, new primality tests using higher-order recurrence sequences are presented.

2. PRIMALITY TESTS

Let n be a positive integer. We discuss various methods to tell whether or not n is prime. Let G be an algebraic group defined over $\mathbb{Q}$ written multiplicatively. Assume that G has an integral structure and that the product N of bad primes with respect to this integral structure is prime to n. For each p not dividing N, we can associate the group $G(\mathbb{F}_p)$ of the rational points over $\mathbb{F}_p$. Let $G(\mathbb{Z}/n\mathbb{Z})$ be the set of $\mathbb{Z}/n\mathbb{Z}$-rational points of G with respect to the above integral model, which may not be a group. If we cannot compute a power of an element $x \in G(\mathbb{Z}/n\mathbb{Z})$, then we can conclude that n is a composite number.

We first consider groups satisfying the following condition:

(P1) There exists an explicit function ψ on the positive integers such that $\mathrm{ord}(x)$ divides $\psi(p)$ for any element $x \in G(\mathbb{F}_p)$.

Theorem 2.1. (Fermat-type test.) *Let n be a positive integer and G an algebraic group defined over $\mathbb{Q}$ satisfying (P1). Assume that n is prime to the product of bad primes. If there exists an element $x \in G(\mathbb{Z}/n\mathbb{Z})$ such that*

$$x^{\psi(n)} \neq 1 \textit{ in } G(\mathbb{Z}/n\mathbb{Z}),$$

then n is composite.

Proof: If n is prime, then we have $x^{\psi(n)} = 1$ in $G(\mathbb{Z}/n\mathbb{Z}) = G(\mathbb{F}_n)$ by (P1). □

By taking $G = \mathbb{G}_m$ and $\psi(n) = n - 1$, we recover the classical Fermat test.

Of course, this test would be useless if G is not carefully chosen (for example, $G = \mathbb{G}_a$). This remark always applies to all tests in this section.

Next we consider the following property.

(P2) The group $G(\mathbb{F}_p)$ can be embedded in the multiplicative group of a field whose characteristic is not 2.

By adding this property we can show:

Theorem 2.2. (Miller-Rabin-type test.) *Let n be a positive integer and G an algebraic group satisfying (P1) and (P2). Assume that n is prime to the product of bad primes. Write $\psi(n) = 2^s m$ with an odd integer m. If there exists $x \in G(\mathbb{Z}/n\mathbb{Z})$ satisfying*

$$x^m \neq 1 \text{ and } x^{2^r m} \neq -1$$

for all $r = 0, 1, \ldots, s-1$ in $G(\mathbb{Z}/n\mathbb{Z})$, then n is composite.

Proof: Suppose that n is prime. Then $G(\mathbb{Z}/n\mathbb{Z})$ is the group $G(\mathbb{F}_n)$. We have $x^{\psi(n)} = 1$ by (P1). This implies that the order of x^m is a power of 2, say 2^k with some $k = 0, 1, \cdots, s$. If $k = 0$, then $x^m = 1$ holds. When $k \geq 1$, the order of $a = x^{m2^{k-1}}$ is 2. This means that a is a root of $X^2 - 1$. Considering this equation in the field containing $G(\mathbb{F}_p)$, we find that the solutions are ± 1. Since the order of a is 2, we have $a = -1$. □

Again if we take $G = \mathbb{G}_m$, then we recover the Miller-Rabin test [Crandall and Pomerance 01, Theorem 3.4.1].

The tests we have developed so far are pseudoprimality tests (or composite tests). To obtain a primality test, we require other properties on G. The first is similar to (P1).

(P3) There exists an explicit increasing function ψ on the positive real numbers satisfying $\#G(\mathbb{F}_p) \leq \psi(p)$.

The second is

(P4) For every $x \in G(\mathbb{Z}/n\mathbb{Z})$, one can determine whether its natural image $\overline{x} \in G(\mathbb{F}_p)$ is 1 or not for all prime divisors p of n.

We can now state our primality test.

Theorem 2.3. (Pocklington-type test.) *Let n be a positive integer and G an algebraic group satisfying (P3) and (P4). Assume that n is prime to the product of bad primes. Suppose there exist $x \in G(\mathbb{Z}/n\mathbb{Z})$ and positive integers F, m with $F|m$ such that for a prime divisor p of n, we have $x^m = 1$ and*

$$\overline{x}^{\frac{m}{q}} \neq 1 \text{ in } G(\mathbb{F}_p) \quad \text{for every prime divisor } q \text{ of } F,$$

where $\overline{x}$ is the image of $x \in G(\mathbb{Z}/n\mathbb{Z})$ under the natural map $G(\mathbb{Z}/n\mathbb{Z}) \to G(\mathbb{F}_p)$. If moreover $F > \psi(\sqrt{n})$ holds, then n is prime.

Remark 2.4. Here the equation $x^m = 1$ means that x^m can be computed in $G(\mathbb{Z}/n\mathbb{Z})$ and the result is 1. Also in $\overline{x}^{\frac{m}{q}} \neq 1$, we assume that the left-hand side is computable. If they are not computable, we can conclude that n is composite as before.

Proof: We first note that the condition $\overline{x}^{\frac{m}{q}} \neq 1$ can be verified by the property (P4). Write $m = Fr$ with an integer r. It is easy to observe that the order of $\overline{x}^r$ divides F. From $(\overline{x}^r)^{\frac{F}{q}} \neq 1$ it follows that the order of $\overline{x}^r$ is exactly F. On the other hand, we have $\mathrm{ord}(\overline{x}^r) \leq \#G(\mathbb{F}_p) \leq \psi(p)$ by (P3). From this inequality and our assumption, it follows $\psi(\sqrt{n}) < F \leq \psi(p)$. Since ψ is strictly increasing, we conclude $\sqrt{n} < p$. This means that n is prime. □

If we take $G = \mathbb{G}_m$ and $\psi(n) = n-1$, then (P3) is clearly satisfied. For $x \in (\mathbb{Z}/n\mathbb{Z})^*$, by checking if $\gcd(x-1, n) = 1$ or not, we can verify whether $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^*$ is 1 or not for all $p|n$. Thus (P4) is also satisfied. The theorem then gives the Pocklington test [Crandall and Pomerance 01, Theorem 4.1.3].

If we take an elliptic curve E as G and $\psi(n) = (1 + \sqrt{n})^2$, then by Hasse's theorem, (P3) is satisfied. We take a Weierstrass model of $E/\mathbb{Q}$. Then $(x, y) \in E(\mathbb{Q})$ corresponds to $\overline{\mathcal{O}} \in E(\mathbb{Z}/p\mathbb{Z})$ if and only if $\gcd(n,$ denominator of $y) > 1$. Therefore E has the property (P4). The resulting test is Goldwasser-Killian's ECPP [Goldwasser and Kilian 99].

3. HIGHER-ORDER RECURRENCE SEQUENCES

Let ξ be a primitive element of a finite Galois extension K over $\mathbb{Q}$. We may assume that ξ is an algebraic integer. We write

$$f(X) = X^d + u_1 X^{d-1} + \cdots + u_{d-1} X + u_d \in \mathbb{Z}[X]$$

for the minimal polynomial of ξ. Let

$$M(a^{(0)}, a^{(1)}, \ldots, a^{(d-1)})$$

$$M(a^{(0)},a^{(1)},a^{(2)}) = \begin{bmatrix} a^{(0)} & a^{(1)} & a^{(2)} \\ -a^{(2)}u_3 & a^{(0)}-a^{(2)}u_2 & a^{(1)}-a^{(2)}u_1 \\ -a^{(1)}u_3+a^{(2)}u_1u_3 & -a^{(1)}u_2-a^{(2)}u_3+a^{(2)}u_1u_2 & a^{(0)}-a^{(1)}u_1-a^{(2)}u_2+a^{(2)}u_1^2 \end{bmatrix}$$

FIGURE 1.

be the $d\times d$ matrix corresponding to $a^{(0)}+a^{(1)}\xi+\cdots+a^{(d-1)}\xi^{d-1}$ by the regular representation with respect to the basis $1,\xi,\dots,\xi^{d-1}$. Namely it satisfies

$$(a^{(0)}+a^{(1)}\xi+\cdots+a^{(d-1)}\xi^{d-1})\begin{bmatrix}1\\ \xi\\ \vdots\\ \xi^{d-1}\end{bmatrix} = M(a^{(0)},a^{(1)},\dots,a^{(d-1)})\begin{bmatrix}1\\ \xi\\ \vdots\\ \xi^{d-1}\end{bmatrix}.$$

These matrices form an algebraic subgroup T of GL_n. In fact, T is isomorphic to the Weil restriction $R_{K/\mathbb{Q}}(\mathbb{G}_m)$. Let $A=M(a^{(0)},a^{(1)},\dots,a^{(d-1)})$. We define d sequences $\{a_k^{(i)}\}_{k=0}^{\infty}$ $(i=0,1,\dots,d-1)$ by

$$A^k = M(a_k^{(0)},a_k^{(1)},\dots,a_k^{(d-1)}).$$

Obviously these sequences are in the same ring to which $(a^{(0)},a^{(1)},\dots,a^{(d-1)})$ belong. Let $\Phi(t)$ be the characteristic polynomial of A. Then each $\{a_k^{(i)}\}_{k=0}^{\infty}$ satisfies the recurrence relation given by substituting $a_k^{(i)}$ for t^k in $\Phi(t)$. The initial terms are computed from A^k $(k=0,1,\dots,d-1)$. Let $\xi_1=\xi,\xi_2,\dots,\xi_d$ be the roots of $f(X)$. Then $\alpha_k=a^{(0)}+a^{(1)}\xi_k+\cdots+a^{(d-1)}\xi_k^{d-1}$ $(k=1,2,\dots,d)$ are the eigenvalues of A. The elements of T are simultaneously diagonalized by the Vandermond matrix

$$P=\begin{bmatrix}1 & \dots & 1\\ \xi_1 & \dots & \xi_d\\ & \dots & \\ \xi_1^{d-1} & \dots & \xi_d^{d-1}\end{bmatrix},$$

and we have $P^{-1}AP=\operatorname{Diag}(\alpha_1,\dots,\alpha_d)$. Therefore the general term of $a_k^{(i)}$ is computed from $A^k=P\operatorname{Diag}(\alpha_1^k,\dots,\alpha_d^k)P^{-1}$. It is now easy to derive the following relation:

$$A^k=1 \text{ if and only if } a_k^{(0)}=1 \text{ and } a_k^{(s)}=0 \text{ for all } s\geq 1. \tag{3–1}$$

In the following examples, we write down the sequences explicitly in the case where $d=2$ and 3.

Example 3.1. Let $K=\mathbb{Q}(\sqrt{D})$ be a quadratic field with the discriminant D. We have $f(X)=X^2-D$ and

$$M(a^{(0)},a^{(1)})=\begin{bmatrix}a^{(0)} & a^{(1)}\\ Da^{(1)} & a^{(0)}\end{bmatrix}.$$

The eigenvalues are $\alpha_1=a^{(0)}+a^{(1)}\sqrt{D}$ and $\alpha_2=a^{(0)}-a^{(1)}\sqrt{D}$. Therefore we have

$$a_k^{(0)}=\frac{1}{2}(\alpha_1^k+\alpha_2^k),\quad a_k^{(1)}=\frac{1}{2\sqrt{D}}(\alpha_1^k-\alpha_2^k).$$

They satisfy the second-order linear recurrence relation

$$a_{j+2}^{(u)}-2a^{(1)}a_{j+1}^{(u)}+\det A\cdot a_j^{(u)}=0 \qquad (j=0,1,2,\dots,u=1,2)$$

with the initial terms $a_0^{(0)}=1$, $a_1^{(0)}=a^{(0)}$, $a_0^{(1)}=0$, and $a_1^{(1)}=a^{(1)}$. The relation of our sequences and the classical Lucas sequences readily follows:

$$2a_k^{(0)}=V_k,\ a_k^{(1)}=a^{(1)}U_k,$$

where

$$V_k=\alpha_1^k+\alpha_2^k,\ U_k=\frac{\alpha_1^k-\alpha_2^k}{\alpha_1-\alpha_2}.$$

Thus (3–1) is paraphrased by the Lucas sequences:

$$A^k=1 \text{ if and only if } V_k=2 \text{ and } U_k=0. \tag{3–2}$$

Example 3.2. We next consider a cyclic cubic field $K=\mathbb{Q}(\xi)$. We assume that ξ is an algebraic integer. Let the minimal equation of ξ be $f(X)=X^3+u_1X^2+u_2X+u_3$. We have the expression given in Figure 1.

By matrix multiplication, we can compute the kth term of $a_k^{(u)}$ $(u=1,2,3)$. Let $\sqrt{\Delta}$ be the Vandermond determinant $\det P$. Then we obtain (1–1) from $A^k=P\operatorname{Diag}(\alpha_1^k,\alpha_2^k,\alpha_3^k)P^{-1}$ with $a^{(0)}=s$, $a^{(1)}=t$, $a^{(2)}=u$. This is a natural generalization of the Lucas sequences. The condition $(t,u)\neq(0,0)$ is equivalent to the condition that $\alpha_1=a^{(0)}+a^{(1)}\xi+a^{(2)}\xi^2$ does not belong to $\mathbb{Q}$. If it belongs to $\mathbb{Q}$, then the above is a trivial procedure. These sequences satisfy an order-three linear recurrence relation arising from the minimal equation of $a^{(0)}+a^{(1)}\xi+a^{(2)}\xi^2$ as is noted in the introduction.

In these examples, we take an ad hoc integral model for computational convenience. A general theory on integral models of algebraic tori is found in [Voskresenski 98, Section 6].

We now return to the general situation. Let p be a rational prime. We assume that p does not divide $\det A$ and $\mathrm{disc}(f)$, because only those primes dividing these quantities can be bad primes with respect to the integral model chosen above.

We consider $\overline{A} = A \bmod p$. For simplicity, we restrict ourselves to the following two extremal cases.

Case I: p splits completely in K.

Case II: p is inert in K.

In Case I, $\Phi(t) \bmod p$ splits into linear factors over $\mathbb{F}_p$. In particular, the roots $\alpha_1, \cdots, \alpha_d \bmod p$ are contained in $\mathbb{F}_p$. From the assumption $\gcd(p, \det(A)) = 1$, it follows that none of these roots mod p is 0. Therefore we have a group homomorphism

$$T(\mathbb{F}_p) \supset \langle \overline{A} \rangle \to (\mathbb{F}_p^*)^d$$

sending A to $(\alpha_1 \bmod p, \cdots, \alpha_d \bmod p)$. In other words, T splits over $\mathbb{F}_p$.

In Case II, $\Phi(t) \bmod p$ is irreducible and we have a homomorphism

$$T(\mathbb{F}_p) \supset \langle \overline{A} \rangle \to (\mathbb{F}_{p^d})^* \tag{3–3}$$

sending A to a root α_1 of $\Phi(t) \bmod p$.

This observation gives the following theorem.

Theorem 3.3. *Let p be a prime number such that $\gcd(p, \mathrm{disc}(f) \cdot \det(A)) = 1$.*

(i) *If p splits completely in $K/\mathbb{Q}$, then*

$$a_{p-1}^{(0)} \equiv 1 \text{ and } a_{p-1}^{(s)} \equiv 0 \pmod p \text{ for all } s \geq 1.$$

(ii) *If p remains prime in $K/\mathbb{Q}$, then*

$$a_{p^d-1}^{(0)} \equiv 1 \text{ and } a_{p^d-1}^{(s)} \equiv 0 \pmod p \quad \text{for all } s \geq 1. \tag{3–4}$$

Moreover we have

$$\begin{aligned} &a_{p^{d-1}+p^{d-2}+\cdots+1}^{(0)} \equiv N_{K/\mathbb{Q}}(\alpha_1) \text{ and} \\ &a_{p^{d-1}+p^{d-2}+\cdots+1}^{(s)} \equiv 0 \pmod p \quad \text{for all } s \geq 1. \end{aligned} \tag{3–5}$$

Proof: Since we know that $\mathrm{ord}\,\overline{A}$ divides $p-1$ or p^d-1 according to Cases I and II, all but the last statements follow from Theorem 2.1.

We shall show (3–5). We have the following commutative diagram:

$$\begin{array}{ccc} \langle \overline{A} \rangle & \longrightarrow & \left(\mathbb{F}_{p^d}\right)^* \\ \downarrow & & \downarrow \mathrm{Norm} \\ \langle \overline{A} \rangle & \longrightarrow & \mathbb{F}_p^* \end{array}$$

where the left vertical map is the powering map sending $\overline{A} \mapsto \overline{A}^{p^{d-1}+p^{d-2}+\cdots+1}$ and the horizontal maps are induced by the homomorphism (3–3). It follows that $\overline{A}^{p^{d-1}+p^{d-2}+\cdots+1}$ is the diagonal matrix whose diagonal entries are $N_{\mathbb{F}_{p^d}/\mathbb{F}_p}(\alpha)$. The proof is now complete. □

In fact, (3–4) and (3–5) are equivalent. If (3–5) holds, then (3–4) holds trivially by Fermat's theorem. Conversely if (3–5) holds, then the order of

$$\overline{A}^{p^{d-1}+\cdots+1}$$

divides $p-1$. Thus by (3–3) it corresponds to an element x of $(\mathbb{F}_{p^d})^*$ satisfying $x^{p-1} = 1$. This implies that x is an element of $\mathbb{F}_p^*$ and $\overline{A}^{p+1}$ is a diagonal matrix. The diagonal entries are computed as in the above proof.

We note here that (3–5) can be also considered as a Fermat-type test associated with the factor group $(\mathbb{F}_{p^d})^*/\mathbb{F}_p^*$ (or the corresponding algebraic group).

In Theorem 3.3 if we take a quadratic field K as in Example 3.1, then using (3–2), we can deduce easily the so-called Lucas test ([Crandall and Pomerance 01, Theorem 3.5.3]) . In this quadratic case, the statement (3–5) is nothing but Grantham's quadratic Frobenius test (see [Crandall and Pomerance 01, Theorem 3.5.6] and [Grantham 01]).

Example 3.4. We apply Theorem 3.3 to the cubic cyclic extension $K/\mathbb{Q}$ in Example 3.2. The unramified primes are those not dividing the discriminant of $K/\mathbb{Q}$ and they either split completely or remain prime. The decomposition of an unramified prime p can be distinguished whether or not $f(X)$ has a root in $\mathbb{F}_p$. This is easily checked by taking the gcd of $f(X)$ and $X^{p-1}-1$. This method is always available when $K/\mathbb{Q}$ is a cyclic extension of prime degree. In particular, for Case II, we have Theorem 1.1.

Let $f(X) = X^3 - 3X - 1$ and K a cyclic cubic field defined by $f(X)$. The discriminant of $K/\mathbb{Q}$ is 81. When we take $(a^{(0)}, a^{(1)}, a^{(2)}) = (0, 1, 0)$, integers prime to 3

can be tested and the smallest pseudoprime (i.e., a composite number satisfying the conditions in Theorem 3.3) is $146611 = 271 \cdot 541$. Other examples of pseudoprimes are $286903, 294409$. These pseudoprimes are eliminated if we take $(a^{(0)}, a^{(1)}, a^{(2)}) = (0, 0, 2)$.

Also we can find an interesting family of pseudoprimes.

Proposition 3.5. *Let $f(X) \in \mathbb{Z}[X]$ be a cubic polynomial defining a cyclic cubic field K. Let p be prime and $n = p(2p-1)$, where $q = 2p-1$ is also prime. Assume that both p and q decompose completely in K. Let $f(X) = (X-\eta_1)(X-\eta_2)(X-\eta_3)$ be the decomposition modulo q. Suppose that all η_1, η_2, η_3 are quadratic residues modulo q. Then n is pseudoprime for K and $(a^{(0)}, a^{(1)}, a^{(2)}) = (0, 1, 0)$.*

Proof: Let $A = M(0, 1, 0)$. We consider the natural map $T(\mathbb{Z}/n\mathbb{Z}) \to T(\mathbb{F}_p) \times T(\mathbb{F}_q)$ sending A to $(A \bmod p, A \bmod q)$. We shall show that A^{n-1} is sent to diagonal matrices. If this is shown, then A^{n-1} itself is diagonal by the Chinese remainder theorem.

Since p splits completely, it follows from Theorem 3.3 (i) that $A^{p-1} \bmod p$ is diagonal. Thus $A^{n-1} = (A^{p-1})^{2p+1} \bmod p$ is also diagonal.

Let x_i be a solution of $x_i^2 \equiv \eta_i \pmod q$ for $i = 1, 2, 3$. These x_i exist by our assumption. Now we have

$$\begin{aligned} A &\equiv P\,\mathrm{Diag}(\eta_1, \eta_2, \eta_3)P^{-1} \\ &\equiv P\,\mathrm{Diag}(x_1^2, x_2^2, x_3^2)P^{-1} \\ &\equiv (P\,\mathrm{Diag}(x_1, x_2, x_3)P^{-1})^2 \pmod q. \end{aligned}$$

This yields

$$A^{p-1} \equiv (P\,\mathrm{Diag}(x_1, x_2, x_3)P^{-1})^{2(p-1)} \pmod q.$$

Since $q - 1 = 2(p-1)$ and q splits completely in K, $A^{p-1} \pmod q$ is diagonal again by Theorem 3.3 (i). Therefore $A^{n-1} = (A^{p-1})^{2p+1} \bmod q$ is diagonal. This completes the proof of the proposition. □

In Example 3.4, the numbers 144611 and 286903 are of the form $p(2p-1)$. The other examples produced by this proposition are $9493903, 12890503$.

In Case II, $\langle \overline{A} \rangle$ is a subgroup of the multiplicative group of a field. In particular, (P2) is satisfied.

Theorem 3.6. *Let p and K be as in Theorem 3.3. Assume that p remains prime in K. Write $p^d - 1 = 2^t m$ with odd integer m. Then we have either*

$$a_m^{(0)} \equiv 1 \text{ and } a_m^{(s)} \equiv 0 \pmod p \quad \text{for all } s \geq 1,$$

or

$$a_{2^r m}^{(0)} \equiv -1 \text{ and } a_{2^r m}^{(s)} \equiv 0 \pmod p \quad \text{for all } s \geq 1$$

for some $r = 0, 1, \ldots, t-1$.

Example 3.7. Let $f(X)$ and K be as in Example 3.4. As before, we take $(a^{(0)}, a^{(1)}, a^{(2)}) = (0, 1, 0)$. Then the smallest pseudoprime for the above theorem is 59231.

If we replace $f(X)$ with $X^3 - X^2 - 2X + 1$, which defines a cubic cyclic field of discriminant 49, then pseudoprimes are $61597, 312391$ from the smallest.

When this paper was almost finished, the author came to know N. Suwa's work on probable primality tests [Suwa 04] . He also uses algebraic tori to reformulate the primality tests using Lucas sequences. Though he concentrates on classical quadratic cases, he obtained a result on the probability of failure of the above test. It would be an interesting problem to extend his result to our case of higher-order recurrence sequences.

Deriving the Pocklington-type test is also easy.

Theorem 3.8. *Let n be a positive integer satisfying $\gcd(n, \mathrm{disc}(f) \cdot \det(A)) = 1$ and being inert in K. Assume that there exists a positive divisor F of $n^d - 1$ that is greater than $n^{d/2} - 1$ satisfying the following conditions:*

$$a_{n^d-1}^{(0)} \equiv 1 \text{ and } a_{n^d-1}^{(s)} \equiv 0 \pmod n \quad \text{for all } s \geq 1$$

and, for all prime divisor q of F and all $s \geq 1$,

$$\gcd(a_{\frac{n^d-1}{q}}^{(0)} - 1, n) = 1 \text{ and } \gcd(a_{\frac{n^d-1}{q}}^{(s)}, n) = 1.$$

Then n is a prime number.

Proof: We can take $\psi(n) = n^d - 1$ in (P3). The gcd conditions ensure (P4). Thus the theorem follows from Theorem 2.3. □

Passing to the factor group modulo diagonal matrices, we have the following corollary.

Corollary 3.9. *Let n and K be as in Theorem 3.8. Assume there exists a positive divisor F of $\dfrac{n^d - 1}{n - 1}$ greater than $\dfrac{n^{d/2} - 1}{n^{1/2} - 1}$ satisfying*

$$a_{\frac{n^d-1}{n-1}}^{(s)} \equiv 0 \pmod n$$

and

$$\gcd(a^{(s)}_{\frac{n^d-1}{q(n-1)}}, n) = 1 \quad \textit{for all prime divisor } q \textit{ of } F$$

for all $s \geq 1$. *Then* n *is a prime.*

If K is a quadratic field, then this is usually called the Lucas $n+1$ test (see [Crandall and Pomerance 01, 4.2.1]). The author unfortunately could not find any good examples to which a general form of this test can apply.

Lastly we give a remark on computation. The classical Lucas sequences can be computed in a very fast way using the so-called binary Lucas chain. This can be generalized as follows. Let $\mathbf{a}_i = (a_i^{(0)}, a_i^{(1)}, \ldots, a_i^{(d-1)})$ be the first row of A^k. Then directly from the definition, it follows that $\mathbf{a}_{j+k} = \mathbf{a}_j A^k$. In particular, we have

$$\mathbf{a}_{2j} = \mathbf{a}_j A^j \text{ and } \mathbf{a}_{2j+1} = \mathbf{a}_j A^{j+1}.$$

To recover the classical formula from this is quite easy. Also since we are working with groups, we are able to use the repeating square method to compute the sequences.

REFERENCES

[Adams and Shanks 82] W. Adams and D. Shanks. "Strong Primality Tests that Are Not Sufficient." *Math. Comp.* 39:159 (1982), 255–300.

[Agrawal et al. 02] M. Agrawal, N. Kayal, and N. Saxena. "PRIMES is in P." Preprint, 2002.

[Crandall and Pomerance 01] R. Crandall and C. Pomerance. *Prime Numbers*. New York: Springer-Verlag, 2001.

[Goldwasser and Kilian 99] S. Goldwasser and J. Kilian. "Primality Testing Using Elliptic Curves." *J. ACM* 46:4 (1999), 450–472.

[Grantham 01] J. Grantham. "Frobenius Pseudoprimes." *Math. Comp.* 70:234 (2001), 873–891.

[Gurak 89] S. Gurak. "Cubic and Biquadratic Pseudoprimes of Lucas Type." In *Théorie des nombres* (Quebec, PQ, 1987), pp. 330–347. Berlin: de Gruyter, 1989.

[Suwa 04] N. Suwa. "Some Remarks on Lucas Pseudoprimes." Preprint, 2004.

[Voskresenski 98] V. E. Voskresenskiĭ. *Algebraic Groups and Their Birational Invariants*, Translations of Mathematical Monographs, 179. Providence, RI: Amer. Math. Soc., 1998.

Masanari Kida, Department of Mathematics, The University of Electro-Communications, Chofu, Tokyo 182-8585, Japan (kida@sugaku.e-one.uec.ac.jp)

Received November 6, 2003; accepted in revised form July 8, 2004.