ABSOLUTE QUADRATIC PSEUDOPRIMES

RICHARD G.E. PINCH

Abstract. We describe some primality tests based on quadratic rings and discuss the absolute pseudoprimes for these tests.

1. Introduction

We describe some primality tests based on quadratic rings and discuss the absolute pseudoprimes for these tests.

2. Primality tests

We briefly recall some standard probabilistic primality tests. We assume throughout that N is the integer under test, and that N is already known to be odd and not a perfect power.

The *Fermat criterion* with base b is the condition $b^{N-1} \equiv 1 \bmod N$. We shall usually distinguish between a *criterion* or *condition*, which is a necessary condition for primality, and a *test*, which specifies the details of the application of that criterion. For example, we would expect a Fermat test to include a preliminary trial division (at least as far as 2), possibly a test to eliminate perfect powers, and to specify a method (deterministic or random) for selecting the base b. A *(Fermat) probable prime* base b is a number N which passes this test: a *(Fermat) pseudoprime* is a composite number which passes. An *absolute (Fermat) pseudoprime* is a composite number which satisfies the Fermat criterion for every base b with $(b, n) = 1$. It is well-known that these are just the *Carmichael* numbers: N is a Carmichael number iff N is square-free with at least three prime factors and $p - 1|N - 1$ for every prime p dividing N.

For background on Carmichael numbers and details of previous computations we refer to our previous paper [24]: in that paper we described the computation of the Carmichael numbers up to 10^{15} and presented some statistics. These computations have since been extended [26] to 10^{16}, using the same techniques.

We can refine this to the *Fermat–Euler criterion* by requiring that $b^{(N-1)/2} \equiv \pm 1 \bmod N$, and again by identifying the sign to form the *Euler–Jacobi criterion* $b^{(N-1)/2} \equiv \left(\frac{b}{N}\right) \bmod N$, where $\left(\frac{b}{N}\right)$ is the Jacobi symbol. This latter is the primality criterion of Solovay–Strassen [31],[32].

Proposition 2.1. (1) *If N is an absolute pseudoprime for the Fermat–Euler criterion we have $b^{(N-1)/2} \equiv +1 \bmod N$ for all b prime to N.*
(2) *There are no absolute pseudoprimes for the Euler–Jacobi criterion.*

Proof. For the first part, suppose that p and q are distinct prime factors of N. Given b prime to N, write $b = b_1 b_2$ where $b_1 \equiv b \bmod p$ and $\equiv 1 \bmod q$; so we have $b_2 \equiv 1 \bmod p$ and $\equiv b \bmod q$. The assumption on N implies that $b_i^{(N-1)/2} \equiv \pm 1 \bmod N$ for $i = 1, 2$, but in each case the sign must be $+1$ considering $b_1^{(N-1)/2} \bmod q$ and $b_2^{(N-1)/2} \bmod p$. So $b^{(N-1)/2} = (b_1 b_2)^{(N-1)/2} \equiv 1 \bmod N$.

Date: 14 August 2006.
1991 *Mathematics Subject Classification.* Primary 11Y99; Secondary 11A51,11Y11.

The second part follows by observing that N is not a perfect square, so $\left(\frac{b}{N}\right) = -1$ for some b. □

The final extension to the Fermat criterion which we consider is the *strong* or Miller–Rabin criterion [20],[21],[27]. Given an odd N, write $N-1 = 2^r s$, with s odd, and for b mod N form the sequence

$$b^s, b^{2s}, \ldots, b^{2^{r-1}s}, b^{2^r s} = b^{N-1} \mod N$$

in which each term is the square of the preceding. The criterion requires that the sequence end in 1, and further that the first occurence of 1 either be at the first term, or be preceded by -1.

It is clear that the Miller–Rabin criterion includes the Fermat–Euler criterion: in fact it includes the Euler–Jacobi criterion as well. There are thus no absolute pseudoprimes for this criterion: indeed, the proportion of bases b for which a composite number can satsify the criterion is at most $1/4$.

3. Quadratic rings

A variety of primality tests have been proposed which extend the Fermat test to a quadratic ring. Let N and d be integers: we shall assume throughout that N is odd and d is prime to N. Let $R = R(N,d)$ denote the quadratic ring $\mathbb{Z}[X]/\langle N, X^2 - d\rangle$. It is natural to denote the image of X in this ring by $\sqrt{d}$. If M and N are coprime then the Chinese Remainder Theorem gives a natural isomorphism between $R(MN,d)$ and $R(M,d) \oplus R(N,d)$, so we shall be interested in the case when N is an odd prime power p^f.

We define an automorphism $'$ of $R = R(N,d)$ by mapping $\sqrt{d} \mapsto -\sqrt{d}$: this is inudeced by the automorphism $X \mapsto -X$ of $\mathbb{Z}[X]$, which is compatible with the quotient map. The fixed points of $'$ form a subring $F(N,d)$ which is just the copy of $\mathbb{Z}/\langle N\rangle$ inside R. The *norm* of an element β is $\mathcal{N}(\beta) = \beta\beta'$: this map takes values in $\mathbb{Z}/\langle N\rangle$. If $\mathcal{N}(\beta)$ is invertible (prime to N), then so is β, with $\beta^{-1} = \beta'/\mathcal{N}(\beta)$. The unit group R^* contains the *corational* or *twisted multiplicative group* $C(N,d)$, consisting of the elements of norm one. The action of $'$ on C is given by $\beta \mapsto \beta^{-1}$. The *anti-norm* is defined on R^* by $\mathcal{A}(\beta) = \beta/\beta'$.

We denote the set of elements of norm b by $C_b(p,d)$. If non-empty, it is a coset of $C = C_1$.

3.1. **Prime modulus.** We first consider the case when N is a prime p. If d is a quadratic non-residue of p then R is the field $\mathbb{F}_{p^2}$, whereas if d is a quadratic residue of p, then R is the direct sum $\mathbb{F}_p \oplus \mathbb{F}_p$. Hence the unit group R^* is either a cyclic group of order p^2-1 or a direct product of two cyclic groups of order $p-1$. If R is $\mathbb{F}_{p^2}$, the automorphism $'$ is the Frobenius automorphism $\beta \mapsto \beta^p$: otherwise it is the interchange of the two direct summands.

The norm map is $\mathcal{N}(\beta) = \beta^{p+1}$ in $\mathbb{F}_{p^2}$ and $(a,b) \mapsto ab$ in $\mathbb{F}_p \oplus \mathbb{F}_p$; the anti-norm is $\mathcal{A}(\beta) = \beta^{1-p}$ in $\mathbb{F}_{p^2}$ and $(a,b) \mapsto a/b$ in $\mathbb{F}_p \oplus \mathbb{F}_p$.

The corational group C is either the subgroup generated by the anti-norm γ^{p-1} of a generator γ of R^* when $R = \mathbb{F}_{p^2}$, or the set of elements corresponding to the form (x, x^{-1}) when $R = \mathbb{F}_p \oplus \mathbb{F}_p$. It is cyclic of order $p - \left(\frac{d}{p}\right)$, that is, $p+1$ or $p-1$ respectively.

If β is an element of R then β^p is either β' or β in the two cases: we can express this succinctly by saying that the *Frobenius condition*

$$(x + y\sqrt{d})^p = x + \left(\frac{d}{p}\right) y\sqrt{d} \tag{3.1}$$

holds.

The subring F fixed by $'$ is the field $\mathbb{F}_p$ in each case, either as a subfield of $\mathbb{F}_{p^2}$ or as the diagonal in $\mathbb{F}_p \oplus \mathbb{F}_p$. So in each case F^* is cyclic of order $p-1$.

The norm map has kernel C and image F^*. The anti-norm has kernel F^* and image C. The restriction of the anti-norm to C is just $\beta \mapsto \beta^2$, with kernel $C \cap F^* = \{\pm 1\}$ and image a cyclic group of order $\left(p - \left(\frac{d}{p}\right)\right)/2$.

When $R = \mathbb{F}_{p^2}$, the norm map is surjective , so C_b is a non-empty coset of $C = C_1$, of order $p+1$. When $R = \mathbb{F}_p \oplus \mathbb{F}_p$ then $C_b = \{(a, b/a) : a \in \mathbb{F}_p\}$ is a coset of C of order $p-1$.

We briefly consider the special case C_{-1}. When $R = \mathbb{F}_{p^2}$, this is the set of odd powers of $\gamma^{(p-1)/2}$, where γ is a generator of the cyclic group R^*. When $R = \mathbb{F}_p \oplus \mathbb{F}_p$, this is the set of pairs $(b, -1/b)$ for $b \in {\mathbb{F}_p}^*$. We note that the map $\beta \mapsto \beta^2$ maps C_- onto C in the first case and onto the index 2 subgroup of pairs $(b^2, 1/b^2)$ in the second case.

Proposition 3.1. *Let $\beta \in \mathbb{F}_{p^2}$ with $\mathcal{N}(\beta) = B$. If the order of B in ${\mathbb{F}_p}^*$ is e, then the order of β in ${\mathbb{F}_{p^2}}^*$ is $e(p+1)$.*

Proof. Let $B = g^f$ where $ef = p-1$ and g is a generator of ${\mathbb{F}_p}^*$. Let γ be a generator of ${\mathbb{F}_{p^2}}^*$ with $\mathcal{N}(\gamma) = \gamma^{p+1} = g$, and let $\beta = \gamma^r$. We have $\mathcal{N}(\beta) = \beta^{p+1} = \gamma^{r(p+1)} = B = g^f = \gamma^{(p+1)f}$, so $r(p+1) \equiv (p+1)f \bmod p^2-1$ and $r \equiv f \bmod p-1$, say $r = f + s(p-1)$. Replacing γ by γ^{1+se}, which is again a generator of ${\mathbb{F}_{p^2}}^*$, we may assume that $\beta = \gamma^f$. The order of β is then $(p^2-1)/f = e(p+1)$. □

Lemma 3.2. *Let G be a cyclic group of order r. The number of solutions to the equation $X^n = b$ in G is zero or (n, f) where the order of b in G is e and $ef = r$. For solutions to exist, it is necessary and sufficient that $n/(n,f)$ be prime to $r/(n,f)$.*

Proof. Choose a generator g of G so that $b = g^f$, and put $X = g^y$. The equation becomes $ny \equiv f \bmod r$, and hence $y.n/(f,n) \equiv f/(f,n) \bmod r/(f,n)$. Since $f/(f,n)$ is coprime to $n/(f,n)$, it is clearly necessary for solutions to exist that $n/(n,f)$ be coprime to $r/(f,n)$.

Suppose now that this condition holds. The equation for y has a unique solution y modulo $r/(f,n)$, and hence (f,n) solutions modulo r. □

3.2. **Prime powers.** We now consider the structure of $R(p^f, d)$. The map $\rho : R(p^f, d) \to R(p, d)$ given by reduction modulo p is a ring homomorphism, with kernel $pR(p^f, d)$ of order $p^{2(f-1)}$. An element $\beta \in R(p^f, d)$ is invertible iff the norm $\mathcal{N}(\beta)$ is invertible in $\mathbb{Z}/\langle p^f \rangle$ iff $\mathcal{N}(\beta)$ is prime to p iff $\rho(\mathcal{N}(\beta)) = \mathcal{N}(\rho(\beta))$ is invertible in $\mathbb{Z}/\langle p \rangle$ iff $\rho(\beta)$ is invertible in $R(p,d)$. So the restriction of ρ to R^* is a group homomorphism onto $R(p,d)^*$ and has kernel with order a power of p.

If d is a quadratic non-residue of p then it cannot be congruent to a square modulo p^f for any f. If d is a quadratic residue of p then by Hensel's Lemma (since $p > 2$), d is a square modulo p^f for any $f \geq 1$ and so $R(p^f, d)$ is isomorphic to the direct sum $\mathbb{Z}/\langle p^f \rangle \oplus \mathbb{Z}/\langle p^f \rangle$.

The group $R(p^f, d)^*$ is cyclic of order $p^{2f-2}(p^2-1)$ if d is a quadratic non-residue of p, since we can lift a generator of ${\mathbb{F}_{p^2}}^*$ to a generator of R^* (see, for example, [25]). If d is a quadratic residue of p, then R^* is $\mathbb{Z}/\langle p^f \rangle^* \oplus \mathbb{Z}/\langle p^f \rangle^*$, a direct product of two cyclic groups of order $p^{f-1}(p-1)$.

We consider the cosets C_b. Again if $\left(\frac{d}{p}\right) = +1$ then $C_b = \{(a, b/a) : a \in \mathbb{Z}/\langle p^f \rangle\}$ is a coset of C of order $p^{f-1}(p-1)$. If $\left(\frac{d}{p}\right) = -1$ then a solution to $\mathcal{N}(\beta) \equiv b \bmod p$ can be lifted by Hensel's Lemma to a solution modulo p^f, so C_b is again a non-empty coset of C, of order $p^{f-1}(p+1)$.

Proposition 3.3. *Let $R = R(p^f, d)$ with $f > 1$. There are elements of multiplicative order divisible by p in every coset C_b.*

Proof. If $\left(\frac{d}{p}\right) = +1$ then $C_b = \{(a, b/a) : a \in \mathbb{Z}/\langle p^f \rangle\}$ and we can choose a to have multiplicative order divisible by p: the order of the pair $(a, b/a)$ will then be a multiple of that of a and hence of p.

If $\left(\frac{d}{p}\right) = -1$, we consider the elements of order not divisible by p: there are $p^2 - 1$ of these. Since the reduction map ρ is one-to-one on such elements, there are $p + 1$ elements of order prime to p in C_1 and so every coset C_b has at most $p + 1$ such elements. Hence each coset has elements of order divisible by p. □

Proposition 3.4. *Let $R = R(p, d)$. Let $\alpha \in C$ and $b \in F$. The equations $\mathcal{N}(\beta) = b$, $\mathcal{A}(\beta) = \alpha$ are soluble if α and b are both squares or both non-squares in C and F respectively.*

Proof. If $\left(\frac{d}{p}\right) = +1$ then let $\beta \leftrightarrow (r, s) \in \mathbb{F}_p \oplus \mathbb{F}_p$ and $\alpha \leftrightarrow (a, 1/a)$. The equations on β are equivalent to $rs = b$, $r/s = a$, and these are equivalent to $r^2 = ab$, $s^2 = b/a$. These are soluble iff ab is a square in $\mathbb{F}_p$, which is in turn equivalent to the stated conditions on α and b.

If $\left(\frac{d}{p}\right) = -1$ then let γ be a generator of ${\mathbb{F}_p}^*$, and write $\beta = \gamma^x$, $b = \gamma^{(p+1)y}$ and $\alpha = \gamma^{(p-1)z}$. The equations on β are equivalent to $(p + 1)x \equiv (p + 1)y$ and $(p-1)x \equiv (p-1)z$ modulo $p^2 - 1$: these are equivalent to $x \equiv y \bmod p-1$ and $x \equiv z \bmod p+1$. By the Chinese Remainder Theorem these are soluble simultaneously iff $y \equiv z \bmod (p-1, p+1)$, that is, modulo 2. Again this is equivalent to the stated conditions on α and b. □

3.3. **Lucas sequences.** Let $\beta = x + y\sqrt{d}$ satisfy the equation $X^2 - AX + B = 0$ where A is the trace $\beta + \beta'$ and B is the norm $\beta\beta'$. We define the *Lucas sequences* $U_k(A, B)$ and $V_k(A, B)$ associated to β by

$$U_k = \frac{\beta^k - {\beta'}^k}{\beta - \beta'} \tag{3.2}$$

$$V_k = \beta^k + {\beta'}^k \tag{3.3}$$

or equivalently

$$\beta^k = \frac{V_k + U_k\sqrt{d}}{2}.$$

There are recurrence relationships

$$\begin{array}{lll} U_0 = 0, & U_1 = 1, & U_{k+1} = AU_k - BU_{k-1} \\ V_0 = 2, & V_1 = A, & V_{k+1} = AV_k - BV_{k-1} \end{array}$$

There are fast formulae for evaluating U and V using the duplication formulae

$$U_{2k} = U_kV_k \tag{3.4}$$

$$V_{2k} = V_k^2 - 2B^k \tag{3.5}$$

and

$$U_{2k+1} = U_{k+1}V_k - B^k \tag{3.6}$$

$$V_{2k+1} = V_{k+1}V_k - AB^k \tag{3.7}$$

which are particularly convenient if $B = \pm 1$: see, for example, Riesel [28] (4.30–47) and Joye and Quisquater [15].

The *Dickson polynomials* $g_k(X, -B)$ are defined by

$$g_k(X, -B) = \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{k}{k-j}\binom{k-j}{j}(-B)^j X^{k-2j}$$

and have the property that

$$V_k = g_k(-A, -B).$$

See Lidl and Niederreiter [19] (7.6).

4. Fermat-type tests and strengthening

We can generalise the notion of the Fermat test to other families of groups. Let $\mathcal{G}$ be a family of abelian groups $G(N)$ defined for all positive integers N composed of integers from some infinite set $\mathcal{P}$ of primes. We suppose that these groups satisfy the *Chinese Remainder property*, that is, $G(MN) \cong G(M) \oplus G(N)$ whenever M and N are coprime. We also assume that the group operations in $G(N)$ are easy to perform. We denote the order of $G(N)$ by $\phi_{\mathcal{G}}(N)$ and the exponent by $\lambda_{\mathcal{G}}(N)$. We suppose that there is a function $F(N)$ which is easily computable and agrees with $\lambda_{\mathcal{G}}(N)$ whenever N is prime. We further suppose that the groups in $\mathcal{G}$ have the *splitting property*: if $x \in G(MN)$ is a *splitting element*, that is, satisfies $x = (1, z) \in G(M) \oplus G(N)$, where 1 is the identity of $G(M)$ and z is not the identity of $G(N)$, then there is a fast algorithm for factoring MN.

The $\mathcal{G}$-Fermat test for primality of N is to take a random element of $b \in G(N)$ and to test whether $b^{F(N)}$ is the identity in $G(N)$. If not, N is certainly composite: otherwise we call N an $\mathcal{G}$-probable prime, and an $\mathcal{G}$-pseudoprime if it is in fact composite. An *absolute* $\mathcal{G}$-pseudoprime has this property whenever $b \in G(N)$.

The first example of such a system is the multiplicative group $G(N) = (\mathbb{Z}/\langle N \rangle)^*$. We have $\mathcal{P} = \{$ all primes $\}$ and $F(p) = p - 1$. The splitting property is achieved by applying Euclid's algorithm to find $\mathrm{hcf}\{x - 1, N\}$ if x is a splitting element.

We can express a number of the quadratic tests in the same framework, using groups associated to the quadratic ring $R(N, d)$. If we take $G(N)$ to be the unit group C in $R(N, d)^*$, then $F(p) = p - \left(\frac{d}{p}\right)$, and the Fermat condition becomes test A^1.

Now let π be a prime: we shall usually take $\pi = 2$. We assume throughout that N is always prime to π. Define the π-*strengthening* of the $\mathcal{G}$-Fermat test for N by writing $f(N) = \pi^r s$ with s prime to π, and forming the sequence

$$b^s, \quad b^{\pi s}, \ \ldots \ , \ b^{\pi^r s} \in G(N) \ :$$

the test requires that the sequence end in 1, which is the Fermat condition, and further that the first occurence of 1 in the sequence not be preceded by a splitting element.

The Miller–Rabin test is the 2-strengthening of the usual Fermat test: a splitting element will be an $e \not\equiv 1 \bmod N$ with $e^2 \equiv 1$, by considering $\mathrm{hcf}\{e \pm 1, N\}$.

We can express the effect of the π-strengthening by letting $o_\pi(b, G(N))$ be the power of π dividing the order of b in the group $G(N)$. The additional requirement of the π-strengthening is that the value of $o_\pi(b, G(p_i^{a_i}))$ should be the same for every prime power $p_i^{a_i}$ dividing N. If so, we call this common value the *level* of b: it is the position in the sequence of the first occurrence of 1.

For a group $G(p^a)$, we define the π-*dimension* d of $G(p^a)$ as the dimension of the elements of $G(p^a)$ of order dividing π as a vector space over $\mathbb{F}_\pi$, and the π-*height* h of $G(p^a)$ as the maximal power of π dividing the order of any element of $G(p^a)$: so h is the largest value of any $o_\pi(b, G(p^a))$. In particular, each of π^d and π^h divides $\phi_{\mathcal{G}}(p^a)$ and π^h divides $\lambda_{\mathcal{G}}(p^a)$.

4.1. **Groups of dimension 1.** Suppose for the moment that the dimension $d = 1$, so that the π-part of $G(p^a)$ is cyclic and $\phi_{\mathcal{G}}(p^a) = \pi^h m$ with m prime to π. Let $c(l)$ denote the proportion of $b \in G(p^a)$ for which $o_\pi(b, G(p^a)) = l$. We have $c(0)$ equal to the proportion of elements x of $G(p^a)$ which satisfy $x^m = 1$, so $c(0) = m/\phi_{\mathcal{G}}(p^a) = \pi^{-h}$. Each subsequent $c(l)$ for $0 < l \leq h$ is the proportion of elements of $G(p^a)$ which satisfy $x^{\pi^l m} = 1$ but not $x^{\pi^{l-1} m} = 1$, that is, $c(l) = \pi^{l-h}(1 - \pi^{-1})$.

Put $N = \prod_{i=1}^t p_i^{a_i}$. Let $c_i(l)$ denote the proportion of $b \in G(p_i^{a_i})$ for which $o_\pi(b, G(p_i^{a_i})) = l$. Let $W(N)$ be the number of element of $G(N)$ which satisfy the Fermat part of the criterion, and $S_\pi(N)$ the number which satisfy the π-strengthening. We have

$$S_\pi(N) = W(N) \sum_{l=0}^{r} \prod_{i=1}^{t} c_i(l).$$

Proposition 4.1. *Suppose that $d = 1$. Let $F(N) = \pi^r s$ with s prime to π. The proportion of elements which satisfy the π-strengthening of the Fermat criterion is at most π^{-H} if r or one of the h_i is zero, and at most π^{1-t} otherwise.*

Proof. Let $S = \sum_{l=0}^r \prod_{i=1}^t c_i(l)$. Put $H = \sum_i h_i$ and let $\rho = \min\{r, h_i\}$. The term $\prod_{i=1}^t c_i(l)$ is π^{-H} for $l = 0$; π^{tl-H-t} for $l \le \rho$; and zero otherwise.

If $\rho = 0$ then $S = \prod_{i=1}^t c_i(0) = \pi^{-H}$. So consider the case $\rho \ge 1$. We have all the $h_i \ge 1$ and $H \ge \rho t \ge t \ge 1$. So

$$S = \pi^{-H} \left(1 + \sum_{l=1}^{\rho} \pi^{t(l-1)} \right) = \pi^{-H} \left(1 + \frac{\pi^{t\rho} - 1}{\pi^t - 1} \right)$$

Suppose that $0 \le a \le H - 1$. We have

$$\left(\pi^{H-a} - \pi\right)(\pi^a - 1) \ge 0$$

and, rearranging, $\pi^H + \pi^1 \ge \pi^{H-a} + \pi^{1+a}$ (alternatively, consider them as integers written in base π). So

$$\pi^H + \pi \ge \pi^{H+1-t} + \pi^t,$$
$$\pi^{H+1} + \pi \ge \pi^H + \pi^{H+1-t} + \pi^t,$$
$$\pi^{\rho t} - 1 \le \pi^H - 1 \le \pi^{H+1} - \pi^t - \pi^{H+1-t} + 1 = \left(\pi^t - 1\right)\left(\pi^{H+1-t} - 1\right)$$
$$\frac{\pi^{\rho t} - 1}{\pi^t - 1} + 1 \le \pi^{H+1-t}$$

giving $S \le \pi^{1-t}$ as required. □

5. Quadratic primality tests

We can use the Frobenius criterion (3.1) as a primality testing criterion. Given N, we select an arbitrary d prime to N and $\beta = x + y\sqrt{d}$. The symbol $\left(\frac{d}{N}\right)$ is interpreted as the Jacobi symbol: its computation can be carried our by a variant of the Euclidean Algorithm and verifies that $(d, n) = 1$ as a by-product. We require that $B = \mathcal{N}(\beta)$ be prime to N and then that the Frobenius condition hold for N to be declared probably prime. See Grantham [12, 11].

There are a number of specialisations of this condition. We let A denote the Frobenius condition (3.1) for the number N: that is, for any $\beta = x + y\sqrt{d}$ we have $V_N \equiv x$ and $U_N \equiv \left(\frac{d}{N}\right) y$ modulo N, where U_k and V_k are the Lucas sequences (3.3) associated to β. We let B denote the condition that $V_N \equiv x \bmod N$, and C the condition that $U_{N-\epsilon} \equiv 0 \bmod N$, where $\epsilon = \left(\frac{d}{N}\right)$.

Let X denote one of these conditions. We introduce some notation for various specialisations of the condition X. We let $X(d)$ denote the requirement that the condition hold for a given discriminant d. We let X_ϵ, where ϵ is $+$ or $-$, denote the requirement that the condition hold whenever $\left(\frac{d}{N}\right) = \epsilon$. We let X^b denote the requirement that the condition hold for all β with norm b. So A^1_-, for example, denotes the condition that $\beta^N = \beta'$ for all $\beta = x + y\sqrt{d}$ of norm 1 with $\left(\frac{d}{N}\right) = -1$.

We refer to these conditions collectively as *quadratic* primality criteria.

Proposition 5.1. *For given $\epsilon = \pm 1$, the conditions B_ϵ and C_ϵ together are equivalent to A_ϵ.*

Proof. It is clear that A_ϵ implies both of B_ϵ and C_ϵ. In the other direction, suppose that $\beta = x + y\sqrt{d}$ satisfies both of B_ϵ and C_ϵ, where $\left(\frac{d}{N}\right) = \epsilon$.

If $\epsilon = +1$ we have $\beta^N = x + z\sqrt{d}$ for some z and $\beta^{N-1} = v + 0\sqrt{d}$. So $\beta^N = v\beta = vx + vz\sqrt{d}$. Equating coefficients, we have $vx \equiv x \bmod N$, so $v \equiv 1$ and $z \equiv y$: that is, $\beta^N \equiv \beta$.

If $\epsilon = -1$ we have $\beta^N = x + z\sqrt{d}$ for some z and $\beta^{N+1} = v + 0\sqrt{d}$. So $\beta^N = v\beta'/B = (v/B)(x - y\sqrt{d})$. Equating coefficients, we must have $v = B$ and $\beta^N \equiv \beta'$.

So in each case condition A_ϵ is satisfied. □

We note that the result applies to the specialisations A^b_ϵ, B^b_ϵ, C^b_ϵ.

Consider condition A_-, which requires that $\beta^N \equiv \beta' \bmod N$. This implies that $\beta^{N+1} = \beta\beta' = B$, and so implies that $B^{N-1} \equiv 1 \bmod N$. It also implies that $(\beta/\beta')^N = \beta'/\beta$, so $\alpha^{N+1} = 1$ for all α in the corational group C_1. We can thus interpret criterion A_- or A as including the conventional Fermat criterion and its analogue for the corational group.

5.1. **Absolute quadratic pseudoprimes.** We consider composite numbers satisfying one of these criteria for all permissible choices of β: we call such a number an *absolute pseudoprime* for the relevant criterion.

We put $\beta = x + y\sqrt{d}$ with norm $B = x^2 - dy^2$. We assume throughout that N is not a prime power, that N is prime to $6dB$ and that, if $B \neq 1$ then N is prime to $B - 1$.

Proposition 5.2. (1) *An absolute pseudoprime for criteria A_+, A_- or B must be a Carmichael number.*
(2) *There are no absolute pseudoprimes for criterion A.*
(3) *An absolute pseudoprime for criterion A^{-1}_ϵ must also be an absolute pseudoprime for criterion A^1_ϵ for each $\epsilon = \pm 1$.*
(4) *The criteria $C_\pm$ are equivalent to $A^1_\pm$ respectively.*
(5) *An absolute pseudoprime for a criterion A^b_+ must be a Carmichael number.*
(6) *An absolute pseudoprime for a criterion $A^b_\pm(d)$ must be square-free.*

Proof. (1) Consider $\beta = x + 0\sqrt{d}$. The condition implies $x^n \equiv x \bmod N$, for any value of x, and so N must be a Carmichael number.
(2) Consider $\beta = \sqrt{d}$. The condition implies $d^{(N-1)/2} \equiv \left(\frac{d}{N}\right) \bmod N$, for which it is already known there are no absolute pseudoprimes by Proposition 2.1.
(3) Consider the map $\beta \mapsto \beta^2$ for d with $\left(\frac{d}{p}\right) = -1$. As already noted this map on C_{-1} is onto C_1 and the Frobenius condition holds for β^2 if it holds for β. So if condition $A^{-1}_\pm$ holds for all $\beta \in C_{-1}$, then condition $A^1_\pm$ must hold for all $\alpha \in C_1$.
(4) We have $U_{N-\epsilon} \equiv 0 \bmod N$ all β iff $\beta^{N-\epsilon} \in F$ all β iff $\beta^{N-\epsilon} = (\beta')^{N-\epsilon}$ all β iff $\alpha^{N-\epsilon} = 1$ all $\alpha \in C$, since the anti-norm is onto C, iff $\alpha^N = \alpha$ resp. α' all $\alpha \in C$.
(5) Suppose p^f is a prime power factor of N and $\left(\frac{d}{p}\right) = +1$. We have $(a, b/a)^N \equiv (a, b/a) \bmod p^f$, so in particular $a^N \equiv a \bmod p^f$ for any a, and any $p^f | N$. Hence N must be a Carmichael number.
(6) The map $\beta \mapsto \beta^N$ is required to be a permutation of the appropriate set C_b. But if p^f divides N with $f > 1$ then by Proposition 3.3 the coset C_b in $R(p^f, d)$ contains elements of order divisible by p and the map cannot be one-to-one on such elements.

□

Indeed, we can strengthen (4) by noting that from Lemma 3.4 the conditions $C^b_\pm$ for two values of b, one a quadratic residue and the other a quadratic non-residue, together imply $A^1_\pm$.

Theorem 5.3. (1) *The requirements for an absolute pseudoprime for each of the quadratic criteria are those given in Table 1.*

(2) *There are no absolute pseudoprimes for criteria A^b_- ($b \neq 1$), A_-, A^1 or A.*

Proof. Suppose that p is a prime factor of N and that N satisfies one of the conditions stated. We let $\beta = x + y\sqrt{d}$ with norm $B = x^2 - dy^2$.

A_+: We have $\beta^N \equiv \beta \bmod p$, so $\beta^{N-1} \equiv 1 \bmod p$. The order of β modulo p can be $p^2 - 1$ or $p - 1$ according as $\left(\frac{d}{p}\right) = -1$ or $+1$: we require either $p^2 - 1 | N - 1$ or $p - 1 | N - 1$ respectively. Since the value of $\left(\frac{d}{p}\right)$ is not constrained by knowing $\left(\frac{d}{N}\right)$, we require $p^2 - 1 | N - 1$.

A^b_+: We have $\beta^N \equiv \beta \bmod p$ for $B = b$. The order of such β modulo p can be $e(p+1)$ or $p - 1$ according as $\left(\frac{d}{p}\right) = -1$ or $+1$, where e denotes the multiplicative order of b in ${\mathbb{F}_p}^*$. We require $\operatorname{lcm}\{p - 1, e(p+1)\}$ to divide $N - 1$.

A^1_+: We have $\beta^N \equiv \beta \bmod p$ for $B = 1$. The order of β modulo p can be $p - \left(\frac{d}{p}\right)$ and we require $p - \left(\frac{d}{p}\right) | N - 1$. Again the value of $\left(\frac{d}{p}\right)$ is unconstrained so we require $\operatorname{lcm}\{p - 1, p + 1\} = \left(p^2 - 1\right)/2$ to divide $N - 1$.

A_-: We have $\beta^N \equiv \beta' \bmod p$. If $\left(\frac{d}{p}\right) = -1$ then $\beta^N = \beta' = \beta^p$ and we require the order of β, which can be $p^2 - 1$, to divide $N - p$. If $\left(\frac{d}{p}\right) = +1$ then it can be the case that β' is not equal to any power of β in R^*, which is not cyclic: for example, suppose β corresponds to $(1, -1) \in \mathbb{F}_p \oplus \mathbb{F}_p$ so that $\beta' \leftrightarrow (-1, 1)$. So there is no condition on p and N which will guarantee that N satisfies the condition in this case. We note that if β corresponds to $(a, b) \in \mathbb{F}_p \oplus \mathbb{F}_p$, then we are requiring that $a^N \equiv b$ and $b^N \equiv a$. So the β which satisfy this condition are the $\beta \leftrightarrow (a, a^N)$ with $a^{N^2} \equiv a \bmod p$: the number of such β is maximised when $p - 1 | N^2 - 1$, and there are then $p - 1$ such values of β.

A^b_-: We have $\beta^N \equiv \beta' \bmod p$ when $B = b$: we assume $b \neq 1$. If $\left(\frac{d}{p}\right) = -1$ then $\beta^N = \beta' = \beta^p$ and we require the order of β, which can be $e(p+1)$, to divide $N - p$, where e is the order of b in ${\mathbb{F}_p}^*$. If $\left(\frac{d}{p}\right) = +1$ then it can again be the case that β' is not equal to any power of β: consider $\beta \leftrightarrow (1, b)$. Again there is no condition on p and N which will guarantee that N satisfies the condition. If $\beta \leftrightarrow (a, b/a)$, we are requiring that $a^N \equiv b/a$ and $(b/a)^N \equiv a \bmod p$. So we require $a^{N+1} \equiv b$ and $a^{N+1} \equiv b^N \bmod p$, which is impossible unless $b^N \equiv b \bmod p$, which is equivalent to the condition that $e | N - 1$ where e is the multiplicative order of $b \bmod p$. We now have the condition that $a^{N+1} \equiv b \bmod p$. Put $p - 1 = ef$. By Lemma 3.2 the number of solutions to this equation is maximised when $f | N + 1$ and n/f is prime to e: when this occurs, the number of solutions is f.

A^1_-: Again we have $\beta^N \equiv \beta' \bmod p$ when $B = 1$, so $\beta^{N+1} \equiv 1 \bmod p$. The order of β can be the order of C, that is, $p - \left(\frac{d}{p}\right)$, so we require $\operatorname{lcm}\{p - 1, p + 1\} = \left(p^2 - 1\right)/2$ to divide $N + 1$.

B: We have $\beta^N = (x + y\sqrt{d})^N = x + z\sqrt{d}$ for some z. Since N is necessarily a Carmichael number, we have $\beta^N(\beta')^N = (\beta\beta')^N = B^N \equiv B \bmod N$, so that $z^2 \equiv y^2 \bmod N$ if this condition is satisfied. For any p dividing N we therefore have $z \equiv \pm y \bmod p$, so that $\beta^N = \beta$ or β' in $R(p, d)$. The condition $\beta^N = \beta'$ need not hold in the case $\left(\frac{d}{p}\right) = +1$, as discussed in case A_-, and there is no condition on p and N which will ensure that this

holds. The condition $\beta^N = \beta$ is equivalent to requiring that the order of β, which can be $p^2 - 1$, divide $N - 1$.

$B_{\pm}^b$**:** We have $\beta^N \equiv (x + y\sqrt{d})^N \equiv x + z\sqrt{d} \bmod N$ for some z whenever $\mathcal{N}(\beta) = x^2 - dy^2 = b$. Suppose that p^f is a prime power factor of N with $\left(\frac{d}{p}\right) = +1$. Consider $\beta \leftrightarrow (1, b) \in \mathbb{Z}/\langle p^f \rangle \oplus \mathbb{Z}/\langle p^f \rangle$, so that $\beta^N \leftrightarrow (1, b^N)$. We have $1 + b \equiv 1 + b^N \bmod p^f$, so that $b^N \equiv b \bmod p^f$. Now consider $\beta \leftrightarrow (a, b/a)$. We have $a + b/a \equiv a^N + b^N/a^N \equiv a^N + b/a^N \bmod p^f$. So $(a^{N-1} - 1)a \equiv b(a^{N-1} - 1)/a^N$, that is, $(a^{N-1} - 1)(a - b/a^N) \equiv 0 \bmod p^f$. If $b \not\equiv 1 \bmod p$ it cannot happen that $a^{N+1} \equiv b \bmod p^f$ for all $a \bmod p^f$, so we require that $a^{N-1} \equiv 1 \bmod p^f$ for all a: that is, that $f = 1$ and $p - 1|N - 1$. If $b \equiv 1 \bmod p$ then the two factors $a^{N-1} - 1$ and $a^{N+1} - b$ cannot both be divisible by p unless $a \equiv \pm 1 \bmod p$. This cannot be the case since $p > 3$. So the alternative condition $f = 1$ and $p - 1|N + 1$ will also suffice to ensure that the condition holds. We see that in any case N must be squarefree.

Now consider the case when $\left(\frac{d}{p}\right) = -1$. Suppose $p|N$. We have $\beta^N + (\beta')^N \equiv \beta + \beta' \bmod p$, so $\beta^N + (b/\beta)^N \equiv \beta + b/\beta$. We have $\beta^N - \beta \equiv b(\beta^N - \beta)/\beta^{N+1}$, so $(\beta^N - \beta)(1 - b/\beta^{N+1}) \equiv 0 \bmod p$. The two factors cannot both be divisible by p unless $\beta^{N-1} \equiv 1$ and $\beta^{N+1} \equiv b \bmod p$, which entail $\beta^2 \equiv b$: since $\beta\beta' \equiv b$ this requires $\beta \equiv \beta' \bmod p$. Otherwise, we have the alternative conditions $\beta^{N-1} \equiv 1 \bmod p$ or $\beta^{N+1} \equiv b \bmod p$. Since by Proposition 3.1 the order of β can be $e(p+1)$, where e is the multiplicative order of $b \bmod p$, we require $e(p+1)|N-1$ for the first condition to hold. For the second condition we have $\beta^{N+1} \equiv b \bmod p$ iff $\beta^{N+1} \equiv \beta\beta'$ iff $\beta^N \equiv \beta'$ iff $\beta^N \equiv \beta^p$, which requires that $e(p+1)|N-p$.

B^{-1}**:** We have $b = -1$, so the multiplicative order of b is 2. We require that N be square-free, that $p - 1|N - 1$ and that $2(p+1)$ divide either $N - 1$ or $N - p$ for each p.

B^1**:** We have $b = 1$, so the multiplicative order of b is 1. We require that N be square-free, that $p - 1|N \pm 1$ and that $p + 1$ divide $N - 1$ or $N - p$.

□

Lidl, Müller and Oswald [17], [18], [23] characterize a *strong Fibonacci pseudoprime* as a Carmichael number $N = \prod p_i$ with one of the following properties: either *(Type I)* an even number of the p_i are $\equiv 3 \bmod 4$ with $p^2 - 1|N - 1$ for the $p_i \equiv 3 \bmod 4$ and $p_i + 1|N \pm 1$ for the $p_i \equiv 1 \bmod 4$; or *(Type II)* there is an odd number of p_i, all $\equiv 3 \bmod 4$, and $p_i^2 - 1|N - p_i$ for all p_i. (A strong type II Fibonacci pseudoprime is termed a *strong* (-1)*-Dickson pseudoprime* in [23].) They were not able to exhibit any such numbers. We found just one Type I strong Fibonacci pseudoprime less than 10^{16}, already mentioned in [24], namely

$$443372888629441 = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331,$$

and none of Type II. This also answered the question of Di Porto and Filipponi [5].

Guillaume and Morain [13] quote Williams [33] as defining a Δ*-Lucas pseudoprime* by the condition $U_{N-\epsilon} \equiv 0 \bmod N$ for all Lucas sequences with defining equation $X^2 - PX + Q$ with $P^2 - 4Q = \Delta$ and $(N, \Delta Q) = 1$. The is just condition $C(\Delta)$, equivalent to $A^1(\Delta)$ by Proposition 5.2 (4). We recover the result that N is an absolute pseudoprime for this test iff N is square-free and $p - \epsilon_p|N - \epsilon_N$.

Guillaume and Morain [13] further define a *strong Dickson-*(c) *pseudoprime* if the Dickson polynomial $g_N(m, c) \equiv m \bmod N$ for all m. This is equivalent to $V_N \equiv m$ for the Lucas sequence attached to the polynomial $X^2 - mX + c$. So this is just condition B^c.

Criterion	$\left(\frac{d}{p}\right)=+1$	P	$\left(\frac{d}{p}\right)=-1$	In general
A_+	$p-1\|N-1$		$p^2-1\|N-1$	$p^2-1\|N-1$
A_+^b	$p-1\|N-1$		$e(p+1)\|N-1$	$\mathrm{lcm}\{p-1,e(p+1)\}\|N-1$
A_+^{-1}	$p-1\|N-1$		$2(p+1)\|N-1$	$\mathrm{lcm}\{p-1,2(p+1)\}\|N-1$
A_+^1	$p-1\|N-1$		$p+1\|N-1$	$(p^2-1)/2\|N-1$
A_-	$\boxed{p-1\|N^2-1}$	$\frac{1}{p-1}$	$p^2-1\|N-p$	$\boxed{p^2-1\|N-p}$
A_-^b	$\boxed{e\|N-1}$ and $\boxed{f\|N+1}$	$\frac{1}{e}$	$e(p+1)\|N-p$	$e(p+1)\|N-p$ and $\boxed{f\|N+1}$
A_-^{-1}	$\boxed{(p-1)/2\|N+1}$	$\frac{1}{2}$	$2(p+1)\|N-p$	—
A_-^1	$p-1\|N+1$		$p+1\|N+1$	$(p^2-1)/2\|N+1$
B	$p-1\|N-1$		$p^2-1\|N-1$ or $p^2-1\|N-p$	$p^2-1\|N-1$ or $p^2-1\|N-p$
B^b	$p-1\|N-1$		$e(p+1)\|N-1$ or $e(p+1)\|N-p$	$\mathrm{lcm}\{p-1,e(p+1)\}\|N-1$ or $\mathrm{lcm}\{p-1,e(p+1)\}\|N-p$
B^{-1}	$p-1\|N-1$		$2(p+1)\|N-1$ or $2(p+1)\|N-p$	$\mathrm{lcm}\{p-1,2(p+1)\}\|N-1$ or $\mathrm{lcm}\{p-1,2(p+1)\}\|N-p$
B^1	$p-1\|N-1$ or $p-1\|N+1$		$p+1\|N-1$ or $p+1\|N+1$	$p-1\|N\pm1$ and $p+1\|N\pm1$

TABLE 1. Requirements for absolute pseudoprimes for criteria of type A and B. Column P gives the proportion of bases for which the criterion can be satisfied when this is not 1: the requirements for such cases are boxed. e denotes the multiplicative order of b modulo p and $f=(p-1)/e$.

A *strong Fibonacci pseudoprime* is a strong Dickson-(-1) pseudoprime: this is just condition B^{-1}. We find that such a pseudoprime is a Carmichael number satisfying $2(p+1)|N-1$ or $N-p$.

A *superstrong Dickson pseudoprime* is a strong Dickson-(c) pseudoprime for all c, hence satisfies condition B. We require such a number to be a Carmichael number with $p^2-1|N-1$ or $N-p$.

Gordon [8],[7], [9],[10] defines an *D-elliptic pseudoprime* to be an N such that $\left(\frac{D}{p}\right)=-1$ and $p+1|N+1$ for all $p|N$, where $-D$ is a discriminant of class-number 1.

Williams [33] asked whether there are any Carmichael numbers N with an odd number of prime divisors and the additional property that for $p|N$, $p+1|N+1$. There are no such Carmichael numbers up to 10^{16}. We note that type II strong Fibonacci pseudoprimes are a special case of this condition.

Jones[1] has defined various special kinds of Carmichael numbers N. A *Lucas–Carmichael-$(-)$ number* has the property that $p|N$ implies $(p-1)/2$ and $(p+1)/2$ both divide $N-1$: it is *strong* if $p-1$ and $p+1$ both divide $N-1$ and *unusually strong* if p^2-1 divides $N-1$.

[1]Private communication.

The five Lucas–Carmichael-$(-)$ numbers up to 10^{16} are

$$\begin{aligned} 28295303263921 &= 29 \cdot 31 \cdot 67 \cdot 271 \cdot 331 \cdot 5237, \\ 443372888629441 &= 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331, \\ 582920080863121 &= 41 \cdot 53 \cdot 79 \cdot 103 \cdot 239 \cdot 271 \cdot 509, \\ 894221105778001 &= 17 \cdot 23 \cdot 29 \cdot 31 \cdot 79 \cdot 89 \cdot 181 \cdot 1999, \\ 2013745337604001 &= 17 \cdot 37 \cdot 41 \cdot 131 \cdot 251 \cdot 571 \cdot 4159. \end{aligned}$$

The number 582920080863121 is a strong Lucas–Carmichael-$(-)$ number, and a pseudoprime for criterion A_+^1 and hence B^1. The number 443372888629441 is unusually strong, and pseudoprime for criteria A_+ and B; hence also for A_+^{-1}, A_+^1, B^{-1} and B^1.

A *Lucas–Carmichael-$(+)$ number* has the property that $p|N$ implies $(p-1)/2$ and $(p+1)/2$ both divide $N+1$: it is *strong* if $p-1$ and $p+1$ both divide $N-1$ and *unusually strong* if $p^2-1|N+1$.

The seven Lucas–Carmichael-$(+)$ numbers up to 10^{13} are

$$\begin{aligned} 6479 &= 11 \cdot 19 \cdot 31, \\ 84419 &= 29 \cdot 41 \cdot 71, \\ 1930499 &= 89 \cdot 109 \cdot 199, \\ 7110179 &= 37 \cdot 41 \cdot 43 \cdot 109, \\ 15857855 &= 5 \cdot 13 \cdot 17 \cdot 113 \cdot 127, \\ 63278892599 &= 13 \cdot 47 \cdot 137 \cdot 239 \cdot 3163, \\ 79397009999 &= 23 \cdot 29 \cdot 41 \cdot 43 \cdot 251 \cdot 269. \end{aligned}$$

Of these, 79397009999 is unusually strong. It is a pseudoprime for criteria A_-^1 and B^1.

6. Strong quadratic tests

Arnault [1] defines a *strong Lucas test* for an odd number N as follows: let $\epsilon = \left(\frac{d}{N}\right)$ and put $N - \epsilon = 2^r s$ with s odd. The criterion requires that either $U_s \equiv 0 \bmod N$ or $V_{2^j s} \equiv 0$ for some j with $0 \le j < r$.

He shows that the proportion of tests which falsely declare N prime is at most $1/2$, and indeed at most $4/15$ if N is not of the special form $N = pq$ with p and $q = p+2$ twin primes and $\left(\frac{D}{p}\right) = -1$, $\left(\frac{D}{q}\right) = +1$.

Since $U_{2k} = U_k V_l$ by equation (3.4), the condition implies that $U_{N-\epsilon} \equiv 0 \bmod N$: this is condition C in the table above, and we have seen that it is equivalent to the Fermat criterion for the corational groups $C(N, d)$. The strong Lucas test is thus the 2-strengthening of test C.

7. A Bayesian result

We noted that for a given composite number, the probability of the strong test incorrectly returning `probable prime` on a random base is at most $\frac{1}{4}$.

More important in practice is the probability that a number which has passed the strong test is in fact composite. We consider, for example, a process which chooses odd numbers N of a given size uniformly at random and outputs N if it passes r rounds of the strong test with random bases. Damgård and Landrock [2] and Kim and Pomerance [16] give results in this direction.

In this section we indicate how similar results may be obtained for the 2-strengthening of criterion A.

It ios necessary to specify a sample space of integers to apply the test to: we consider the space $\mathcal{M}_k$ of all odd k-bit integers taken uniformly at random. Our

strategy is to find "small" subsets $\mathcal{E}_m$ of $\mathcal{M}_k$ such that if N is composite and not in $\mathcal{E}_m$ then the probability that N passes the test is also small.

Let $\Psi(N) = N - \left(\frac{d}{N}\right)$. Let $\Phi_{\mathcal{G}} = \Phi$ be the multiplicative function extending $\Phi(p) = \Psi(p) = p - \left(\frac{d}{p}\right)$ for prime p.

Suppose $N \in \mathcal{M}_k$, and put $N = \prod_i^d p_i^{a_i}$. For $p_i \mid N$, let $c_i = \mathrm{hcf}(\Phi(p_i), \Psi(N))$ and let $b_i c_i = \Phi(p_i)$. We have a bound on the probability of composite N passing the criterion

$$\mu(N) \le 2^{-d+1} \prod_{i=1}^{d} \frac{b_i}{p_i}$$

coming from the 2-strengthening part of the criterion.

Put $X = 2^k$. We have $|\mathcal{M}_k| = \frac{1}{4}X$. Fix m with $2 \le m \le \sqrt{k/2}$ and put $A = 2^{m-1}$, $\delta = 1/m$. Put $Y = \frac{1}{2}X^{\delta}$. Put

$$\mathcal{E}_m = \{N \in \mathcal{M}_k \mid N \text{ is composite}, b_i < A \text{ for some } p_i | N \text{ with } p_i > Y\}.$$

Proposition 7.1. *For $2 \le m \le \sqrt{k/2}$ the set $\mathcal{E}_m$ of composite numbers satisfies*

- *(i) for composite $N \in \mathcal{M}_k \setminus \mathcal{E}_m$, we have $\mu(N) \le 2^{-m}$;*
- *(ii) $|\mathcal{E}_m|/|\mathcal{M}_k| = O\left(\frac{m}{k}\right) 2^{2m-k/m}$.*

Proof. Put

$$W(N) = \frac{1}{\Psi(N)} \prod_i c_i = \frac{1}{N} \prod_i \frac{1}{b_i}$$

We first need to show (i). Suppose that N is composite and not in $\mathcal{E}_m$.

If $d > m$ then $\mu(N) \le 2^{-m} W(N) \le 2^{-m}$, as required. So we suppose that $N \notin \mathcal{E}_m$ and that $d \le m$.

Suppose first that $n \notin \mathcal{E}_m$ because the prime factors p_i of N all satisfy $p_i < Y$. Put $D = \prod_i p_i$. Now N/D is coprime to $\Psi(N)$ but divides $\Phi(N)$: indeed

$$\Phi(N) = N \prod_{p|N} \left(\frac{p-1}{p}\right) = \frac{N}{D} \prod_{p|N} (p-1).$$

Now $D < Y^m$ and $N > \frac{1}{2}X$, so

$$N/D \ge NY^{-m} = N \left(\frac{1}{2}X^{\delta}\right)^{-m} \ge \frac{1}{2}X/2^{-m}X = 2^{m-1}.$$

Now $W(N) \le D/N$, so $W(N) \le 2^{1-m}$ and again $\mu(N) \le 2^{-m}$.

Finally suppose that N has a prime factor $p_i > Y$; since $N \notin \mathcal{E}_m$, we must have $b_i > A$. Then $W(N) < 1/A$ and since $\mu(N) \le W(N)/2$, we have $\mu(N) < 1/2A = 2^{-m}$.

We now prove part (ii). Fix a prime $p > Y$. Suppose $N \in \mathcal{E}_m$ because $p|N$ with $p > Y$ and $b < A$. Now $N \equiv 0 \mod p$ and $N \equiv \left(\frac{d}{N}\right) \mod c$. Since $c | p \pm 1$, we have p and c coprime, and so N satisfies a congruence condition modulo pc. Since N cannot equal p, the number of such N in $\mathcal{M}_k$ is at most $\frac{1}{2}X/pc$, which is $\frac{1}{2}Xb/p(p-1)$.

Summing over all $p > Y$ and $b < A$, we have

$$|\mathcal{E}_m| \le \sum_{p>Y} \sum_{b<A} \frac{\frac{1}{2}Xb}{p(p-1)} \le \sum_{p>Y} \frac{XA^2}{p^2} = \mathrm{O}\left(\frac{XA^2}{Y}\right).$$

□

Theorem 7.2.

$$\mathbb{P}(N \text{ composite} | N \text{ passes } r \text{ tests}) = O\left(k\, 2^{-\sqrt{k}/2}\right).$$

Proof. We have

$$\mathbb{P}(N \text{ composite}|N \text{ passes } r \text{ tests}) = \frac{\mathbb{P}(N \text{ composite and } N \text{ passes } r \text{ tests})}{\mathbb{P}(N \text{ passes } r \text{ tests})}$$

Now

$$\begin{aligned}\mathbb{P}(N \text{ composite and passes } r \text{ tests}) &< \mathbb{P}(N \in \mathcal{E}_m \text{ and passes } r \text{ tests}) \\ &+\mathbb{P}(N \text{ composite and } N \notin \mathcal{E}_m \text{ and passes } r \text{ tests}) \\ &< 2^{-m} + \mathrm{O}\Big(\frac{m}{k}\, 2^{2m-k/m}\Big)\end{aligned}$$

and

$$\mathbb{P}(N \text{ passes } r \text{ tests}) > \mathbb{P}(N \text{ prime}) > 1/k,$$

using the Prime Number Theorem. Hence

$$\mathbb{P}(N \text{ composite}|N \text{ passes } r \text{ tests}) < k(2^{-m} + \mathrm{O}\Big(\frac{m}{k}\, 2^{2m-k/m}\Big)).$$

Now putting $m = \sqrt{k}/2$ we have

$$\mathbb{P}(N \text{ composite}|N \text{ passes } r \text{ tests}) = \mathrm{O}\Big(k2^{-\sqrt{k}/2}\Big).$$

□

References

[1] François Arnault, *The Rabin–Monier theorem for Lucas pseudoprimes*, Math. Comp. **66** (1997), no. 218, 869–881.

[2] Ivan Damgård and Peter Landrock, *Improved bounds for the Rabin primality test*, in Ganley [6], Proceedings, 3rd IMA conference on cryptography and coding, Cirencester, December 1991., pp. 117–128.

[3] D.W. Davies (ed.), *Advances in cryptology — EUROCRYPT '91*, Lecture notes in Computer Science, vol. 547, Berlin, Springer–Verlag, 1991.

[4] Jean-Marie De Koninck and Claude Levesque (eds.), *Number theory: proceedings of the international number theory conference, Université de Laval, 1987*, Berlin, Walter de Gruyter, 1989.

[5] A. Di Porto and P. Filipponi, *A probabilistic primality test based on the properties of certain generalized Lucas numbers*, in Günther [14], pp. 211–223.

[6] M. Ganley (ed.), *Cryptography and coding III*, IMA conference series (n.s.), vol. 45, Institute of Mathematics and its Applications, Oxford University Press, 1993, Proceedings, 3rd IMA conference on cryptography and coding, Cirencester, December 1991.

[7] Dan M. Gordon, *On the number of elliptic pseudoprimes*, Math. Comp. **52** (1989), no. 185, 231–245.

[8] Daniel M. Gordon, *Pseudoprimes on elliptic curves*, in De Koninck and Levesque [4], pp. 290–305.

[9] Daniel M. Gordon and Carl Pomerance, *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. **57** (1991), no. 196, 825–838, See also [10].

[10] ———, *The distribution of Lucas and elliptic pseudoprimes: corrigendum*, Math. Comp. **60** (1993), no. 202, 877, Corrigendum to [9].

[11] Jon Grantham, *A probable prime test with high confidence*, J. Number Theory **72** (1998), no. 1, 32–47.

[12] ———, *Frobenius pseudoprimes*, Math. Comp. **70** (2001), no. 234, 873–891.

[13] Dominique Guillaume and François Morain, *Building pseudoprimes with a large number of prime factors*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 4, 263–267.

[14] C.G. Günther (ed.), *Advances in cryptology — EUROCRYPT '88*, Lecture notes in Computer Science, vol. 330, Berlin, Springer–Verlag, 1988.

[15] Marc Joye and Jean-Jacques Quisquater, *Efficient computation of full Lucas sequences*, Electronics Letters **32** (1996), no. 6, 537–538.

[16] Su Hee Kim and Carl Pomerance, *The probability that a random probable prime is composite*, Math. Comp. **53** (1989), no. 188, 721–741.

[17] Rudolf Lidl and Winfried B. Müller, *A note on strong Fibonacci pseudoprimes*, in Seberry and Pieprzyk [29], pp. 311–317.

[18] Rudolf Lidl, Winfried B. Müller, and Alan Oswald, *Some remarks on strong Fibonacci pseudoprimes*, Appl. Algebra Engrg. Comm. Comput. **1** (1990), 59–65.

[19] Rudolf Lidl and Harald Niederreiter, *Finite fields*, second ed., Encyclopaedia of Mathematics and its applications, vol. 20, Cambridge University Press, Cambridge, 1997.
[20] G.L. Miller, *Riemann's hypothesis and tests for primality*, Conference Record of Seventh Annual ACM Symposium on Theory of Computation (Albuquerque, New Mexico), ACM, 5–7 May 1975, pp. 234–239.
[21] ———, *Riemann's hypothesis and tests for primality*, J. Comp. System Sci. **13** (1976), 300–317.
[22] R.A. Mollin (ed.), *Number theory and its applications*, Dordrecht, Kluwer Academic, 1989, Proceedings of the NATO Advanced Study Institute on Number Theory and Applications.
[23] W.B. Müller and A. Oswald, *Dickson pseudoprimes and primality testing*, in Davies [3], pp. 512–516.
[24] Richard G.E. Pinch, *The Carmichael numbers up to* 10^{15}, Math. Comp. **61** (1993), 381–391, Lehmer memorial issue.
[25] ———, *Recurrent sequences modulo prime powers*, in Ganley [6], Proceedings, 3rd IMA conference on cryptography and coding, Cirencester, December 1991., pp. 297–310.
[26] ———, *The Carmichael numbers up to* 10^{16}, March 1998, `arXiv:math.NT/9803082`.
[27] Michael O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), no. 1, 128–138.
[28] Hans Riesel, *Prime numbers and computer methods for factorization*, second ed., Progress in mathematics, vol. 126, Birkhauser, Boston, 1994.
[29] Jennifer Seberry and Josef Pieprzyk (eds.), *Advances in cryptology* - AUSCRYPT *'90*, Lecture notes in Computer Science, vol. 453, Berlin, Springer–Verlag, 1990.
[30] Jennifer Seberry and Yuliang Zheng (eds.), *Advances in cryptology* - AUSCRYPT *'92*, Lecture notes in Computer Science, vol. 718, Berlin, Springer–Verlag, 1993.
[31] R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), no. 1, 84–85.
[32] ———, *Erratum: A fast Monte-Carlo test for primality*, SIAM J. Comput. **7** (1978), no. 1, 118.
[33] Hugh C. Williams, *On numbers analogous to the Carmichael numbers*, Canad. Math. Bull. **20** (1977), 133–143.

2 Eldon Road, Cheltenham, Glos GL52 6TU, U.K.
E-mail address: `rgep@chalcedon.demon.co.uk`